A New Multiple Access Wiretap Channel Model

Mohamed Nafea and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
mnafea@psu.edu *yener@engr.psu.edu*

***Abstract*—A new model for the two-user multiple-access wiretap channel is considered. In this model, the legitimate (main) channel is a discrete memoryless channel (DMC), and the wiretapper chooses a fixed-length subset of the channel uses where she has perfect access to the transmitted symbols of the both users, while observing the remainder of the transmitted codewords through a second DMC. As such, it generalizes the existing multiple-access wiretap channel models and extends the recently proposed new wiretap channel model to a multiple access setting. An achievable strong secrecy rate region for the model is derived. The achievability is established by solving a dual multi-terminal secret key agreement problem in the source model, where two independent sources are communicating confidential keys to a common decoder over a public channel in the presence of a compound wiretapping source. The secrecy of the two keys in the dual source model is established by deriving a lemma which provides a doubly exponential convergence rate for the probability of the keys being uniform and independent from the public discussion and the wiretapping source observation.**

I. Introduction

The wiretap channel II (WTC-II) models a wiretap channel (WTC) with a noiseless main channel and a wiretapper who selects a fixed-length subset of the transmitted codeword symbols to noiselessly observe, while observing erasures in the remaining positions [1]. Authors in [1] have shown that the secrecy capacity of this model is equal to the secrecy capacity when the channel to the wiretapper is a discrete memoryless (DM) binary erasure channel (EC), concluding that the additional capability at the wiretapper of choosing erasure positions does not deteriorate the secrecy capacity.

Reference [2] introduced a DM main channel to the WTC-II in order to address a more general model with a wiretapper that is more capable than a passive observer. Authors in [2] derived inner and outer bounds for the capacity-equivocation region. Later, the secrecy capacity of the channel was shown to be equal to the secrecy capacity when the wiretapper has a DM EC [3], showing that, once again, the secrecy capacity does not degrade by the additional capability at the wiretapper. The WTC-II with a DM main channel is recently extended to the multiple access setting, with the wiretapper partially observing one user or a superposition of two users, in [4].

In recent reference [5], we have introduced and identified the strong secrecy capacity of a new WTC model in which the main channel is a DMC and the wiretapper, in addition to perfectly accessing a subset of the transmitted symbols of her choosing, observes the output of a DMC in the remaining positions instead of erasures. This new model includes as special cases both the classical WTC [6] by setting the subset size to zero, and the WTC-II with a DM main channel [2] by setting the wiretapper DMC to an EC with erasure probability one. Reference [5] thus quantifies the deterioration in secrecy capacity with respect to the previous wiretap models.

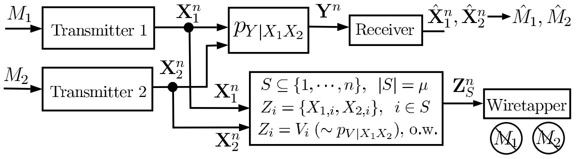
M_1
Transmitter 1
$\mathbf{X}_1^n$
$p_{Y|X_1X_2}$
$\mathbf{Y}^n$
Receiver
$\hat{\mathbf{X}}_1^n, \hat{\mathbf{X}}_2^n \rightarrow \hat{M}_1, \hat{M}_2$
M_2
Transmitter 2
$\mathbf{X}_2^n$
$\mathbf{X}_1^n$
$S \subseteq \{1, \cdots, n\}, \ |S| = \mu$
$Z_i = \{X_{1,i}, X_{2,i}\}, \ i \in S$
$Z_i = V_i \ (\sim p_{V|X_1X_2})$, o.w.
$\mathbf{X}_2^n$
$\mathbf{Z}_S^n$
Wiretapper
$\cancel{M_1}$ $\cancel{M_2}$

Fig. 1. New multiple-access wiretap channel model.

In this paper, we extend the new WTC model to a two-user multiple-access WTC (MAC-WT) [7]. The wiretapper in this model noiselessly observes both the symbols of the two users in the positions of the subset she chooses, while observing the remainder of the two codewords through a DMC. An achievable strong secrecy rate region is derived by solving a dual multi-terminal secret key agreement problem [8] and converting the solution to the original channel model using probability distribution approximation arguments [9].

Notation: We use the convention $A_{1:2} = (A_1, A_2)$ for random variables (vectors) and their realizations. $\mathbf{X}_S = \{X_i\}_{i \in S}$, $S \subseteq \mathbb{N}$. p_X^U denotes a uniform distribution over X. $\mathbb{V}(p_X, q_X)$, $\mathbb{D}(p_X || q_X)$ denote the total variation distance and K-L divergence between p_X, q_X. $\mathbf{Conv}(\mathcal{R})$ is the convex hull of $\mathcal{R}$.

II. Channel Model

We consider the channel model in Fig. 1. The main channel $\{\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, p_{Y|X_1X_2}\}$ is a DMC which consists of two finite input alphabets $\mathcal{X}_1, \mathcal{X}_2$, a finite output alphabet $\mathcal{Y}$, and a transition probability $p_{Y|X_1X_2}$. In order to communicate message M_j, $j = 1, 2$, which is uniformly distributed over $\mathcal{M}_j = [\![1, 2^{nR_j}]\!]$, to the common receiver, and to keep it secret from the wiretapper, transmitter j maps its message into the codeword $\mathbf{X}_j^n = [X_{j,1} \ \cdots \ X_{j,n}] \in \mathcal{X}^n$ using a stochastic encoder. The messages M_1, M_2 are independent. The receiver, upon receiving $\mathbf{Y}^n \in \mathcal{Y}^n$, outputs the estimates $\hat{M}_j, j = 1, 2$, of the transmitted messages. Let $\mathbf{V}^n = [V_1 \ \cdots, V_n] \in \mathcal{V}^n$ denote the n-letter output of the DMC $p_{V|X_1X_2}$; $\mathcal{V}$ is a finite alphabet. The wiretapper chooses the subset $S \in \mathcal{S}$, with

$$\mathcal{S} \triangleq \left\{ S : S \subseteq [\![1, n]\!], \ |S| = \mu \leq n, \ \alpha = \frac{\mu}{n} \in [0, 1] \right\}, \quad (1)$$

and observes $\mathbf{Z}_S^n = [Z_1^S \ \cdots \ Z_n^S] \in \mathcal{Z}^n$, where

$$Z_i^S = \begin{cases} \{X_{1,i}, X_{2,i}\}, & i \in S \\ V_i, & \text{otherwise}, \end{cases} \tag{2}$$

and $\mathcal{Z} = \{\mathcal{X}_1 \times \mathcal{X}_2\} \cup \mathcal{V}$. An $(n, 2^{nR_1}, 2^{nR_2})$ channel code $\mathcal{C}_n = \{\mathcal{C}_{1,n}, \mathcal{C}_{2,n}\}$ consists of the message sets $\mathcal{M}_j$, the stochastic encoders $P_{\mathbf{X}_j^n|M_j,\mathcal{C}_{j,n}}$, $j = 1, 2$, and the decoder. (R_1, R_2) is an achievable strong secrecy rate pair if there is a sequence of $(n, 2^{nR_1}, 2^{nR_2})$ codes, $\{\mathcal{C}_n\}_{n\geq 1}$, such that (s.t.)

$$\lim_{n\to\infty} \mathbb{P}\big(\hat{M}_{1:2} \neq M_{1:2}|\mathcal{C}_n\big) = 0 \qquad \textbf{Reliability},$$
$$\lim_{n\to\infty} \max_S I(M_{1:2}; \mathbf{Z}_S^n|\mathcal{C}_n) = 0 \qquad \textbf{Strong Secrecy.}$$

III. Main Result

Theorem 1 *For $\alpha \in [0, 1]$, an achievable strong secrecy rate region for the new MAC-WT model in Fig. 1 is given by*

$$\begin{aligned}\mathcal{R}(\alpha) = \textbf{Conv} \bigcup_{p_{U_1X_1}p_{U_2X_2}} \Big\{&(R_1, R_2) : \\ &R_1 \leq I(U_1; Y|U_2) - I(U_1; V) - \alpha I(U_1; X_1|V), \\ &R_2 \leq I(U_2; Y|U_1) - I(U_2; V) - \alpha I(U_2; X_2|V), \\ &R_1 + R_2 \leq I(U_{1:2}; Y) - I(U_{1:2}; V) - \alpha I(U_{1:2}; X_{1:2}|V)\Big\}.\end{aligned} \tag{3}$$

where the union is over all distributions $p_{U_1X_1}p_{U_2X_2}$ which satisfy the Markov chains $U_1 - X_1 - YV$ and $U_2 - X_2 - YV$.

Proof: The proof is provided in Section IV. ■

Remark 1 By setting the size of the subset S to zero, i.e., $\alpha = 0$, in (3), we obtain the achievable strong secrecy rate region derived in [10, Theorem 1] for the MAC-WT. The same region was derived under a weak secrecy criterion in [7], [11].

Reference [4] provides achievable strong secrecy rate regions for the two-user MAC-WT II, where the main channel is a DMC and the wiretapper selects a subset of the channel uses and observes erasures outside this subset, under two different wiretapping scenarios. In the first scenario, the wiretapper, in each position of the subset, decides to noiselessly observe either the first or the second user's transmitted symbol, while in the second scenario, the wiretapper observes a noiseless superposition of the two symbols. In the following corollary, we provide an achievable rate region for the MAC-WT II when the wiretapper observes *both* the transmitted symbols.

Corollary 1 *An achievable strong secrecy rate region for the two-user MAC-WT II with the wiretapper noiselessly observing both the transmitted symbols in the positions of the subset, is*

$$\begin{aligned}\mathcal{R}_{\text{II}}(\alpha) = \textbf{Conv} \bigcup_{p_{U_1X_1}p_{U_2X_2}} \Big\{&(R_1, R_2) : \\ &R_1 \leq I(U_1; Y|U_2) - \alpha I(U_1; X_1), \\ &R_2 \leq I(U_2; Y|U_1) - \alpha I(U_2; X_2), \\ &R_1 + R_2 \leq I(U_{1:2}; Y) - \alpha I(U_{1:2}; X_{1:2})\Big\}.\end{aligned} \tag{4}$$

where the union is over all distributions $p_{U_1X_1}p_{U_2X_2}$ which satisfy the Markov chains $U_1 - X_1 - Y$ and $U_2 - X_2 - Y$.

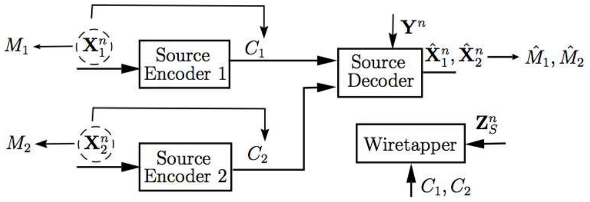

Fig. 2. Protocol A: Secret key agreement in the source model.

The proof follows from (3) by setting the DMC $p_{V|X_1X_2}$ to an EC with erasure probability one, i.e., $V =$ "?".

Remark 2 Not surprisingly, the rate region achievable for the first scenario in [4] is equal to the rate region achievable for the MAC-WT II model with the more capable wiretapper in (4). The reason is that when the wiretapper has the power of choosing to observe either symbol in every tapped position, each user ought to design their transmission according to the worst case scenario in which the wiretapper decides to observe only his symbols in all the positions she taps.

IV. Proof for Theorem 1

We first consider $U_{1:2} = X_{1:2}$. We fix $p_{X_{1:2}} = p_{X_1}p_{X_2}$ and describe two protocols; each protocol defines a set of random variables and induces a joint distribution over them.

Protocol A: This protocol considers a multi-terminal secret key agreement problem in the source model, see Fig. 2. In particular, let $\mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}$ be i.i.d. according to the distribution $p_{X_1}p_{X_2}p_{Y|X_{1:2}}$, where $p_{Y|X_{1:2}}$ is the transition probability of the main channel in Fig. 1. The sequence $\mathbf{X}_j, j = 1, 2$, observed at the jth source encoder, is randomly and independently binned into the two indices $M_j = \mathcal{B}_1^{(j)}(\mathbf{X}_j)$, $C_j = \mathcal{B}_2^{(j)}(\mathbf{X}_j)$, where $\mathcal{B}_1^{(j)}, \mathcal{B}_2^{(j)}$ are uniform over $[\![1, 2^{nR_j}]\!]$, $[\![1, 2^{n\tilde{R}_j}]\!]$. The indices $M_{1:2}$ represent the confidential keys. The messages $C_{1:2}$ are transmitted over a noiseless public channel to the decoder and observed by the wiretapper. The decoder observes the sequence $\mathbf{Y}$ and $C_{1:2}$, and outputs the estimates $\hat{\mathbf{X}}_{1:2}$, which are mapped to the estimates $\hat{M}_{1:2}$. Let $\mathcal{S}, \mathbf{Z}_S, \forall S \in \mathcal{S}$, be as in (1), (2). The wiretapper is a compound source $\mathbf{Z}_S \triangleq \{\mathcal{Z}, p_{\mathbf{Z}_S}\}$ whose distribution is only known to belong to the finite class $\{p_{\mathbf{Z}_S}\}_{S\in\mathcal{S}}$, where $|\mathcal{S}| = \binom{n}{\alpha n} \leq 2^n$.

Let $\mathbb{1}_\mathcal{A}$ denotes the indicator function of the event $\mathcal{A}$. The induced distribution for protocol A is expressed as

$$\begin{aligned}&\tilde{P}_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}} = p_{\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S}\tilde{P}_{M_{1:2}C_{1:2}|\mathbf{X}_{1:2}}\tilde{P}_{\hat{\mathbf{X}}_{1:2}|\mathbf{Y}C_{1:2}} \\ &= p_{\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S}\ \mathbb{1}_{\{\mathcal{B}_1^{(j)}(\mathbf{X}_j)=M_j,\mathcal{B}_2^{(j)}(\mathbf{X}_j)=C_j,\forall j=1,2\}}\ \tilde{P}_{\hat{\mathbf{X}}_{1:2}|\mathbf{Y}C_{1:2}} \\ &= \tilde{P}_{M_{1:2}C_{1:2}}\tilde{P}_{\mathbf{X}_{1:2}|M_{1:2}C_{1:2}}\ p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}_{1:2}}\tilde{P}_{\hat{\mathbf{X}}_{1:2}|\mathbf{Y}C_{1:2}}.\end{aligned} \tag{5}$$

Protocol B: This protocol considers the original channel model in Fig. 1, with the addition of common randomness $C_j, j = 1, 2$, that is available at all nodes, uniform over $[\![1, 2^{n\tilde{R}_j}]\!]$ and independent from all other variables. The encoders and decoder are defined as in (5). The induced joint distribution for protocol B, $P_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}}$, is equal to

$$p^U_{M_{1:2}}p^U_{C_{1:2}}\tilde{P}_{\mathbf{X}_{1:2}|M_{1:2}C_{1:2}}p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}_{1:2}}\tilde{P}_{\hat{\mathbf{X}}_{1:2}|\mathbf{Y}C_{1:2}}. \tag{6}$$

From protocol A, $\tilde{P}_{\mathbf{X}_{1:2}|M_{1:2}C_{1:2}} = \tilde{P}_{\mathbf{X}_1|M_1C_1}\tilde{P}_{\mathbf{X}_2|M_2C_2}$. Thus, for protocol B, the common randomness C_i available at the jth transmitter, $i,j = 1,2, i \neq j$, is not used to generate $\mathbf{X}_j$. At the end of the proof, we eliminate the common randomness $C_{1:2}$ by conditioning on certain instance of it.

The induced distributions in (5), (6) are random due to the random binning. We have ignored the $\hat{M}$ variables at this stage, as we will introduce them later as deterministic functions of the $\hat{\mathbf{X}}$ vectors after fixing the binning. The following two lemmas provide conditions on the rates $R_j, \tilde{R}_j, j = 1,2$, required for the closeness of the two induced distributions and secrecy of protocol A. Lemma 1 provides an *exponential decay* rate for the average, over the binning, of the total variation distance between the induced distributions, which is used to show a convergence in probability result that allows converting the secrecy criterion from protocol A to protocol B.

Lemma 1 *Let* $X_j \triangleq \{\mathcal{X}_j, p_{X_j}\}$, $j = 1,2$, *be two independent sources.* X_j *is randomly binned into* $M_j = \mathcal{B}_1^{(j)}(X_j)$, $C_j = \mathcal{B}_2^{(j)}(X_j)$, *where* $\mathcal{B}_1^{(j)}, \mathcal{B}_2^{(j)}$ *are independent and uniform over* $[\![1, \tilde{M}_j]\!]$, $[\![1, \tilde{C}_j]\!]$. *For* $\gamma_j > 0, j = 1,2$, *define the event* $\mathcal{D}_{\gamma_j}$ *as* $\mathcal{D}_{\gamma_j} \triangleq \{x_j \in \mathcal{X}_j : -\log p_{X_j}(x_j) > \gamma_j\}$. *Let* $\mathcal{B} \triangleq \{\mathcal{B}_1^{(j)}(x_j), \mathcal{B}_2^{(j)}(x_j)\}_{j=1,2,x_j\in\mathcal{X}_j}$. *Then, we have*

$$\mathbb{E}_{\mathcal{B}}\Big(\mathbb{V}\big(P_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}}p^U_{C_{1:2}}\big)\Big) \leq \sum_{j=1,2}\Big(\mathbb{P}(X_j \notin \mathcal{D}_{\gamma_j}) + {}^1\!/\!{}_2(\tilde{M}_j\tilde{C}_j2^{-\gamma_j})^{\frac{1}{2}}\Big), \text{ } P \textit{ is the induced distribution.} \quad (7)$$

Proof: See Appendix A. ■

Lemma 2 below provides a *doubly exponential* convergence rate for the probability that, in protocol A, the confidential keys and the public messages are uniform, and independent from the wiretapper's observation $\mathbf{Z}_S$ for any $S \in \mathcal{S}$, which is used, along with the union bound, to guarantee secrecy for the exponentially many possibilities of the subset S.

Lemma 2 *Let* $X_j \triangleq \{\mathcal{X}_j, p_{X_j}\}$, $j = 1,2$, *be two independent sources, both correlated with the compound source* $\{Z_S\} \triangleq \{\mathcal{Z}, p_{Z_S}\}, S \in \mathcal{S}$, *where* $|\mathcal{X}_1|, |\mathcal{X}_2|, |\mathcal{Z}|, |\mathcal{S}| < \infty$. X_j *is randomly binned into* M_j, C_j *as in Lemma 1. For* $\gamma_j, \gamma_{ij} > 0, j,i = 1,2, i \neq j$, *and any* $S \in \mathcal{S}$, *define*

$$\mathcal{D}_j^S \triangleq \big\{(x_{1:2}, z) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Z} : (x_j, z) \in \mathcal{D}^S_{\gamma_j}, (x_{1:2}, z) \in \mathcal{D}^S_{\gamma_{ij}}\big\}, \text{ where } \mathcal{D}^S_{\gamma_j} \triangleq \big\{(x_j, z) : -\log p_{X_j|Z_S}(x_j|z) > \gamma_j\big\}, \text{ and } \mathcal{D}^S_{\gamma_{ij}} \triangleq \big\{(x_{1:2}, z) : -\log p_{X_i|X_jZ_S}(x_i|x_j, z) > \gamma_{ij}\big\}.$$

If $\exists\delta \in]0, \frac{1}{2}[$ *s.t.* $\forall S$, $\min_{j=1,2}\mathbb{P}_{p_{X_{1:2}Z_S}}\big((X_{1:2}, Z_S) \in \mathcal{D}_j^S\big) \geq 1 - \delta^2$, *then, we have, for every* $\epsilon \in [0,1]$, *that*

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}}\mathbb{D}(P_{M_{1:2}C_{1:2}Z_S}||p^U_{M_{1:2}}p^U_{C_{1:2}}p_{Z_S}) \geq 2\tilde{\epsilon}\Big) \leq |\mathcal{S}||\mathcal{Z}|\min_{j,i=1,2,i\neq j}\Big\{e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_j}}{3\tilde{M}_j\tilde{C}_j}\right)} + e^{\left(\frac{-\epsilon^2(1-\delta)2^{\gamma_{ij}}}{3\tilde{M}_i\tilde{C}_i}\right)}\Big\}, \quad (8)$$

where $\tilde{\epsilon} = \max_{j=1,2}\{\epsilon + (\delta+\delta^2)\log(\tilde{M}_j\tilde{C}_j) + H_b(\delta^2)\}$, H_b *is the binary entropy function, and* P *is the induced distribution.*

Proof: See Appendix B. ■

We now apply Lemma 1 to protocol A to show the closeness of the two induced distributions. In Lemma 1, set $X_j = \mathbf{X}_j$, $\tilde{M}_j = 2^{nR_j}$, $\tilde{C}_j = 2^{n\tilde{R}_j}$, $\gamma_j = (1-\epsilon')nH(X_j), j = 1,2$; $\epsilon' > 0$ and $\mathbf{X}_j$ is defined as in protocol A, i.e., an i.i.d. sequence. Without loss of generality, we assume that $\forall x_j \in \mathcal{X}_j$, $p_{X_j}(x_j) > 0$. Using Hoeffding inequality, $\exists\beta_j > 0$ s.t.

$$\mathbb{P}(\mathbf{X}_j \notin \mathcal{D}_{\gamma_j}) = \mathbb{P}\Big(-\log p_{\mathbf{X}_j}(\mathbf{X}_j) \leq (1-\epsilon')nH(X_j)\Big) = \mathbb{P}\Big(\sum_{k=1}^{n}\log\frac{1}{p(X_{j,k})} \leq (1-\epsilon')nH(X_j)\Big) \leq e^{-\beta_jn}. \quad (9)$$

Substituting (9) and the choices for $\tilde{M}_j, \tilde{C}_j, \gamma_j$ in (7), gives

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}}, P_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}})\big) = \mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}}p^U_{C_{1:2}})\big) \leq 4\exp(-\beta n), \quad (10)$$

as long as $R_j + \tilde{R}_j < (1-\epsilon')H(X_j), \forall j = 1,2$, where $\beta > 0$.

For reliability of protocol A, we consider a Slepian-Wolf decoder, which implies that $\lim_{n\to\infty}\mathbb{E}_{\mathcal{B}}\big(\mathbb{P}_{\tilde{P}}(\hat{\mathbf{X}}_{1:2} \neq \mathbf{X}_{1:2})\big) = 0$ if $\tilde{R}_1 \geq H(X_1|X_2, Y)$, $\tilde{R}_2 \geq H(X_2|X_1, Y)$ and $\tilde{R}_1 + \tilde{R}_2 \geq H(X_{1:2}|Y)$ [12, Theorem 10.3]. Thus, $\forall S \in \mathcal{S}$ [9, Lemma 1]

$$\lim_{n\to\infty}\mathbb{E}_{\mathcal{B}}\Big(\mathbb{V}\big(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}}, \tilde{P}_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S}\mathbb{1}_{\{\hat{\mathbf{X}}_{1:2}=\mathbf{X}_{1:2}\}}\big)\Big) = 0. \quad (11)$$

Next, we apply Lemma 2 to protocol A in order to establish the secrecy criterion. In Lemma 2, for $j = 1,2$, set $X_j = \mathbf{X}_j$, $\tilde{M}_j = 2^{nR_j}$, $\tilde{C}_j = 2^{n\tilde{R}_j}$, $Z_S = \mathbf{Z}_S, \forall S \in \mathcal{S}$, where $\mathbf{X}_j, \mathcal{S}, \mathbf{Z}_S$ are defined as in protocol A. Since $\mathbf{X}_j$ is i.i.d. and the channel $p_{V|X_{1:2}}$ is a DMC, we have, $\forall S \in \mathcal{S}$ and $j,i = 1,2, i \neq j$,

$$\begin{aligned} H(\mathbf{X}_j|\mathbf{Z}_S) &= H(\mathbf{X}_{j,S}, \mathbf{X}_{j,S^c}|\mathbf{X}_{i,S}, \mathbf{X}_{j,S}, \mathbf{V}_{S^c}) \\ &= H(\mathbf{X}_{j,S^c}|\mathbf{V}_{S^c}) = (n-\mu)H(X_j|V) \\ H(\mathbf{X}_i|\mathbf{X}_j, \mathbf{Z}_S) &= H(\mathbf{X}_{i,S}, \mathbf{X}_{i,S^c}|\mathbf{X}_{j,S}, \mathbf{X}_{j,S^c}, \mathbf{X}_{i,S}, \mathbf{V}_{S^c}), \\ &= H(\mathbf{X}_{i,S^c}|\mathbf{X}_{j,S^c}, \mathbf{V}_{S^c}) = (n-\mu)H(X_i|X_j, V). \end{aligned}$$

For $\bar{\epsilon} > 0$, let $\gamma_j = (1-\bar{\epsilon})(n-\mu)H(X_j|V)$, $\gamma_{ij} = (1-\bar{\epsilon})(n-\mu)H(X_i|X_j, V)$. In order to compute $\mathbb{P}_{p_{\mathbf{X}_{1:2}\mathbf{Z}_S}}\big((\mathbf{X}_{1:2}, \mathbf{Z}_S) \notin \mathcal{D}_j^S\big)$, we only consider the tuples $(\mathbf{x}_{1:2}, \mathbf{z})$ s.t. $p_{\mathbf{X}_j|\mathbf{Z}_S}(\mathbf{x}_j|\mathbf{z}) > 0$, or $p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S}(\mathbf{x}_i|\mathbf{x}_j, \mathbf{z}) > 0$, since all the tuples $(\mathbf{x}_{1:2}, \mathbf{z})$ with $p_{\mathbf{X}_j|\mathbf{Z}_S}(\mathbf{x}_j|\mathbf{z}) = p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S}(\mathbf{x}_i|\mathbf{x}_j, \mathbf{z}) = 0$ belong to $\mathcal{D}_j^S$, for $\gamma_j, \gamma_{ij} < \infty$, by definition. For $p_{\mathbf{X}_j|\mathbf{Z}_S}$ and $p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S} > 0$, we have, $\forall S \in \mathcal{S}$, and $j,i = 1,2, i \neq j$, that

$$p_{\mathbf{X}_j|\mathbf{Z}_S} = p_{\mathbf{X}_j|\mathbf{X}_{j,S}\mathbf{X}_{i,S}\mathbf{V}_{S^c}} = p_{\mathbf{X}_{j,S^c}|\mathbf{V}_{S^c}} = \prod_{k\in S^c}p(x_{j,k}|v_k),$$

$$p_{\mathbf{X}_i|\mathbf{X}_j\mathbf{Z}_S} = p_{\mathbf{X}_{i,S^c}|\mathbf{X}_{j,S^c}\mathbf{V}_{S^c}} = \prod_{k\in S^c}p(x_{i,k}|x_{j,k}, v_k).$$

Once again, using Hoeffding inequality and the choice for γ_j, we have, for some $\beta_j > 0, j = 1,2$, and $\forall S \in \mathcal{S}$, that

$$\mathbb{P}\big((\mathbf{X}_j, \mathbf{Z}_S) \notin \mathcal{D}^S_{\gamma_j}\big) = \mathbb{P}_{p_{\mathbf{X}_j\mathbf{Z}_S}}\big(-\log p_{\mathbf{X}_j|\mathbf{Z}_S}(\mathbf{X}_j|\mathbf{Z}_S) \leq \gamma_j\big) = \mathbb{P}\Big(\sum_{k\in S^c}\log\frac{1}{p(X_{j,k}|V_k)} \leq (1-\bar{\epsilon})(n-\mu)H(X_j|V)\Big) \leq \exp(-\tilde{\beta}_jn). \quad (12)$$

Similarly, for $j, i = 1, 2, i \neq j$, $\exists \tilde{\beta}_{ij} > 0$ s.t. $\mathbb{P}\big((\mathbf{X}_{1:2}, \mathbf{Z}_S) \notin \mathcal{D}^S_{\gamma_{ij}}\big) \leq \exp(-\tilde{\beta}_{ij} n)$. Taking $\delta^2 = 2\exp(-\tilde{\beta} n)$, where $\tilde{\beta} = \min\{\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_{12}, \tilde{\beta}_{21}\} > 0$, gives $\mathbb{P}((\mathbf{X}_{1:2}, \mathbf{Z}_S) \notin \mathcal{D}^S_j) \leq \delta^2$, $\forall S \in \mathcal{S}$ and $j = 1, 2$. Since $\lim_{n\to\infty} \delta^2 = 0$, then, for n large enough, $\delta^2 \in]0, \frac{1}{4}[$. Thus, the conditions of Lemma 2 are satisfied. By substituting the choices for $\tilde{M}_j, \tilde{C}_j, \gamma_j, \gamma_{ij}$ and $|\mathcal{S}||\mathcal{Z}^n| \leq e^{n\left[\ln 2 + \ln(|\mathcal{X}_1| \times |\mathcal{X}_2| + |\mathcal{V}|)\right]}$ in (8), we have, $\forall \epsilon, \epsilon' > 0$, $\tilde{\epsilon} = \epsilon + \epsilon'$, $\exists n^* \in \mathbb{N}$ and $\kappa_\epsilon, \tilde{\kappa} > 0$ s.t. $\forall n \geq n^*$,

$$\mathbb{P}(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) \geq 2\tilde{\epsilon}) \leq e^{-\kappa_\epsilon e^{\tilde{\kappa} n}},$$
$$\text{if } R_j + \tilde{R}_j < (1-\bar{\epsilon})(1-\alpha)H(X_j|V), \ \ \forall j = 1, 2, \ \text{and,}$$
$$R_1 + R_2 + \tilde{R}_1 + \tilde{R}_2 < (1-\bar{\epsilon})(1-\alpha)H(X_{1:2}|V). \quad (13)$$

Remark 3 By setting $j = 1, i = 2$, instead of the minimum, in the RHS of (8), Lemma 2 results in the maximum rate $R_1 + \tilde{R}_1$, and the corresponding rate $R_2 + \tilde{R}_2$ (according to the maximum sum rate) such that the probability in the LHS of (8) is vanishing. By switching i and j, the Lemma gives the maximum rate $R_2 + \tilde{R}_2$, and the corresponding rate $R_1 + \tilde{R}_1$ according to the maximum sum rate. Using this, one can deduce the maximum rate region, i.e., the maximum individual and sum rates, required for a vanishing probability.

Let $D_n \triangleq \max_S \mathbb{D}(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S})$, $\mathcal{K}_n \triangleq \{D_n \geq r\}$, $r > 0$. From (13), $\sum_{n=1}^{\infty} \mathbb{P}(\mathcal{K}_n) < \infty$. By the Borel-Cantelli lemma, $\mathbb{P}\big(\mathcal{K}_n$ infinitely often (i.o.)$\big) = 0$. This implies that $\forall r > 0$, $\mathbb{P}\big(\{D_n < r\}$ i.o.$\big) = 1$. Thus, the sequence D_n converges to zero almost surely, and hence, converges to zero in probability as well. We conclude that,

$$\lim_{n\to\infty} \mathbb{P}\big(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) > 0\big) = 0. \quad (14)$$

Now, we show that protocol B is also reliable and secure with the rate conditions above. Equations (10), (11) imply that

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(P_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}},$$
$$P_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S} \mathbb{1}_{\{\hat{\mathbf{X}}_{1:2} = \mathbf{X}_{1:2}\}})\big) = 0. \quad (15)$$

By applying Markov inequality to (10), we have, $\forall r > 0$,

$$\sum_{n=1}^{\infty} \mathbb{P}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}} p^U_{C_{1:2}}) > r\big) \leq \frac{4}{r} \sum_{n=1}^{\infty} e^{-\beta n} < \infty.$$

By Borel-Cantelli lemma, $\lim_{n\to\infty} \mathbb{P}\big(\mathbb{V}(\tilde{P}_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}} p^U_{C_{1:2}}) > 0\big) = 0$. Thus, by using the union bound and (14), we have

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) > 0\big)$$
$$\leq \lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) > 0\big)$$
$$+ \lim_{n\to\infty} \mathbb{P}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}} p^U_{C_{1:2}}) > 0\big) = 0. \quad (16)$$

The selection lemma [13, Lemma 2.2] when applied to (15), (16), implies that there is at least one binning realization $\mathbf{b}^*$, with a corresponding joint distribution p^* for protocol B, s.t.,

$$\lim_{n\to\infty} \mathbb{V}\big(p^*_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}_{1:2}},$$
$$p^*_{M_{1:2}C_{1:2}\mathbf{X}_{1:2}\mathbf{Y}\mathbf{Z}_S} \mathbb{1}_{\{\hat{\mathbf{X}}_{1:2} = \mathbf{X}_{1:2}\}}\big) = 0, \text{ and} \quad (17)$$

$$\lim_{n\to\infty} \mathbb{1}_{\big\{\max_{S\in\mathcal{S}} \mathbb{D}(p^*_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) > 0\big\}} = 0, \quad (18)$$

with $M_j = b_1^{*(j)}(\mathbf{X}_j), C_j = b_2^{*(j)}(\mathbf{X}_j), j = 1, 2$. We introduce $p^*_{\hat{M}_{1:2}|\hat{\mathbf{X}}_{1:2}} = \mathbb{1}_{\{\hat{M}_j = b_1^{*(j)}(\hat{\mathbf{X}}_j), \forall j = 1,2\}}$ to (17). Then,

$$\mathbb{E}_{C_{1:2}}\big(\mathbb{P}(\hat{M}_{1:2} \neq M_{1:2}|C_{1:2})\big) = \mathbb{V}\big(p^*_{M_{1:2}\hat{M}_{1:2}C_{1:2}},$$
$$p^U_{M_{1:2}} p^U_{C_{1:2}} \mathbb{1}_{\{\hat{M}_{1:2} = M_{1:2}\}}\big) \underset{n\to\infty}{\longrightarrow} 0, \quad (19)$$

follows from (17). Using the union bound and (18), we have

$$\mathbb{P}_{C_{1:2}}\big(\max_S \mathbb{D}(p^*_{M_{1:2}\mathbf{Z}_S|C_{1:2}} || p^U_{M_{1:2}} p^*_{\mathbf{Z}_S|C_{1:2}}) > 0\big)$$
$$\leq \mathbb{1}_{\big\{\max_S \mathbb{D}(p^*_{M_{1:2}C_{1:2}\mathbf{Z}_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}) > 0\big\}}$$
$$+ \mathbb{P}\Big(\max_S \mathbb{D}(p^*_{M_{1:2}\mathbf{Z}_S|C_{1:2}} || p^U_{M_{1:2}} p^*_{\mathbf{Z}_S|C_{1:2}}) > 0, \text{ and}$$
$$\forall S, \ p^*_{M_{1:2}C_{1:2}\mathbf{Z}_S} = p^U_{M_{1:2}} p^U_{C_{1:2}} p_{\mathbf{Z}_S}\Big) \underset{n\to\infty}{\longrightarrow} 0, \quad (20)$$

as the second term in the RHS of (20) is equal to zero.

Applying the selection lemma to (19), (20), implies that there exists $c^*_{1:2}$ s.t. both $\mathbb{P}(\hat{M}_{1:2} \neq M_{1:2}|C_{1:2} = c^*_{1:2})$ and $\max_S I(M_{1:2}; \mathbf{Z}_S|C_{1:2} = c^*_{1:2})$ converge to 0 as $n \to \infty$. We use $\tilde{p}^*(\mathbf{x}_{1:2}|m_{1:2}, c^*_{1:2})$ and $(\tilde{p}^*(\hat{\mathbf{x}}_{1:2}|\mathbf{y}, c^*_{1:2}), b_1^{*(j)}(\hat{\mathbf{x}}_j), j = 1, 2)$ as the encoder and decoder for the original model; $\tilde{p}^*$ is the induced distribution in protocol A, corresponding to $\mathbf{b}^*$.

So far, we have considered the case $U_{1:2} = X_{1:2}$. Now, we prefix two independent channels, $p_{X_1|U_1}$, $p_{X_2|U_2}$, at the transmitters of the original model and repeat the same steps in the proof above. In particular, the main channel in the new model is $p_{Y|U_1U_2}$ and the wiretapper channel is described by $p_{X_1|U_1}p_{X_2|U_2}$ and (2). The rate conditions required for the success of the Slepian-Wolf decoder in protocol A are $\tilde{R}_1 \geq H(U_1|U_2, Y)$, $\tilde{R}_2 \geq H(U_2|U_1, Y)$, $\tilde{R}_1 + \tilde{R}_2 \geq H(U_{1:2}|Y)$. Taking $\bar{\epsilon} \to 0$, the rate conditions required for secrecy of protocol A, resulting from Lemma 2, are, for $j = 1, 2$,

$$R_j + \tilde{R}_j \leq \alpha H(U_j|X_j) + (1-\alpha)H(U_j|V), \text{ and}$$
$$R_1 + R_2 + \tilde{R}_1 + \tilde{R}_2 \leq \alpha H(U_{1:2}|X_{1:2}) + (1-\alpha)H(U_{1:2}|V).$$

Combining these conditions establish the achievability of the union of the region in (3). The convex hull of the union follows by time sharing independent codes and the fact that maximizing the secrecy constraint over S in the whole block-length is upper bounded by its maximization over the individual segments of the time sharing.

V. Conclusion

In this paper, we have extended the recently proposed new WTC model [5] to the two-user multiple-access channel, where the main channel is a DMC and the wiretapper selects a subset of the channel uses to perfectly access the transmitted symbols of the both users, while observing the remainder of the transmitted codewords through a second DMC. We have derived an achievable strong secrecy rate region for the proposed model. This result quantifies the secrecy penalty of this additional capability at the wiretapper. Future work includes upper bounds for the model and other multi-terminal settings with more capable wiretappers.

Appendix A
Proof of Lemma 1

Using the triangle inequality, we obtain

$$\mathbb{V}(P_{M_{1:2}C_{1:2}}, p^U_{M_{1:2}} p^U_{C_{1:2}}) \leq \mathbb{V}(P_{M_{1:2}C_{1:2}}, p^U_{M_1} p^U_{C_1} P_{M_2C_2}) + \mathbb{V}(p^U_{M_1} p^U_{C_1} P_{M_2C_2}, p^U_{M_{1:2}} p^U_{C_{1:2}}) = \sum_{j=1,2} \mathbb{V}(P_{M_jC_j}, p^U_{M_j} p^U_{C_j}).$$

Using [5, Appendix. A], we have, for $j = 1, 2$,

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(P_{M_jC_j}, p^U_{M_j} p^U_{C_j})\big) \leq \mathbb{P}(X_j \notin \mathcal{D}_{\gamma_j}) + \frac{1}{2}\sqrt{\tilde{M}_j \tilde{C}_j 2^{-\gamma_j}}.$$

Appendix B
Proof of Lemma 2

For all $S \in \mathcal{S}$, $\mathbb{D}(P_{M_{1:2}C_{1:2}Z_S} || p^U_{M_{1:2}} p^U_{C_{1:2}} p_{Z_S})$ is equal to

$$E_{p_{Z_S}}\left(\mathbb{D}(P_{M_{1:2}C_{1:2}|Z_S} || P_{M_1C_1|Z_S} p^U_{M_2} p^U_{C_2})\right) + \mathbb{D}(p_{M_1C_1Z_S} || p^U_{M_1} p^U_{C_1} p_{Z_S}). \quad (21)$$

Thus, the probability in the LHS of (8) is upper bounded by

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}} \mathbb{E}_{p_{Z_S}}\left(\mathbb{D}(P_{M_{1:2}C_{1:2}|Z_S} || P_{M_1C_1|Z_S} p^U_{M_2} p^U_{C_2})\right) > \tilde{\epsilon}\Big) + \mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}} \mathbb{D}(P_{M_1C_1Z_S} || p^U_{M_1} p^U_{C_1} p_{Z_S}) > \tilde{\epsilon}\big). \quad (22)$$

We upper bound each term in (22). For all $S \in \mathcal{S}$, define

$$\mathcal{A}_S \triangleq \big\{z \in \mathcal{Z} : \mathbb{P}_{p_{X_{1:2}|Z_S}}\big((X_{1:2}, z) \in \mathcal{D}^S_1\big) \geq 1 - \delta\big\}.$$

Using Markov inequality, we have, for all $S \in \mathcal{S}$,

$$\mathbb{P}_{p_{Z_S}}(\mathcal{A}^c_S) \leq \frac{1}{\delta} \mathbb{P}_{p_{X_{1:2}Z_S}}\big((X_{1:2}, Z_S) \notin \mathcal{D}^S_1\big) \leq \delta. \quad (23)$$

Let $\mathbb{1}_{\{x,m,c,\mathcal{J}\}} \triangleq \mathbb{1}_{\{\mathcal{B}^{(j)}_1(x_j)=m_j, \mathcal{B}^{(j)}_2(x_j)=c_j, \forall j\in\mathcal{J}\}}$, where $\mathcal{J} \subseteq \{1, 2\}$. For any $m_{1:2}, c_{1:2}$, $z \in \mathcal{Z}$, $S \in \mathcal{S}$, define

$$P^S_1(m_{1:2}, c_{1:2}|z) = \sum_{x_{1:2}} p(x_{1:2}|z) \mathbb{1}_{\{x,m,c,\{1,2\}\}} \mathbb{1}_{\{(x_{1:2},z)\in\mathcal{D}^S_1\}}$$

$$P^S_2(m_{1:2}, c_{1:2}|z) = \sum_{x_{1:2}} p(x_{1:2}|z) \mathbb{1}_{\{x,m,c,\{1,2\}\}} \mathbb{1}_{\{(x_{1:2},z)\notin\mathcal{D}^S_1\}},$$

hence $P_{M_{1:2}C_{1:2}|Z_S} = P^S_1 + P^S_2$. For every $x_2 \in \mathcal{X}_2$, define

$$U_{x_2} = \sum_{x_1\in\mathcal{X}_1} p(x_{1:2}|z) \mathbb{1}_{\{x,m,c,\{2\}\}} \mathbb{1}_{\{(x_{1:2},z)\in\mathcal{D}^S_1\}}.$$

$\{U_{x_2}\}_{x_2\in\mathcal{X}_2}$ are independent. For $(x_{1:2}, z) \in \mathcal{D}^S_1$, we have $(x_{1:2}, z) \in \mathcal{D}^S_{\gamma_{21}}$ and $p(x_2|x_1, z) \leq 2^{-\gamma_{21}}$. Thus,

$$U_{x_2} \leq \sum_{x_1} p(x_1|z) p(x_2|x_1, z) \mathbb{1}_{\{(x_{1:2},z)\in\mathcal{D}^S_{\gamma_{21}}\}} \leq 2^{-\gamma_{21}}, \text{ and}$$

$$\bar{m} = \sum_{x_2} \mathbb{E}_{\mathcal{B}}(U_{x_2}) = \frac{1}{\tilde{M}_2\tilde{C}_2} \mathbb{P}_{p_{X_{1:2}|Z_S}}((X_{1:2}, z) \in \mathcal{D}^S_1).$$

Also, notice that $\sum_{m_1c_1} P^S_1(m_{1:2}, c_{1:2}|z) = \sum_{x_2} U_{x_2}$ since $\sum_{m_1c_1} \mathbb{1}_{\{x,m,c,\{1\}\}} = 1$. Using a variation of Chernoff bound [5, Lemma 3], we have, for all $\epsilon \in [0, 1]$ and $z \in \mathcal{A}_S$, that

$$\mathbb{P}_{\mathcal{B}}\Big(P^S_1(m_{1:2}, c_{1:2}|z) \geq \frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2} P_{M_1C_1|Z_S}(m_1, c_1|z)\Big) \leq \mathbb{P}\Big(\sum_{x_2} U_{x_2} \geq \frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2} \sum_{m_1,c_1} P_{M_1C_1|Z_S}(m_1, c_1|z)\Big) \leq \mathbb{P}\Big(\sum_{x_2} U_{x_2} \geq (1+\epsilon)\bar{m}\Big) \leq \exp\Big(\frac{-\epsilon^2(1-\delta)2^{\gamma_{21}}}{3\tilde{M}_2\tilde{C}_2}\Big), \quad (24)$$

where $\bar{m} \geq (1-\delta)(\tilde{M}_2\tilde{C}_2)^{-1}, \forall z \in \mathcal{A}_S$.

Let $\mathbf{b}$ be a realization of $\mathcal{B}$. Note that P^S_1 is identically distributed for all $m_{1:2}, c_{1:2}$ due to the symmetry in the binning. We then define the class $\mathcal{G}$ of binning functions as

$$\mathcal{G} \triangleq \Big\{\mathbf{b} : P^S_1(m_{1:2}, c_{1:2}|z) < \frac{1+\epsilon}{\tilde{M}_2\tilde{C}_2} P_{M_1C_1|Z_S}(m_1, c_1|z), \forall S \in \mathcal{S}, \text{ and } \forall z \in \mathcal{A}_S\Big\}. \quad (25)$$

Using the union bound and (24), we have

$$\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c) \leq |\mathcal{S}||\mathcal{Z}| \exp\Big(\frac{-\epsilon^2(1-\delta)2^{\gamma_{21}}}{3\tilde{M}_2\tilde{C}_2}\Big). \quad (26)$$

Using the same analysis as in [5, Appendix. B], we show that, $\forall S \in \mathcal{S}$ and $\mathbf{b} \in \mathcal{G}$,

$$\mathbb{E}_{p_{Z_S}}\left(\mathbb{D}(P_{M_{1:2}C_{1:2}|Z_S} || P_{M_1C_1|Z_S} p^U_{M_2} p^U_{C_2})\right) \leq \epsilon + (\delta + \delta^2)\log(\tilde{M}_2\tilde{C}_2) + H_b(\delta^2) \leq \tilde{\epsilon}.$$

Thus, the first probability in (22) is upper bounded by $\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c)$ in (26). Using similar arguments, we show that the second probability in (22) is upper bounded by $|\mathcal{S}||\mathcal{Z}|e^{(\frac{-\epsilon^2(1-\delta)2^{\gamma_1}}{3\tilde{M}_1\tilde{C}_1})}$. Finally, by rewriting (21) with switching the roles of (M_1, C_1) and (M_2, C_2) and repeating the proof, we obtain the second term in the minimum in (8), which completes the proof.

References

[1] L. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Sys. Tech. Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[2] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," *Int. Symp. Info. Theory*, pp. 1159–1163, June 2015.

[3] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Info. Theory*, vol. 62, no. 7, pp. 3863–3879, 2016.

[4] M. Nafea and A. Yener, "The multiple access wiretap channel II with a noisy main channel," *Int. Symp. Info. Theory*, July 2016.

[5] ——, "A new wiretap channel model and its strong secrecy capacity," *Int. Symp. Info. Theory*, July 2016.

[6] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[8] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–Part I: Secret sharing," *IEEE Trans. Info. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[9] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Info. Theory*, vol. 60, no. 11, pp. 6760–6786, 2014.

[10] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," *IEEE Info. Theory Workshop*, November 2010.

[11] O. Simeone and A. Yener, "The cognitive multiple access wire-tap channel," *IEEE Conf. Info. Sci. and Sys.*, March 2009.

[12] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge university press, 2011.

[13] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University Press, 2011.