A New Wiretap Channel Model and its Strong Secrecy Capacity

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*—In this paper, a new wiretap channel (WTC) model with a discrete memoryless (DM) main channel and a wiretapper who noiselessly observes a fixed portion, of her choice, of the transmitted symbols, while observing the remaining transmitted symbols through another DM channel (DMC), is considered. The strong secrecy capacity of the model is identified. The achievability is established using the output statistics of random binning framework which exploits the duality between source and channel coding problems. The converse is derived by upper bounding the secrecy capacity of an equivalent model with the secrecy capacity of a DM-WTC. This result generalizes both the classical DM-WTC and the WTC-II with a DM main channel.**

I. Introduction

Wyner introduced the wiretap channel (WTC) which models point-to-point communication in the presence of a passive wiretapper who *only listens* to the transmitted signal through a cascaded discrete memoryless channel (DMC) [1]. Later, Ozarow and Wyner introduced the WTC-II, which considered a special instance of a WTC with a noiseless main channel and a binary erasure channel (EC) to the wiretapper, but assumed the wiretapper was able to select the positions of erasures [2]. Using random partitioning and combinatorial arguments, the authors showed that the secrecy capacity did not deteriorate despite this capability of the wiretapper.

While considerable research on practical coding design for WTCs followed the coset coding scheme proposed in [2], see for example [3], the idea of the WTC-II remained linked with the assumption of a noiseless main channel for thirty years. Recently, reference [4] introduced a discrete memoryless (DM) main channel to the WTC-II with the objective of addressing a more general model of a wiretapper who is smarter than a passive observer. Reference [4] provided an outer bound and derived an achievability scheme that is optimal for the special case of the maximizing input distribution being uniform. More recently, reference [5] provided a tight converse, and established a stronger version of Wyner's soft covering lemma which enabled the achievability proof for the model, showing that, once again, its secrecy capacity is equal to the secrecy capacity when the wiretapper channel is a DM-EC.

This work goes one step further and introduces a new WTC model with a DM main channel and a wiretapper who observes a subset of transmitted codeword symbols of her choosing perfectly, while observing the remaining symbols through a DMC. This general model includes as special cases both the classical DM-WTC by setting the subset size to zero and the WTC-II with a noisy main channel [4] by setting the wiretapper DMC to an EC with erasure probability one.

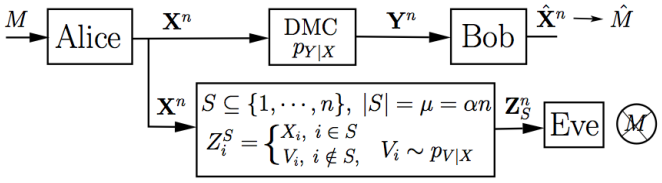


Fig. 1. A new wiretap channel model.

The achievability is established by solving a dual secret key agreement problem in the source model [6], and infering the optimal encoder and decoder design for the original problem from the solution of the dual problem [7]. The advantage of the conversion to a dual source coding problem is that it renders the analysis of the scenario at hand simpler and tractable. The converse is derived by using Sanov's theorem [8] to upper bound the secrecy capacity of the model by the secrecy capacity when the subset is randomly chosen by nature.

Notation: For $a, b \in \mathbb{R}$, $[\![a, b]\!]$ denotes $\{i \in \mathbb{N} : a \leq i \leq b\}$. For $S \subseteq \mathbb{N}$, $\mathbf{X}_S = \{X_i\}_{i \in S}$. p_X^U denotes a uniform distribution over X. $\mathbb{V}(p_X, q_X)$, $\mathbb{D}(p_X || q_X)$ denote the variational distance and the K-L divergence between the distributions p_X, q_X.

II. Channel Model

We consider the model in Fig. 1. The transmitter (Alice) aims to reliably transmit a message M, uniformly distributed over $[\![1, 2^{nR_s}]\!]$, to the receiver (Bob) and to keep it secret from the wiretapper (Eve). The message M is mapped to the transmitted codeword $\mathbf{X}^n \in \mathcal{X}^n$; the mapping is allowed to be stochastic. Alice-Bob channel is a DMC with a finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$, and transition probability $p_{Y|X}$. Bob observes $\mathbf{Y}^n \in \mathcal{Y}^n$ and outputs the estimate $\hat{M}$ of M. Eve chooses $S \subseteq [\![1, n]\!]$ with $|S| = \mu \leq n$, $\alpha = \frac{\mu}{n}$, and observes $\mathbf{Z}_S^n = [Z_1^S \ \cdots \ Z_n^S] \in \mathcal{Z}^n$, where

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

$V_i \in \mathcal{V}$ is the ith output of the DMC $p_{V|X}$, $\mathcal{Z}^n = \{\mathcal{X} \cup \mathcal{V}\}^n$.

978-1-5090-1805-5/16/$31.00 ©2016 IEEE

An $(n, 2^{nR_s})$ channel code $\mathcal{C}_n$ for this model consists of i) the message set $\mathcal{M} = [\![1, 2^{nR_s}]\!]$, ii) the stochastic encoder $P_{\mathbf{X}^n|M,\mathcal{C}_n}$ at Alice, and iii) the decoder at Bob. We consider the strong secrecy constraint at Eve, see (2). The rate R_s is an achievable strong secrecy rate if there exists a sequence of $(n, 2^{nR_s})$ channel codes, $\{\mathcal{C}_n\}_{n\geq 1}$, such that

$$\lim_{n\to\infty} \mathbb{P}(\hat{M} \neq M|\mathcal{C}_n) = 0, \text{ and } \lim_{n\to\infty} \max_{S\in\mathcal{S}} I(M; \mathbf{Z}_S^n|\mathcal{C}_n) = 0, \tag{2}$$

$\mathcal{S} = \{S : S \subseteq [\![1, n]\!], |S| = \mu\}$. The strong secrecy capacity, C_s, is the supremum of all achievable strong secrecy rates.

III. Main Result

Theorem 1 *For $\alpha \in [0, 1]$, the strong secrecy capacity of the new wiretap channel model in Fig. 1 is given by*

$$\mathsf{C}_s^{\alpha} = \max_{U-X-YV} [I(U;Y) - I(U;V) - \alpha I(U;X|V)]^+, \tag{3}$$

where the maximization is over all p_{UX} which satisfy $U - X - YV$, and the cardinality of U is bounded as $|\mathcal{U}| \leq |\mathcal{X}|$.

Proof: The achievability and converse proofs for Theorem 1 are provided in Sections IV and V, respectively. ■

Remark 1 The secrecy capacity in (3) can be rewritten as $\mathsf{C}_s^{\alpha} = \max_{U-X-YV} [I(U;Y) - \alpha I(U;X) - (1-\alpha) I(U;V)]^+$.

Remark 2 When $|S| = 0$, i.e., $\alpha = 0$, (3) is equal to the secrecy capacity of the DM-WTC. Also, when V is an erasure with probability one, (3) is equal to the secrecy capacity of the WTC-II with a noisy main channel [5]. The secrecy cost of the additional capability at the wiretapper in the new model with respect to the DM-WTC (WTC-II with a DM main channel [4]) is equal to $\alpha I(U;X|V)$ ($(1-\alpha)I(U;V)$).

IV. Achievability

We first consider $U = X$. We fix p_X and define two protocols, each of which introduces a set of random variables and induces a joint distribution over them.

Protocol A (Secret key agreement in a source model): The protocol is illustrated in Fig. 2. $\mathbf{X}^n, \mathbf{Y}^n$ are independent and identically distributed (i.i.d.) according to $p_{XY} = p_X p_{Y|X}$, where $p_{Y|X}$ is the transition probability of the main channel in Fig. 1. The source encoder observes the sequence $\mathbf{X}^n$ and randomly assigns (bins) it into the two bin indices $M = \mathcal{B}_1(\mathbf{X}^n)$, $C = \mathcal{B}_2(\mathbf{X}^n)$, where $\mathcal{B}_1, \mathcal{B}_2$ are uniformly distributed over $[\![1, 2^{nR_s}]\!]$, $[\![1, 2^{n\tilde{R}_s}]\!]$, respectively. That is, each $\mathbf{x} \in \mathcal{X}^n$ is randomly and independently assigned to the indices $m \in [\![1, 2^{nR_s}]\!]$ and $c \in [\![1, 2^{n\tilde{R}_s}]\!]$. The bin index C represents the public message which is transmitted over a noiseless channel to the decoder and perfectly accessed by the wiretapper. The bin index M represents the secret key to be generated at the source encoder and decoder. The source decoder observes C and the i.i.d. sequence $\mathbf{Y}^n$, and outputs the estimate $\hat{\mathbf{X}}^n$ of $\mathbf{X}^n$, which in turn generates the estimate $\hat{M}$ of M. For any $S \in \mathcal{S}$, where $\mathcal{S}$ is defined as in (2), the wiretapper source node observes C and the sequence $\mathbf{Z}_S^n$ in (1). The

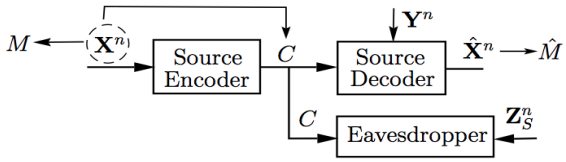


Fig. 2. Protocol A: Secret key agreement in the source model.

subset S is selected by the wiretapper and her selection is unknown to the legitimate parties. Thus, the wiretapper can be represented as a compound source $\mathbf{Z}_S^n \triangleq \{\mathcal{Z}, p_{\mathbf{Z}_S^n}\}$ whose distribution is only known to belong to the finite class $\{p_{\mathbf{Z}_S^n}\}_{S\in\mathcal{S}}$ with no prior distribution over the class, where $|\mathcal{S}| \leq 2^n$. For $S \in \mathcal{S}$, the induced joint distribution for this protocol, $\tilde{P}_{MC\mathbf{X}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}}$, is equal to

$$\begin{aligned} &p_{\mathbf{X}\mathbf{Y}\mathbf{Z}_S} \mathbb{1}\{\mathcal{B}_1(\mathbf{X}) = M\} \mathbb{1}\{\mathcal{B}_2(\mathbf{X}) = C\} \tilde{P}_{\hat{\mathbf{X}}|\mathbf{Y}C} \\ &= \tilde{P}_{MC} \tilde{P}_{\mathbf{X}|MC}\, p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}} \tilde{P}_{\hat{\mathbf{X}}|\mathbf{Y}C}. \end{aligned} \tag{4}$$

Protocol B (Main problem assisted with common randomness): This protocol is defined as the channel model in Fig. 1, with an addition of a common randomness C that is uniform over $[\![1, 2^{n\tilde{R}_s}]\!]$, independent from all other variables, and known at all terminals. The encoder and decoder are defined as in (4); $P_{\mathbf{X}|MC} = \tilde{P}_{\mathbf{X}|MC}$, $P_{\hat{\mathbf{X}}|\mathbf{Y}C} = \tilde{P}_{\hat{\mathbf{X}}|\mathbf{Y}C}$. The induced joint distribution for this protocol is

$$P_{MC\mathbf{X}\mathbf{Y}\mathbf{Z}_S\hat{\mathbf{X}}} = p_M^U p_C^U \tilde{P}_{\mathbf{X}|MC}\, p_{\mathbf{Y}\mathbf{Z}_S|\mathbf{X}} \tilde{P}_{\hat{\mathbf{X}}|\mathbf{Y}C}. \tag{5}$$

The induced joint distributions in (4) and (5) are random due to the random binning of $\mathbf{X}^n$. Note that we have ignored the $\hat{M}$ from the induced distributions at this stage. We will introduce them later to the distributions as deterministic functions of the random variables $\hat{\mathbf{X}}^n$, after fixing the binning functions. The remaining steps are: (i) we derive a condition on $R_s, \tilde{R}_s$ so that the two induced distributions, in (4), (5), are close in the variational distance sense, when averaged over the random binning, (ii) we derive other conditions on $R_s, \tilde{R}_s$ such that protocol A is reliable and secure, (iii) we use the closeness of the two distributions to show that protocol B is reliable and secure as well, and finally (iv) we eliminate the common randomness C from protocol B by showing that the reliability and secrecy constraints still hold when we condition on a certain instance of C, i.e., $C = c^*$.

Before continuing with the proof, we state the following two lemmas. Using these, we derive the conditions on $R_s, \tilde{R}_s$ required for the closeness of the two induced distributions, and security of protocol A. A result similar to Lemma 1 below was derived in [7, Appendix A]. However, the convergence rate Lemma 1 provides is needed in our proof.

Lemma 1 *Let the source $X \triangleq \{\mathcal{X}, p_X\}$ be randomly binned into $M = \mathcal{B}_1(X)$, $C = \mathcal{B}_2(X)$, where $\mathcal{B}_1, \mathcal{B}_2$ are uniform over $[\![1, \tilde{M}]\!]$, $[\![1, \tilde{C}]\!]$. Let $\mathcal{B} \triangleq \{\mathcal{B}_1(x), \mathcal{B}_2(x)\}_{x\in\mathcal{X}}$, and for $\gamma > 0$, define $\mathcal{D}_\gamma \triangleq \left\{x \in \mathcal{X} : \log \frac{1}{p_X(x)} > \gamma\right\}$. Then, we have*

$$\mathbb{E}_{\mathcal{B}} \left(\mathbb{V}(P_{MC}, p_M^U p_C^U)\right) \leq \mathbb{P}(X \notin \mathcal{D}_\gamma) + \frac{1}{2}\sqrt{\tilde{M}\tilde{C}2^{-\gamma}}, \tag{6}$$

where P is the induced distribution over M, C.

Proof: See Appendix A. ■

Lemma 2 below provides a *doubly-exponential* decay rate for the probability of failure of achieving secrecy for protocol A, which is needed, along with the union bound, to guarantee secrecy for the exponentially many choices of the subset S.

Lemma 2 *Let $X \triangleq \{\mathcal{X}, p_X\}$ and $\{Z_S\} \triangleq \{\mathcal{Z}, p_{Z_S}\}$ be two correlated sources, where $\{Z_S\}_{S\in\mathcal{S}}$ is a compound source and $|\mathcal{X}|, |\mathcal{Z}|, |\mathcal{S}| < \infty$. Let X be randomly binned into the bin indices M, C, as in Lemma 1. For $\gamma > 0$ and any $S \in \mathcal{S}$, define $\mathcal{D}_\gamma^S \triangleq \Big\{(x,z) \in \mathcal{X}\times\mathcal{Z} : \log \frac{1}{p_{X|Z_S}(x|z)} > \gamma\Big\}$. If there exists $\delta \in]0, \frac{1}{2}[$ such that for all S, $\mathbb{P}_{p_{XZ_S}}\big((X, Z_S) \in \mathcal{D}_\gamma^S\big) \geq 1-\delta^2$, then, we have, for every $\epsilon_1 \in [0,1]$, that*

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}} \mathbb{D}(P_{MCZ_S}||p_M^U p_C^U p_{Z_S}) \geq \tilde{\epsilon}\Big) \leq |\mathcal{S}||\mathcal{Z}|e^{\left(\frac{-\epsilon_1^2(1-\delta)2^\gamma}{3\tilde{M}\tilde{C}}\right)}, \tag{7}$$

where $\tilde{\epsilon} = \epsilon_1 + (\delta+\delta^2)\log(\tilde{M}\tilde{C}) + H_b(\delta^2)$, H_b is the binary entropy function, and P is the induced distribution.

Proof: The proof is given in Appendix B, the analysis therein is adapted from [9, Appendix]. ■

Apply Lemma 1 to protocol A, with $X = \mathbf{X}$, $\tilde{M} = 2^{nR_s}$, $\tilde{C} = 2^{n\tilde{R}_s}$, $\gamma = n(1-\epsilon_2)H(X)$. Without loss of generality, let $p(x) > 0,\ \forall x \in \mathcal{X}$. Let $p_{\min} = \min_x p(x)$. The random variables $\log\frac{1}{p(X_i)}, i \in [\![1,n]\!]$, are i.i.d. and each is bounded by the interval $[0, \log\frac{1}{p_{\min}}]$. Using Hoeffding inequality [10],

$$\mathbb{P}(\mathbf{X} \notin \mathcal{D}_\gamma) = \mathbb{P}\Big(\sum_{i=1}^n \log\frac{1}{p(X_i)} \leq (1-\epsilon_2)nH(X)\Big) \leq e^{-\beta_1 n},$$

where $\beta_1 > 0$. Using (6), there exists $\beta > 0$ such that

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{MC}, p_M^U p_C^U)\big) \leq 2\exp(-\beta n), \tag{8}$$

as long as $R_s + \tilde{R}_s < (1-\epsilon_2)H(X)$. From (4), (5), (8),

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}}, P_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}})\big) \leq 2\exp(-\beta n). \tag{9}$$

For protocol A, we use Slepian-Wolf decoder. By [11, Theorem 10.1] we have $\lim_{n\to\infty}\mathbb{E}_{\mathcal{B}}\big(\mathbb{P}_{\tilde{P}}(\hat{\mathbf{X}} \neq \mathbf{X})\big) = 0$ as long as $\tilde{R}_s \geq H(X|Y)$. Thus, we have [7, Lemma 1],

$$\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(\tilde{P}_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}}, \tilde{P}_{MC\mathbf{XYZ}_S}\mathbb{1}\{\hat{\mathbf{X}} = \mathbf{X}\})\big) \underset{n\to\infty}{\longrightarrow} 0. \tag{10}$$

Now, apply Lemma 2 to protocol A, with $X = \mathbf{X}$, $\tilde{M} = 2^{nR_s}$, $\tilde{C} = 2^{n\tilde{R}_s}$, $Z_S = \mathbf{Z}_S, \forall S \in \mathcal{S}$, and $\gamma = n(1-\tilde{\epsilon}_2)(1-\alpha)H(X|V)$. Let $\mathbf{V}^n$ be the n-letter output of the DMC $p_{V|X}$. Since $\mathbf{X}$ is i.i.d., we have, for $p_{\mathbf{X}|\mathbf{Z}_S}(\mathbf{x}|\mathbf{z}) > 0$, that

$$p_{\mathbf{X}|\mathbf{Z}_S} = p_{\mathbf{X}_S\mathbf{X}_{S^c}|\mathbf{X}_S\mathbf{V}_{S^c}} = p_{\mathbf{X}_{S^c}|\mathbf{V}_{S^c}} = \prod_{i\in S^c} p(x_i|v_i). \tag{11}$$

Once again, using Hoeffding inequality, we have, for any S,

$$\mathbb{P}\big((\mathbf{X}, \mathbf{Z}_S) \notin \mathcal{D}_\gamma^S\big) = \mathbb{P}\Big(\sum_{i\in S^c}\log\frac{1}{p(X_i|V_i)} \leq (1-\tilde{\epsilon}_2)(n-\mu)H(X|V)\Big) \leq e^{-\beta_2(1-\alpha)n} = \delta^2, \tag{12}$$

where $\beta_2 > 0$. Thus, $\delta^2 \to 0$ as $n \to \infty$, and for sufficiently large n, $\delta^2 \in]0, \frac{1}{4}[$. Since $|\mathcal{S}||\mathcal{Z}^n| \leq e^{n[\ln 2 + \ln(|\mathcal{X}|+|\mathcal{V}|)]}$, and $\lim_{n\to\infty}\tilde{\epsilon} = \epsilon_1$, then, using (7), we have $\forall \epsilon_1, \epsilon_1' > 0$, $\tilde{\epsilon} = \epsilon_1 + \epsilon_1'$, there exist $n^* \in \mathbb{N}$, $\phi(\epsilon_1), \kappa > 0$ so that, for $n \geq n^*$,

$$\mathbb{P}_{\mathcal{B}}\Big(\max_{S\in\mathcal{S}} \mathbb{D}(\tilde{P}_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S}) \geq \tilde{\epsilon}\Big) \leq e^{-\phi(\epsilon_1)e^{\kappa n}}, \tag{13}$$

as long as $R_s + \tilde{R}_s < (1-\tilde{\epsilon}_2)(1-\alpha)H(X|V)$.

Take $r > 0$ and let $D_n = \max_S \mathbb{D}(\tilde{P}_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S})$ and $\mathcal{K}_n \triangleq \{D_n \geq r\}$. Using (13), $\sum_{n=1}^\infty \mathbb{P}(\mathcal{K}_n) < \infty$. Thus, using the first Borel-Cantelli lemma, $\mathbb{P}(\mathcal{K}_n$ infinitely often (i.o.)$) = 0$, which implies that, $\forall r > 0$, $\mathbb{P}\big(\{D_n < r\}$ i.o.$\big) = 1$, i.e., $D_n \to 0$ almost surely. Thus, for $R_s + \tilde{R}_s$ as above, we have

$$\lim_{n\to\infty}\mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}}\mathbb{D}(\tilde{P}_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S}) > 0\big) = 0. \tag{14}$$

Next, we deduce that protocol B is also reliable and secure when the aforementioned rate conditions are satisfied. Using (9), (10), and the triangle inequality, we have

$$\mathbb{E}_{\mathcal{B}}(\mathbb{V}(P_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}}, P_{MC\mathbf{XYZ}_S}\mathbb{1}\{\hat{\mathbf{X}} = \mathbf{X}\})) \underset{n\to\infty}{\longrightarrow} 0. \tag{15}$$

We also have, using the union bound and (14), that

$$\mathbb{P}_{\mathcal{B}}\big(\max_{S\in\mathcal{S}}\mathbb{D}(P_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S}) > 0\big) \leq \mathbb{P}\big(\mathbb{V}(\tilde{P}_{MC}, p_M^U p_C^U) > 0\big) + \mathbb{P}\big(\max_{S\in\mathcal{S}}\mathbb{D}(\tilde{P}_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S}) > 0\big) \underset{n\to\infty}{\longrightarrow} 0, \tag{16}$$

where, using the exponential decay in (8), Markov inequality, and the first Borel-Cantelli lemma, we can show that $\lim_{n\to\infty}\mathbb{P}(\mathbb{V}(\tilde{P}_{MC}, p_M^U p_C^U) > 0) = 0$.

By applying the selection lemma [12, Lemma 2.2] to (15) and (16), there exists at least one binning realization $\mathbf{b}^*$ (with a corresponding joint distribution p^* for protocol B) such that

$$\lim_{n\to\infty}\mathbb{V}(p^*_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}}, p^*_{MC\mathbf{XYZ}_S}\mathbb{1}\{\hat{\mathbf{X}} = \mathbf{X}\}) = 0 \tag{17}$$

$$\lim_{n\to\infty}\mathbb{1}\big\{\max_{S\in\mathcal{S}}\mathbb{D}(p^*_{MC\mathbf{Z}_S}||p_M^U p_C^U p_{\mathbf{Z}_S}) > 0\big\} = 0, \tag{18}$$

where $M = b_1^*(\mathbf{X})$, and $C = b_2^*(\mathbf{X})$. By introducing $p^*_{\hat{M}|\hat{\mathbf{X}}} = \mathbb{1}\{\hat{M} = b_1^*(\hat{\mathbf{X}})\}$ to (17), we have

$$\mathbb{E}_C(\mathbb{P}(\hat{M} \neq M|C)) = \mathbb{V}\big(p^*_{M\hat{M}C}, p_M^U p_C^U \mathbb{1}\{\hat{M} = M\}\big) = \mathbb{V}\big(p^*_{MC\mathbf{XYZ}_S\hat{\mathbf{X}}\hat{M}}, p^*_{MC\mathbf{XYZ}_S}\mathbb{1}\{\hat{M} = M\}\big) \underset{n\to\infty}{\longrightarrow} 0. \tag{19}$$

Using (18) and the union bound, we have that

$$\mathbb{P}_C(\max_S \mathbb{D}(p^*_{M\mathbf{Z}_S|C}||p_M^U p^*_{\mathbf{Z}_S|C}) > 0) \leq \mathbb{P}\Big(\max_S \mathbb{D}\big(p^*_{M\mathbf{Z}_S|C} ||p_M^U p^*_{\mathbf{Z}_S|C}\big) > 0, \text{ and } \forall S,\ p^*_{MC\mathbf{Z}_S} = p_M^U p_C^U p_{\mathbf{Z}_S}\Big) + \mathbb{1}\Big\{\max_S \mathbb{D}(p^*_{MC\mathbf{Z}_S^n}||p_M^U p_C^U p_{\mathbf{Z}_S}) > 0\Big\} \underset{n\to\infty}{\longrightarrow} 0, \tag{20}$$

where the first term in the RHS of (20) is equal to zero.

Finally, in order to eliminate C from the channel model in protocol B, we apply the selection lemma to (19), (20), which implies that there is at least one c^* such that both $\mathbb{P}(\hat{M} \neq M|C = c^*)$ and $\max_S I(M; \mathbf{Z}_S|C = c^*)$ converge to zero as $n \to \infty$. Let $\tilde{p}^*$ be the induced distribution for protocol A corresponding to $\mathbf{b}^*$. We use $\tilde{p}^*_{\mathbf{X}|M,C=c^*}$ as the encoder and $(\tilde{p}^*_{\hat{\mathbf{X}}|\mathbf{Y},C=c^*}, b_1^*(\hat{\mathbf{X}}))$ as the decoder for the original model. By combining the rate conditions $R_s + \tilde{R}_s < (1-\tilde{\epsilon}_2)(1-$

$\alpha)H(X|V)$, $\tilde{R}_s \geq H(X|Y)$, and taking $\tilde{\epsilon}_2 \to 0$, the rate $R_s = \max_{p_X}[I(X;Y) - I(X;V) - \alpha H(X|V)]$ is achievable.

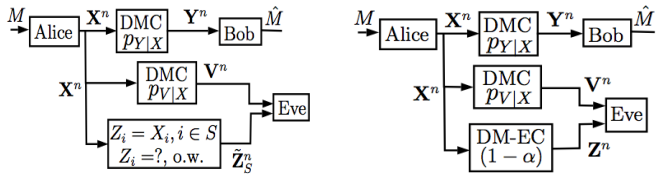
So far, we have considered $U = X$. By prefixing a channel $p_{X|U}$ to the original model, we obtain the achievability of (3). The cardinality bound on $\mathcal{U}$ follows by [11, Appendix C].

V. Converse

Consider the model in Fig. 3(a), where Eve observes the outputs of two independent channels, with $\mathbf{X}^n$ being the input to both the channels; one channel is the DMC $p_{V|X}$ and the other channel is the wiretapper channel in the WTC-II model. We first show that, for $\alpha \in [0,1]$, the strong secrecy capacity of this model, $\tilde{\mathsf{C}}_s^{\alpha}$, is equal to C_s^{α} in (3). To do so, since the main channels are the same, it suffices to show that $\forall S \in \mathcal{S}$, $I(M;\mathbf{Z}_S^n) = I(M;\tilde{\mathbf{Z}}_S^n\mathbf{V}^n)$, which follows because

$$\begin{aligned} H(M|\tilde{\mathbf{Z}}_S^n\mathbf{V}^n) &= H(M\mathbf{X}^n|\tilde{\mathbf{Z}}_S^n\mathbf{V}^n) - H(\mathbf{X}^n|M\tilde{\mathbf{Z}}_S^n\mathbf{V}^n) \\ &= H(\mathbf{X}^n|\tilde{\mathbf{Z}}_S^n\mathbf{V}^n) - H(\mathbf{X}^n|M\tilde{\mathbf{Z}}_S^n\mathbf{V}^n) \\ &= H(\mathbf{X}_{S^c}|\mathbf{X}_S\mathbf{V}_S\mathbf{V}_{S^c}) - H(\mathbf{X}_{S^c}|M\mathbf{X}_S\mathbf{V}_S\mathbf{V}_{S^c}) \\ &= H(\mathbf{X}_{S^c}|\mathbf{X}_S\mathbf{V}_{S^c}) - H(\mathbf{X}_{S^c}|M\mathbf{X}_S\mathbf{V}_{S^c}) \qquad (21) \\ &= H(\mathbf{X}^n|\mathbf{Z}_S^n) - H(\mathbf{X}^n|M\mathbf{Z}_S^n) = H(M|\mathbf{Z}_S^n), \qquad (22) \end{aligned}$$

for all $S \in \mathcal{S}$, where $\mathbf{Z}_S^n$ is defined in (1) and (21) follows since $p_{V|X}$ is a DMC.



(a) Equivalent model. (b) DM-WTC model.

Fig. 3. Channel models used for the converse proof.

Next, consider the model in Fig. 3(b), where the second channel to Eve is replaced with a DM-EC with erasure probability $1-\alpha$. The strong secrecy capacity of the model is

$$\mathsf{C}_{s,\mathrm{DM}}^{\alpha} = \max_{U-X-YVZ}[I(U;Y) - I(U;VZ)]^+. \qquad (23)$$

In order to compute (23), define $\Phi \sim \mathrm{Bern}(\alpha)$ whose i.i.d. samples represent the erasure process in the DM-EC, where $\Phi = 0$ when $Z = X$ and $\Phi = 1$ when $Z =?$. Φ is determined by Z and is independent of X. Thus, we have the Markov chain $U - X - YVZ\Phi$. Since the two channels to Eve are independent, we also have the Markov chain $V - X - Z\Phi$. We conclude that Φ and U are independent given V. Thus,

$$I(U;Z|V) = I(U;Z\Phi|V) = I(U;Z|\Phi V) = \alpha I(U;X|V).$$

Thus, (23) can be rewritten as

$$\mathsf{C}_{s,\mathrm{DM}}^{\alpha} = \max_{U-X-YV}[I(U;Y) - I(U;V) - \alpha I(U;X|V)]^+.$$

The converse is established by showing that, for $\alpha \in [0,1]$ and sufficiently large n, $\tilde{\mathsf{C}}_s^{\alpha} \leq \mathsf{C}_{s,\mathrm{DM}}^{\alpha}$. This is shown using similar arguments to [5, Section V-C]. The idea is that[1] when the number of erasures of the DM-EC is more than $(1-\alpha)n$, Eve's channel in Fig. 3(a) is better than its channel in Fig. 3(b), and $\tilde{\mathsf{C}}_s^{\alpha} \leq \mathsf{C}_{s,\mathrm{DM}}^{\alpha}$. The result is established by using Sanov's theorem in method of types [8], to show that the probability that the DM-EC causes erasures less than $(1-\alpha)n$ goes to 0 as $n \to \infty$. This completes the proof for Theorem 1.

[1]We provide a sketch of the proof due to space limitations.

VI. Conclusion

In this work, we have introduced a new wiretap channel (WTC) model and derived its strong secrecy capacity. This model generalizes the classical WTC [1] to one with a wiretapper who chooses a subset of the transmitted codeword to perfectly access, and generalizes the WTC-II with a DM main channel in [4] to one with a wiretapper who observes an output of a noisy channel instead of the erasures. The wiretapper in this model does not inject signals to the channel, yet she is more capable than a classical wiretapper since she can tap a subset of the symbols of her choosing noiselessly, while still receiving the remaining symbols through a channel. This result quantifies the secrecy cost of this additional capability of Eve.

Appendix A
Proof of Lemma 1

Define $V_x(m,c) \triangleq p_X(x)\mathbb{1}\{(\mathcal{B}_1(x),\mathcal{B}_2(x)) = (m,c)\}$, for all m, c. Thus, $P_{MC}(m,c) = \sum_{x\in\mathcal{X}} V_x(m,c)$. Since $\mathbb{E}_{\mathcal{B}}(\mathbb{1}\{(\mathcal{B}_1(x),\mathcal{B}_2(x)) = (m,c)\}) = \frac{1}{M\tilde{C}}$, $\forall x \in \mathcal{X}$, we have $\mathbb{E}_{\mathcal{B}}(P_{MC}) = \frac{1}{M\tilde{C}}$. Define the random variables $P_1(m,c) = \sum_{x\notin\mathcal{D}_\gamma} V_x(m,c)$ and $P_2(m,c) = \sum_{x\in\mathcal{D}_\gamma} V_x(m,c)$ such that $P_{MC}(m,c) = P_1(m,c) + P_2(m,c)$. Thus,

$$\begin{aligned} 2\mathbb{E}_{\mathcal{B}}\big(\mathbb{V}(P_{MC}, p_M^U p_C^U)\big) &= \mathbb{E}_{\mathcal{B}}\Big(\sum_{m,c}|P(m,c) - \mathbb{E}_{\mathcal{B}}P(m,c)|\Big) \\ &\leq \sum_{i=1,2}\sum_{m,c}\mathbb{E}_{\mathcal{B}}|P_i(m,c) - \mathbb{E}_{\mathcal{B}}P_i(m,c)| \leq 2\sum_{m,c}\mathbb{E}_{\mathcal{B}}P_1(m,c) \\ &\quad + \sum_{m,c}\mathbb{E}_{\mathcal{B}}\sqrt{(P_2(m,c) - \mathbb{E}_{\mathcal{B}}P_2(m,c))^2} \\ &\leq 2\mathbb{P}(X \notin \mathcal{D}_\gamma) + \sum_{m,c}\sqrt{\mathbb{V}\mathrm{ar}_{\mathcal{B}}(P_2(m,c))}, \qquad (24) \end{aligned}$$

where (24) follows from Jensen's inequality. For all m, c,

$$\begin{aligned} \mathbb{V}\mathrm{ar}P_2(m,c) &= \sum_{x\in\mathcal{D}_\gamma}\mathbb{V}\mathrm{ar}\big(p(x)\mathbb{1}\{(\mathcal{B}_1(x),\mathcal{B}_2(x)) = (m,c)\}\big) \\ &\leq \sum_{x\in\mathcal{D}_\gamma} p^2(x)\mathbb{E}(\mathbb{1}\{(\mathcal{B}_1(x),\mathcal{B}_2(x)) = (m,c)\}) \leq \frac{2^{-\gamma}}{M\tilde{C}} \qquad (25) \end{aligned}$$

as $p(x) \leq 2^{-\gamma}, \forall x \in \mathcal{D}_\gamma$. Lemma 1 follows from (24), (25).

Appendix B
Proof of Lemma 2

Lemma 3 *(Variation of Chernoff bound:) Let $\{U_i\}_{i=1}^n$ be independent random variables with $\mathbb{E}(U_i) = \bar{m}_i$. If $U_i \in [0,b]$, for all $i \in [\![1,n]\!]$, and $\sum_{i=1}^n \bar{m}_i \leq \bar{m}$, then, for every $\epsilon \in [0,1]$,*

$$\mathbb{P}\Big(\sum_{i=1}^n U_i \geq (1+\epsilon)\bar{m}\Big) \leq \exp\Big(-\epsilon^2\frac{\bar{m}}{3b}\Big). \qquad (26)$$

Proof: The proof can be adapted from [5, Lemma 4]. ■

For all $S \in \mathcal{S}$, define $\mathcal{A}_S \triangleq \big\{z \in \mathcal{Z} : \mathbb{P}_{p_{X|Z_S}}\big((X,z) \in \mathcal{D}_\gamma^S\big) \geq 1-\delta\big\}$. Using Markov inequality, we have

$$\mathbb{P}_{pz_S}(\mathcal{A}_S^c) \leq \frac{1}{\delta}\mathbb{P}_{pXz_S}\big((X,Z_S) \notin \mathcal{D}_\gamma^S\big) \leq \frac{\delta^2}{\delta} = \delta. \quad (27)$$

Let $\mathbb{1}_{\{x,m,c\}} \triangleq \mathbb{1}\{(\mathcal{B}_1(x),\mathcal{B}_2(x)) = (m,c)\}$. For all $m,c \in [\![1,\tilde{M}]\!] \times [\![1,\tilde{C}]\!]$, $z \in \mathcal{Z}$, $S \in \mathcal{S}$, define

$$P_1^S(m,c|z) = \sum_{x\in\mathcal{X}} p_{X|Z_S}(x|z)\mathbb{1}_{\{x,m,c\}}\mathbb{1}\{(x,z) \in \mathcal{D}_\gamma^S\}$$
$$P_2^S(m,c|z) = \sum_{x\in\mathcal{X}} p_{X|Z_S}(x|z)\mathbb{1}_{\{x,m,c\}}\mathbb{1}\{(x,z) \notin \mathcal{D}_\gamma^S\}.$$

Thus, $P_{MC|Z_S} = P_1^S + P_2^S$. Let $Q_z^S = \mathbb{P}_{p_{X|Z_S}}\big((X,z) \in \mathcal{D}_\gamma^S\big)$. Fix S and z, and let $P_1^S(m,c|z) = \sum_{x\in\mathcal{X}} U_x$, where

$$U_x = p_{X|Z_S}(x|z)\mathbb{1}_{\{x,m,c\}}\mathbb{1}\{(x,z) \in \mathcal{D}_\gamma^S\}.$$

Thus, $\{U_x\}_{x\in\mathcal{X}}$ are independent random variables, and

$$0 \leq U_x \leq p_{X|Z_S}(x|z)\mathbb{1}\{(x,z) \in \mathcal{D}_\gamma^S\} < 2^{-\gamma},$$

where $p_{X|Z_S}(x|z) < 2^{-\gamma}$, for all $(x,z) \in \mathcal{D}_\gamma^S$. Also, we have $\sum_x \mathbb{E}_{\mathcal{B}}(U_x) = Q_z^S/(\tilde{M}\tilde{C})$. Using Lemma 3, we have, for every $\epsilon_1 \in [0,1]$ and $z \in \mathcal{A}_S$, that

$$\mathbb{P}_{\mathcal{B}}\Big(P_1^S(m,c|z) \geq \frac{1+\epsilon_1}{\tilde{M}\tilde{C}}\Big) \leq \mathbb{P}\Big(\sum_x U_x \geq \frac{1+\epsilon_1}{\tilde{M}\tilde{C}}Q_z^S\Big)$$
$$\leq \exp\Big(\frac{-\epsilon_1^2 Q_z^S 2^\gamma}{3\tilde{M}\tilde{C}}\Big) \leq \exp\Big(\frac{-\epsilon_1^2(1-\delta)2^\gamma}{3\tilde{M}\tilde{C}}\Big), \quad (28)$$

where $Q_z^S \geq (1-\delta)$, for all $z \in \mathcal{A}_S$. We also have

$$\mathbb{E}_{pz_S}\Big(\sum_{m,c} P_2^S(m,c|Z_S)\Big) = \sum_{(x,z)\notin\mathcal{D}_\gamma^S} p_{XZ_S}(x,z) \times \sum_{m,c}\mathbb{1}_{\{x,m,c\}} = \mathbb{P}_{pXz_S}\Big((X,Z_S) \notin \mathcal{D}_\gamma^S\Big) \leq \delta^2, \quad (29)$$

since every $x \in \mathcal{X}$ is assigned to only one pair (m,c).

Note that for fixed (z,S), the random variable P_1^S is identically distributed for every (m,c), because of the symmetry in the random binning. We then define the event $\mathcal{G}$ as

$$\mathcal{G} \triangleq \Big\{P_1^S(m,c|z) < \frac{1+\epsilon_1}{\tilde{M}\tilde{C}}, \forall S \in \mathcal{S}, \text{ and } \forall z \in \mathcal{A}_S\Big\}. \quad (30)$$

Thus, using the union bound and (28), we have

$$\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c) = \mathbb{P}_{\mathcal{B}}\Big(\bigcup_{S,z\in\mathcal{A}_S} P_1^S(m,c|z) \geq \frac{1+\epsilon_1}{\tilde{M}\tilde{C}}\Big) \leq \sum_S |\mathcal{A}_S|$$
$$\mathbb{P}_{\mathcal{B}}\Big(P_1^S(m,c|z) \geq \frac{1+\epsilon_1}{\tilde{M}\tilde{C}}\Big) \leq |\mathcal{S}||\mathcal{Z}|e^{\left(\frac{-\epsilon_1^2(1-\delta)2^\gamma}{3\tilde{M}\tilde{C}}\right)}. \quad (31)$$

Let $\mathbf{b} \triangleq (b_1,b_2)$ be a realization of $\mathcal{B}$ such that $\mathbf{b} \in \mathcal{G}$, and set $M = b_1(X)$ and $C = b_2(X)$. For every $S \in \mathcal{S}$, we have

$$\mathbb{D}(P_{MCZ_S}||p_M^U p_C^U p_{Z_S}) = \mathbb{E}_{pz_S}\big(\mathbb{D}(P_{MC|Z_S}||p_M^U p_C^U)\big) =$$
$$\mathbb{E}_{pz_S}\sum_{m,c}\sum_{i=1}^2 P_i^S(m,c|Z_S)\log\frac{\sum_{i=1}^2 P_i^S(m,c|Z_S)}{\sum_{i=1}^2\sum_{m,c} P_i^S(m,c|Z_S)/\tilde{M}\tilde{C}}$$
$$\leq \mathbb{E}_{pz_S}\sum_{i=1}^2\sum_{m,c} P_i^S(m,c|Z_S)\log\frac{\tilde{M}\tilde{C}P_i^S(m,c|Z_S)}{\sum_{m,c}P_i^S(m,c|Z_S)}, \quad (32)$$

where (32) follows by the log-sum inequality. Using (29),

$$\mathbb{E}_{pz_S}\Big(\sum_{m,c} P_2^S(m,c|Z_S)\log\big(\tilde{M}\tilde{C}P_2^S(m,c|Z_S)\big)\Big)$$
$$\leq \log(\tilde{M}\tilde{C})\,\mathbb{E}_{pz_S}\big(\sum_{m,c} P_2^S(m,c|Z_S)\big) \leq \delta^2\log(\tilde{M}\tilde{C}). \quad (33)$$

Since $\sum_i\sum_{m,c} P_i^S(m,c|Z_S) = 1$, and $\sum_{m,c} P_1^S(m,c|Z_S) = \mathbb{P}_{p_{X|Z_S}}((X,Z_S) \in \mathcal{D}_\gamma^S)$, using Jensen's inequality gives

$$\mathbb{E}_{pz_S}\Big(\sum_{i=1}^2\sum_{m,c} P_i^S(m,c|Z_S)\log\frac{1}{\sum_{m,c}P_i^S(m,c|Z_S)}\Big) \leq$$
$$H_b(\mathbb{P}_{pXz_S}((X,Z_S) \in \mathcal{D}_\gamma^S)) \leq H_b(1-\delta^2) = H_b(\delta^2), \quad (34)$$

where the second inequality follows since $H_b(x)$ is monotonically decreasing in $x \in]\frac{1}{2},1[$. Finally, for $\mathbf{b} \in \mathcal{G}$, we have

$$\mathbb{E}_{pz_S}\Big(\sum_{m,c} P_1^S(m,c|Z_S)\log\big(\tilde{M}\tilde{C}P_1^S(m,c|Z_S)\big)\Big) =$$
$$\mathbb{E}_{pz_S}\Big(\sum_{m,c,Z_S\in\mathcal{A}_S} P_1^S(m,c|Z_S)\log\big(\tilde{M}\tilde{C}P_1^S(m,c|Z_S)\big)\Big) +$$
$$\mathbb{E}_{pz_S}\Big(\sum_{m,c,Z_S\notin\mathcal{A}_S} P_1^S(m,c|Z_S)\log\big(\tilde{M}\tilde{C}P_1^S(m,c|Z_S)\big)\Big) \leq$$
$$\log(1+\epsilon_1) + \mathbb{P}(Z_S \notin \mathcal{A}_S)\log\tilde{M}\tilde{C} \leq \epsilon_1 + \delta\log\tilde{M}\tilde{C}. \quad (35)$$

Using (32)-(35), we have, for $\mathbf{b} \in \mathcal{G}$ and $\forall S \in \mathcal{S}$, that

$$\mathbb{D}(P_{MCZ_S}||p_M^U p_C^U p_{Z_S}) \leq \epsilon_1 + (\delta+\delta^2)\log(\tilde{M}\tilde{C}) + H_b(\delta^2).$$

Thus, the probability in (7) is upper bounded by $\mathbb{P}_{\mathcal{B}}(\mathcal{G}^c)$.

REFERENCES

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

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

[3] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

[4] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," *International Symposium on Information Theory*, June 2015.

[5] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *Submitted to IEEE Trans. Info. Theory*, 2015, arXiv pre-print arXiv:1509.03619v1.

[6] 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.

[7] 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.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory, 2nd edition*. New York, NY, USA: Wiley, 2006.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–Part II: CR capacity," *IEEE Trans. Info. Theory*, vol. 44, no. 1, pp. 225–240, 1998.

[10] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journ. Amer. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963.

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

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