An Achievable Region for the Wiretap Multiple-Access Channel with Common Message

Moritz Wiese, Holger Boche
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
{wiese, boche}@tum.de

***Abstract*—We derive a rate region which is achievable by the Wiretap MAC with Common Message under the strong secrecy criterion. We follow Devetak's approach to establishing strong secrecy. Using the concentration of the normed sum of bounded i.i.d. random variables around its mean, it is possible to show the existence of a code where the channel outputs at the eavesdropper are almost independent of the messages. The encoders may use a certain amount of common randomness. We give the example of a channel where the availability of common randomness is necessary for secret transmission.**

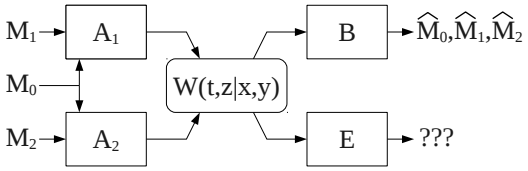

Fig. 1. The Wiretap MAC with encoders Alice$_1$ (A_1), Alice$_2$ (A_2), intended receiver Bob (B) and eavesdropper Eve (E).

I. Introduction

This paper studies the discrete memoryless Multiple Access Channel (MAC) where communication is overheard by a second receiver named Eve who acts as an eavesdropper. The encoders Alice$_1$ and Alice$_2$ have a private message each and a common message all of which need to be kept secret from Eve, whereas the intended receiver Bob should be able to decode all messages with arbitrarily small average error, see Fig. I. We apply the strong secrecy criterion. In order to satisfy this criterion, the encoders may use some amount of common randomness measured by its entropy. Conditional on this randomness, they can additionally apply independent stochastic encoding. The result of this paper will be the basis for deriving a strongly secret rate region for the wiretap MAC with conferencing encoders as in [18]. This is the basic model for base station cooperation and requires to keep track of the common randomness used by the encoders.

We use Devetak's approach [7] to establishing strong secrecy, which was originally used to establish strong secrecy in the Quantum Wiretap channel with classical inputs. In contrast to the weak secrecy criterion introduced in the papers of Wyner [19] and Csiszár and Körner [6], only the strong secrecy criterion has been given an operational meaning so far. It was shown in [1] that if the strong secrecy criterion is satisfied, then the average error of the non-legitimate user for any decoding scheme it might apply tends to one as the codelength tends to infinity. The strong secrecy criterion was used, among others, in [2][3][4][13].

We do not obtain a converse, but a single-letter achievable region. This is in contrast to [9], where a multi-letter achievable region for the wiretap MAC with external eavesdroppers, without common message nor common randomness is derived under the weak secrecy criterion. For special "weak" wiretap MACs, a multi-letter converse is found.

There are many other ways of incorporating secrecy issues into MAC models. For example, each encoder may obtain generalized feedback and want to keep the other sender instead of an eavesdropper uninformed about its message [8][11][12]. The case where the encoders have access to generalized feedback but do not have to keep their messages secret from each other, but from an external eavesdropper, is considered in [16].

In the cognitive MAC, the encoders have a common message and one has a private message. If there is no eavesdropper, the encoder without a private message obtains a noisy version of the codeword sent by the other encoder and must be kept ignorant of the other encoder's private message [10]. In [14], the cognitive MAC without feedback was investigated where the messages must be kept secret from an eavesdropper and the encoders have unrestricted access to common randomness.

Our paper is organized as follows. Section II contains the problem and the main result which is proved in Section III. In the last section, we discuss the result and give an example.

Notation: We set $[K] := \{1, \dots, K\}$ for positive integers K. $[x]_+ := \max(x, 0)$. $\mathscr{P}(\mathscr{X})$ are the probability measures on the finite set $\mathscr{X}$, and for measures μ_1, μ_2 on $\mathscr{X}$, we define the metric $\|\mu_1 - \mu_2\| := \sum_{x \in \mathscr{X}} |\mu_1(x) - \mu_2(x)|$. $\delta(x, \cdot)$ is the Dirac measure with mass in x. P_X is the distribution of the random variable X. For a random pair (U, X), $T^n_{U,\delta}$ denotes the U-typical n-sequences and $T^n_{X|U,\delta}(\mathbf{u})$ the $X|U$-typical n-sequences conditional on $\mathbf{u}$ with constant δ, see [5] for details.

II. System Model and Main Result

The encoders have the finite input alphabets $\mathscr{X}$ and $\mathscr{Y}$, respectively, Bob's alphabet is $\mathscr{T}$, and Eve receives outputs from the alphabet $\mathscr{Z}$. The wiretap channel is memoryless, it is determined by a stochastic matrix $W : \mathscr{X} \times \mathscr{Y} \to \mathscr{P}(\mathscr{T} \times \mathscr{Z})$ whose marginals are denoted by W_T and W_Z, respectively.

The transmission of words $\mathbf{x} \in \mathscr{X}^n$ and $\mathbf{y} \in \mathscr{Y}^n$ is governed by the probabilities

$$W^{\otimes n}(\mathbf{t}, \mathbf{z}|\mathbf{x}, \mathbf{y}) = \prod_{i=1}^{n} W(t_i, z_i|x_i, y_i), \quad (\mathbf{t}, \mathbf{z}) \in \mathscr{T}^n \times \mathscr{Z}^n.$$

Encoding may be stochastic. We fix a number $H_C \geq 0$ and let the encoders have access to any source of common randomness with entropy at most H_C which can be used in encoding. That means that if the message sets are $[K_0], [K_1], [K_2]$ for the common and the private messages, respectively, blocklength-n encoding is given by a stochastic matrix $G : [K_0] \times [K_1] \times [K_2] \to \mathscr{P}(\mathscr{X}^n \times \mathscr{Y}^n)$ which has the form

$$G(\mathbf{x}, \mathbf{y}|k_0, k_1, k_2) = \sum_{j \in \mathscr{J}} G_0(j|k_0) G_1(\mathbf{x}|k_0, k_1, j) G_2(\mathbf{y}|k_0, k_2, j).$$

Here $\mathscr{J}$ is a finite set and $H(G_0(\cdot|k_0)) \leq nH_C$ for every k_0. Decoding is done deterministically in the usual way. A code with blocklength n and message sets $[K_0], [K_1], [K_2]$ is called a code (n, K_0, K_1, K_2).

A rate R is achievable if for every $\varepsilon > 0$ there is for sufficiently large n a code (n, K_0, K_1, K_2) satisfying

$$\log K_\nu \geq n(R_\nu - \varepsilon) \quad (\nu = 0, 1, 2),$$
$$\mathbb{P}[\phi(T^n) \neq (M_0, M_1, M_2)] \leq \varepsilon,$$
$$I(M_0, M_1, M_2 \wedge Z^n) \leq \varepsilon,$$

where the M_ν are uniformly distributed on $[K_\nu]$ $(\nu = 0, 1, 2)$, where ϕ is the decoder of the code (n, K_0, K_1, K_2) and where T^n and Z^n are the output random variables at Bob and Eve, respectively, induced by the random message selection, the stochastic encoding, and transmission over the channel.

Let $\mathscr{U}, \mathscr{V}_1, \mathscr{V}_2$ be finite alphabets and let $U, (V_1, V_2), (X, Y), (T, Z)$ be a Markov chain with U taking values in $\mathscr{U}$, with V_1, V_2 taking values in $\mathscr{V}_1$ and $\mathscr{V}_2$ and independent conditional on U, with X only depending on V_1 and Y only depending on V_2 and with $P_{TZ|XY} = W$. We denote the joint distribution of this Markov chain by p. If $H_C = 0$, we need that U is single-valued, i.e. we have independent inputs. For $H_C > 0$, the form of the rate region achievable with input distribution p depends on the information between the inputs and Eve's outputs. Due to lack of space we concentrate here on the most challenging case that $I(Z \wedge U) < H_C \leq \min\{I(Z \wedge V_1, U), I(Z \wedge V_2, U)\}$.

For $H_C > 0$, let Π_{H_C} be the set of p that additionally satisfy

$$I(Z \wedge V_1|U) \leq I(T \wedge V_1|V_2, U), \tag{1}$$
$$I(Z \wedge V_2|U) \leq I(T \wedge V_2|V_1, U), \tag{2}$$
$$I(Z \wedge V_1, V_2|U) \leq I(T \wedge V_1|V_2, U) + I(Z \wedge V_2|V_1, U), \tag{3}$$
$$I(Z \wedge V_1, V_2) \leq I(T \wedge V_1, V_2). \tag{4}$$

Then we define the rate set $\mathscr{R}(p)$ as the set of triples of nonnegative reals satisfying

$$\begin{aligned} R_1 &\leq I(T \wedge V_1|V_2, U) - I(Z \wedge V_1|U) \\ &\quad - [I(Z \wedge V_2|V_1, U) - I(T \wedge V_2|V_1, U)]_+, \\ R_2 &\leq I(T \wedge V_2|V_1, U) - I(Z \wedge V_2|U) \\ &\quad - [I(Z \wedge V_1|V_2, U) - I(T \wedge V_1|V_2, U)]_+, \\ R_1 + R_2 &\leq I(T \wedge V_1, V_2|U) - I(Z \wedge V_1, V_2|U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1, V_2) - I(Z \wedge V_1, V_2). \end{aligned}$$

We set $p \in \Pi_0$ if U is deterministic and (1)-(4) are satisfied. $\mathscr{R}(p)$ is defined analogously in this case except that the transmission of a common message is impossible.

Theorem 1. *For the common randomness entropy limited by $H_C \geq 0$, an achievable rate region for the wiretap MAC with common message is given by*

$$\mathscr{A} := closure\left(conv\left(\bigcup_{p \in \Pi_{H_C}} \mathscr{R}(p)\right)\right),$$

where conv is the convex hull operator.

III. The Proof

Using [5, Lemma 2.7], one has

$$I(Z^n \wedge M_0, M_1, M_2) \leq -\eta \log \frac{\eta}{|\mathscr{Z}|^n K_0 K_1 K_2},$$

where $\eta = \|P_{Z^n} \otimes P_{M_0 M_1 M_2} - P_{Z^n M_0 M_1 M_2}\|$. Thus if η tends to zero exponentially and if the K_ν do not grow faster than exponentially, then $I(Z^n \wedge M_0, M_1, M_2)$ also tends to zero exponentially. If there is a measure θ on $\mathscr{Z}^n$ satisfying

$$\|P_{Z^n|k_0,k_1,k_2} - \theta\| \leq 2^{-n\beta} \tag{5}$$

for some $\beta > 0$ uniformly in k_0, k_1, k_2, then η is exponentially small, because

$$\eta = \frac{1}{K_0 K_1 K_2} \sum_{k_0,k_1,k_2} \|P_{Z^n} - P_{Z^n|k_0,k_1,k_2}\| \leq 2 \cdot 2^{-n\beta}.$$

Thus for secrecy, it is sufficient to show (5). We concentrate on proving the achievability of those sets $\mathscr{R}(p)$ whose p does not involve the auxiliary random variables V_1, V_2. These can be included in the usual way by prefixing them to W independently at the two encoders. Note that no common randomness is needed to do that. Thus let a $p \in \Pi_{H_C}$ be given which is the joint probability distribution of random variables $U, (X, Y), (T, Z)$. We use a random code construction. Let a family $\{(U_{k_0}^{l_0}, X_{k_0 k_1}^{l_0 l_1}, Y_{k_0 k_2}^{l_0 l_2})\}$ be given, where k_0, k_1, k_2 are messages and $l_\nu \in [L_\nu]$, $\nu = 0, 1, 2$ are indices needed in stochastic encoding. The $U_{k_0}^{l_0}$ are i.i.d. on $\mathscr{U}^n$ according to

$$P'_{U^n}(\mathbf{u}) := \frac{P_U^{\otimes n}(\mathbf{u})}{P_U^{\otimes n}(T_{U,\delta}^n)}$$

for some $\delta > 0$. For any k_0, l_0, given $U_{k_0}^{l_0} = \mathbf{u}$, the $X_{k_0 k_1}^{l_0 l_1}$ are conditionally i.i.d. on $\mathscr{X}^n$ according to

$$P'_{X^n|U^n}(\mathbf{x}|\mathbf{u}) := \frac{P_{X|U}^{\otimes n}(\mathbf{x}|\mathbf{u})}{P_{X|U}^{\otimes n}(T_{X|U,\delta}^n(\mathbf{u})|\mathbf{u})},$$

and the $Y_{k_0k_2}^{l_0l_2}$ on $\mathscr{Y}^n$ according to $P'_{Y^n|U^n}$ which is defined analogously to $P'_{X^n|U^n}$ with $\mathbf{x}$ replaced by $\mathbf{y}$ and X replaced by Y. Following Devetak's approach [7], we obtain the following bounds (6)-(8) on the L_ν that need to be satisfied to establish (5):

$$\log L_0 \geq n(I(Z \wedge U) + 4\tau), \tag{6}$$
$$\log L_1 \geq n(I(Z \wedge X|Y,U) + 4\tau), \tag{7}$$
$$\log L_2 \geq n(I(Z \wedge Y|U) + 4\tau). \tag{8}$$

An alternative triple of bounds (6')-(8') can be obtained with X and Y exchanged. τ depends on δ and $\tau \searrow 0$ as $\delta \to 0$. (6)-(8) and (6')-(8') ensure that the probability of obtaining a realization of the random variables $\{U_{k_0}^{l_0}, X_{k_0k_1}^{l_0l_1}, Y_{k_0k_2}^{l_0l_2}\}$ for which (5) is not true is exponentially small. The proofs of (6)-(8) all build on the following Chernoff-Hoeffding bound.

Lemma 2. *Let $b > 0$. For an independent sequence of random variables $Z_1, \ldots, Z_L$ with values in $[0, b]$ with $\mu_l := \mathbb{E}[X_l]$ and $\mu := \frac{1}{L}\sum_l \mu_l$, one has*

$$\mathbb{P}\left[\frac{1}{L}\sum_{l=1}^{L} Z_l \notin [(1 \pm \varepsilon)\mu]\right] \leq \exp\left(-L \cdot \frac{\varepsilon^2 \mu}{2b \ln 2}\right)$$

In order to make use of Lemma 2, we need to exploit the structure of the random family. For (6)-(8), we use that the $X_{k_0k_1}^{l_0l_1}$ are i.i.d. given $U_{k_0}^{l_0}$ and $Y_{k_0k_2}^{l_0l_2}$, the $Y_{k_0k_2}^{l_0l_2}$ are i.i.d. given the $U_{k_0}^{l_0}$ and the $U_{k_0}^{l_0}$ are unconditionally i.i.d. Analogous properties are used for (6')-(8'). All the applications of Lemma 2 involve modifications of W_Z which are necessary to obtain useful estimates. They can be undone with small error after choosing an appropriate realization of the random variables as the modifications are restrictions to typicality. Due to lack of space, we cannot go into the details of the proof of (6)-(8), but we describe the settings to which Lemma 2 is applied. For every (k_0, k_1, k_2), the corresponding random variables exhibit the same behavior, so we pick one (k_0, k_1, k_2) and omit these indices here. Starting with (7), let $(\mathbf{u}, \mathbf{y}) \in T^n_{UY,2\delta}$ and

$$E_1(\mathbf{u},\mathbf{x},\mathbf{y}) := \{\mathbf{z} \in T^n_{Z|YU,2|\mathscr{X}|\delta}(\mathbf{y},\mathbf{u}) : W_Z^{\otimes n}(\mathbf{z}|\mathbf{x},\mathbf{y}) \leq 2^{-n(H(Z|X,Y)-\tau)}\}.$$

This will give a bound on the random variables corresponding to the b from Lemma 2. $\tau > 0$ is chosen later when $\|P_{Z^n|k_0k_1k_2} - \theta\|$ is estimated. Define

$$\theta'_{\mathbf{uy}}(\mathbf{z}) := \mathbb{E}[W_Z^{\otimes n}(\mathbf{z}|X^{11},\mathbf{y})1_{E(\mathbf{u},X^{11},\mathbf{y})}(\mathbf{z})|U^1 = \mathbf{u}],$$
$$F_1(\mathbf{u},\mathbf{y}) := \{\mathbf{z} \in T^n_{Z|YU,2|\mathscr{X}|\delta}(\mathbf{y},\mathbf{u}) : \theta'_{\mathbf{uy}}(\mathbf{z}) \geq \varepsilon |T^n_{Z|YU,2|\mathscr{X}|\delta}(\mathbf{y},\mathbf{u})|^{-1}\}$$

and $\theta_{\mathbf{uy}} := \theta'_{\mathbf{uy}} \cdot 1_{F_1(\mathbf{u},\mathbf{y})}$. This will provide a lower bound on the mean of the random variables used. We set $E_2(\mathbf{u},\mathbf{x},\mathbf{y}) := E_1(\mathbf{u},\mathbf{x},\mathbf{y}) \cap F_1(\mathbf{u},\mathbf{y})$. For every $\mathbf{z} \in \mathscr{Z}^n$ and every (l_0, l_2), let $A_1(l_0, l_2, \mathbf{z})$ be the event

$$\frac{1}{L_1}\sum_{l_1} W_Z^{\otimes n}(\mathbf{z}|X^{l_0l_1}, Y^{l_0l_2})1_{E_2(U^{l_0},X^{l_0l_1},Y^{l_0l_2})}(\mathbf{z}) \in [(1 \pm \varepsilon)\theta_{U^{l_0}Y^{l_0l_2}}(\mathbf{z})].$$

Then, conditioning on all possible realizations of $U^{l_0}, Y^{l_0l_2}$ adn applying the law of total probability, one obtains with Lemma 2 for n sufficiently large

$$\mathbb{P}[A_1(l_0,l_2,\mathbf{z})^c] \leq 2\exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge X|Y,U)+2\tau)}}{2\ln 2}\right). \tag{9}$$

We denote the intersection of all $A_1(l_0, l_2, \mathbf{z})$ as l_0, l_2 and $\mathbf{z}$ are varied by A_1.

Next we turn to (8). Define

$$\theta'_{\mathbf{u}}(\mathbf{z}) := \mathbb{E}[W_Z^{\otimes n}(\mathbf{z}|X^{11},Y^{11})1_{E_2(\mathbf{u},X^{11},Y^{11})}(\mathbf{z})|U^1 = \mathbf{u}],$$
$$F_2(\mathbf{u}) := \{\mathbf{z} \in T^n_{Z|U,3|\mathscr{Y}||\mathscr{X}|\delta}(\mathbf{u}) : \theta'_{\mathbf{u}}(\mathbf{z}) \geq \varepsilon |T^n_{Z|U,\delta}(\mathbf{u})|^{-1}\}.$$

Further set $\theta_{\mathbf{u}} = \theta'_{\mathbf{u}} \cdot 1_{F_2(\mathbf{u})}$ and $E_0(\mathbf{u},\mathbf{x},\mathbf{y}) := E_2(\mathbf{u},\mathbf{x},\mathbf{y}) \cap F_2(\mathbf{u},\mathbf{y})$. For every l_0 and $\mathbf{z} \in \mathscr{Z}^n$, let $A_2(l_0, \mathbf{z})$ be the event

$$\frac{1}{L_1L_2}\sum_{l_1l_2} W_Z^{\otimes n}(\mathbf{z}|X^{l_0l_1}, Y^{l_0l_2})1_{E_0(U^{l_0},X^{l_0l_1},Y^{l_0l_2})}(\mathbf{z}) \in [(1 \pm 3\varepsilon)\theta_{U^{l_0}}(\mathbf{z})].$$

Then for ε small and n large,

$$\mathbb{P}[A_2(l_0,\mathbf{z})^c] \leq 2|\mathscr{Y}|^n \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge X|Y,U)+2\tau)}}{2\ln 2}\right) + 2\exp\left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge Y|U)+2\tau)}}{4\ln 2}\right). \tag{10}$$

The first term in the above bound comes from the probability that conditional on any realization of $U^{l_0}, Y^{l_0l_2}$, the family $\{X^{l_0l_1} : l_1 \in [L_1]\}$ does not satisfy $A_1(l_0, l_2, \mathbf{z})$. The second term is obtained by an application of Lemma 2 to the L_2 normed sums over l_1 of random variables found in the definition of $A_2(l_0, \mathbf{z})$ where the realizations of the $X^{l_0l_1}$ do satisfy $A_1(l_0, l_2, \mathbf{z})$ for every realization of $U^{l_0}, Y^{l_0l_2}$. $F_2(\mathbf{u})$ again gives a lower bound on their mean. We denote the intersection of the $A_2(l_0, \mathbf{z})$ by A_2.

Next we consider (6). We also need $A_2(\mathbf{z})$, the intersection over l_0 of the $A_2(l_0, \mathbf{z})$. For every $\mathbf{z}$ define a new probability measure $\hat{\mathbb{P}}_{\mathbf{z}} := \mathbb{P}[\cdot|A_2(\mathbf{z})]$. Let $\theta'(\mathbf{z}) := \hat{\mathbb{E}}_{\mathbf{z}}[\theta_{U_1^1}(\mathbf{z})]$ and

$$F_0 := \{\mathbf{z} \in T^n_{Z,4|\mathscr{Y}||\mathscr{X}||\mathscr{U}|\delta} : \theta'(\mathbf{z}) \geq |T^n_{Z,4|\mathscr{Y}||\mathscr{X}||\mathscr{U}|\delta}|^{-1}\}.$$

Finally, set $\theta := \theta' \cdot 1_{F_0}$. For $\mathbf{z} \in F_0$ let $A_0(\mathbf{z})$ be the event that

$$\frac{1}{L_0L_1L_2}\sum_{l_0,l_1,l_2} W_Z^{\otimes n}(\mathbf{z}|X^{l_0l_1}, Y^{l_0l_2})1_{E_0(U^{l_0},X^{l_0l_1},Y^{l_0l_2})}(\mathbf{z}) \in [(1 \pm 5\varepsilon)\theta(\mathbf{z})].$$

Then for n large and ε small

$$\mathbb{P}[A_0(\mathbf{z})^c] \leq 2\,L_0|\mathscr{Y}|^n \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge X|Y,U)+2\tau)}}{2\ln 2}\right) + 2\,L_0 \exp\left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge Y|U)+2\tau)}}{4\ln 2}\right) + 2\exp\left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z\wedge U)+2\tau)}}{4\ln 2}\right). \tag{11}$$

Here we again use the law of total probability. The first two terms in (11) come from the bound on $\mathbb{P}[A_2(l_0,\mathbf{z})^c]$. The third term results from an application of Lemma 2 to the L_0 random variables appearing in the definition of $A_0(\mathbf{z})$ which are i.i.d. conditional on $A_2(\mathbf{z})$ with respect to $\hat{\mathbb{P}}_{\mathbf{z}}$. We denote the intersection of all $A_0(\mathbf{z})$ by A_0.

Lemma 2 also establishes that given l_0, l_2, most of the $X^{l_0 l_1} : l_1 \in [L_1]$ are typical conditional on $(Y^{l_0 l_2}, U^{l_0})$ with high probability. For every (l_0, l_2) let the event $A_*(l_0, l_2)$ be defined by

$$A_*(l_0,l_2) := \big\{|\{l_1 \in [L_1] : X^{l_0 l_1} \in T^n_{X|YU,\delta}(Y^{l_0 l_2}, U^{l_0})\}| \\ \geq (1-\varepsilon)(1-2\cdot 2^{-nc\delta^2})L_1\big\}.$$

Then

$$\mathbb{P}\left[A_*(l_0,l_2)^c\right] \leq \exp\left(-L_1 \cdot \frac{\varepsilon^2(1-2\cdot 2^{-nc\delta^2})}{2\ln 2}\right). \quad (12)$$

We denote the intersection of all $A_*(l_0, l_2)$ by A_*.

If $\varepsilon = 2^{-n\beta}$ for sufficiently small $\beta > 0$ and L_0, L_1, L_2 are chosen according to (6)-(8), then the bounds (9)-(12) tend to zero doubly-exponentially. By symmetry, it is possible to prove an analogous sequence of statements where the roles of the $X^{l_0 l_1}$ and $Y^{l_0 l_2}$ are exchanged. This gives the alternative bounds (6')-(8').

Now we use the indices k_0, k_1, k_2 again. Before passing to a realization of our random variables, we need to consider the transmission of messages to Bob. By the coding theorem for the MAC W_T with common message and without an eavesdropper [15], all rate triples $(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2)$ are achievable that are contained in the set $\tilde{\mathscr{R}}(p)$ defined by

$$\begin{aligned} \tilde{R}_1 &\leq I(T\wedge X|Y,U),\\ \tilde{R}_2 &\leq I(T\wedge Y|X,U),\\ \tilde{R}_1+\tilde{R}_2 &\leq I(T\wedge X,Y|U),\\ \tilde{R}_0+\tilde{R}_1+\tilde{R}_2 &\leq I(T\wedge X,Y). \end{aligned}$$

It is easy to see that with probability exponentially close to 1, the elements of $\{X^{l_0 l_1}_{k_0 k_1}, Y^{l_0 l_2}_{k_0 k_2} : k_0, \ldots, l_2\}$ are the codewords of a deterministic code for the non-wiretap MAC W_T with common message with an exponentially small average error if $(1/n)(\log(K_0L_0)+\eta, \log(K_1L_1)+\eta, \log(K_2L_2)+\eta)$ is contained in $\tilde{\mathscr{R}}(p)$ for some $\eta > 0$.

In particular, this requires $(1/n)(\log(L_0)+\eta, \log(L_1)+\eta, \log(L_2)+\eta) \in \tilde{\mathscr{R}}(p)$. This does not have to be true for the vector $I^{(1)} := (I(Z\wedge U), I(Z\wedge X|Y,U), I(Z\wedge Y|U))$ nor its analog $I^{(2)}$ with the roles of X and Y exchanged. However, a convex combination of the two might be contained in $\tilde{\mathscr{R}}(p)$. Thus we have to include time-sharing in the random coding structure instead of doing it after derandomization as usual. We need two families of random variables as above, one with blocklength n_1, the other with blocklength n_2, and with message and randomization sets $[K^{(1)}_\nu], [L^{(1)}_\nu]$ and $[K^{(2)}_\nu], [L^{(2)}_\nu]$, respectively $(\nu = 0,1,2)$. For the first of these families, we know that $A_* \cap A_0 \cap A_1 \cap A_2$ holds and that it is the deterministic codeword set for a non-wiretap MAC code with exponentially high probability. Analogous statements are true for the second family, where the roles of X and Y are exchanged in (9)-(12). Thus we can conclude that there is a realization of the two families satisfying all the above events. We thus obtain for the two concatenated parts $\nu = 1,2$ of the code independent stochastic encoders $G^{(1)}, G^{(2)}$. They are defined analogously. For $G^{(\nu)}$ set $\mathscr{J}^{(\nu)} = [L^{(\nu)}_0]$ and $G^{(\nu)}_0(l^{(\nu)}_0|k^{(\nu)}_0) := 1/L^{(\nu)}_0$. Given $k^{(\nu)}_0, k^{(\nu)}_1, l^{(\nu)}_0$, Alice$_1$ chooses the codeword $\mathbf{x}^{l^{(\nu)}_0 l^{(\nu)}_1}_{k^{(\nu)}_0 k^{(\nu)}_1}$ with probability $1/L^{(\nu)}_1$ and Alice$_2$ independently of Alice$_1$ chooses $\mathbf{y}^{l^{(\nu)}_0 l^{(\nu)}_2}_{k^{(\nu)}_0 k^{(\nu)}_2}$ with probability $1/L^{(\nu)}_2$. For δ small and $L_0 = L^{(1)}_0 L^{(2)}_0$ close to its bound (6), the encoder satisfies the common randomness restriction because of $I(Z\wedge U) < H_C$. Bob can still decode all messages from the Alices using the deterministic MAC encoder given by the realization of the random variables. If $n_1/(n_1+n_2) \approx \alpha \in [0,1]$, then the rates achieved by this code are approximately

$$\begin{aligned} R_1 &\approx I(T\wedge X|Y,U) - \alpha I(Z\wedge X|Y,U)\\ &\quad - (1-\alpha)I(Z\wedge X|U),\\ R_2 &\approx I(T\wedge Y|X,U) - \alpha I(Z\wedge Y|U)\\ &\quad - (1-\alpha)I(Z\wedge Y|Y,U),\\ R_1+R_2 &\approx I(T\wedge X,Y|U) - I(Z\wedge X,Y)|U),\\ R_0+R_1+R_2 &\approx I(T\wedge X,Y) - I(Z\wedge X,Y). \end{aligned}$$

We denote the rate region defined by the bounds on the right-hand side by $\mathscr{R}_\alpha(p)$. It remains to show (5) for the chosen realization. As the encoders in the two parts of the code are independent and the channel memoryless, it is sufficient to prove the secrecy of the first part, the proof for the second being analogous. We omit the family index (also setting $n_1 =: n$) and introduce the symbols $\sum' := (1/L_0L_1L_2)\sum$ and $\tilde{W} := W_Z^{\otimes n}$ for brevity. We have for every (k_0,k_1,k_2)

$$\begin{aligned} &\|P_{Z^n|k_0k_1k_2} - \theta\|\\ \leq &\|\theta - \sum_{l_0,l_1,l_2}{}' \tilde{W}(\cdot|\mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2}) 1_{E_0(\mathbf{u}^{l_0}_{k_0}, \mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2})} 1_{F_0}\|\\ +&\|\sum_{l_0,l_1,l_2}{}' \tilde{W}(\cdot|\mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2}) 1_{E_0(\mathbf{u}^{l_0}_{k_0}, \mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2})} 1_{F_0^c}\|\\ +&\|\sum_{l_0,l_1,l_2}{}' \tilde{W}(\cdot|\mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2}) 1_{E_2(\mathbf{u}^{l_0}_{k_0}, \mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2})} 1_{F_2(\mathbf{u}^{l_0}_{k_0})^c}\|\\ +&\|\sum_{l_0,l_1,l_2}{}' \tilde{W}(\cdot|\mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2}) 1_{E_1(\mathbf{u}^{l_0}_{k_0}, \mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2})} 1_{F_1(\mathbf{u}^{l_0}_{k_0}, \mathbf{y}^{l_0l_2}_{k_0k_2})^c}\|\\ +&\|\sum_{l_0,l_1,l_2}{}' \tilde{W}(\cdot|\mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2}) 1_{E_1(\mathbf{u}^{l_0}_{k_0}, \mathbf{x}^{l_0l_1}_{k_0k_1}, \mathbf{y}^{l_0l_2}_{k_0k_2})} - P_{Z^n|k_0k_1k_2}\|. \end{aligned}$$

We denote the five terms by I-V in that order. I is at most ε because A_0 is satisfied by choice of the realization of the random family. II-IV are shown backwards. One has to apply several properties of typical sets together with assumption A_1 in IV, A_2 in III and A_0 in II. In V, we use that A_* is satisfied. Altogether this gives an upper bound on (5) of $20\cdot\varepsilon + 5\cdot 2^{-nc\delta^2}$.

So far, we have proved that for every $p \in \Pi_{H_C}$ without auxiliary random variables V_1, V_2, the union of all $\mathscr{R}_\alpha(p)$ is achievable for those α satisfying

$$\alpha I^{(1)} + (1-\alpha) I^{(2)} \in \tilde{\mathscr{R}}(p).$$

It remains to determine this union and the extremal α (the convexity of the rate region implies that the set of permissible α is an interval). The Markovity of the sequence $U, (X,Y), (T,Z)$ easily implies that the union of the permissible $\mathscr{R}_\alpha(p)$ is the set defined by the bounds

$$\begin{aligned} R_1 &\le I(T \wedge X|Y,U) - \alpha_0 I(Z \wedge X|Y,U) \\ &\quad - (1-\alpha_0) I(Z \wedge X|U), \qquad (13) \\ R_2 &\le I(T \wedge Y|X,U) - \alpha_1 I(Z \wedge Y|U) \\ &\quad - (1-\alpha_1) I(Z \wedge Y|Y,U), \qquad (14) \\ R_1 + R_2 &\le I(T \wedge X,Y|U) - I(Z \wedge X,Y)|U), \qquad (15) \\ R_0 + R_1 + R_2 &\le I(T \wedge X,Y) - I(Z \wedge X,Y), \qquad (16) \end{aligned}$$

where α_0 is the smallest permissible α and α_1 the largest. First note that there is no permissible α at all if (4) is not satisfied. (1) and (2) must be satisfied as $\alpha \in [0,1]$ and (3) ensures $\alpha_0 \le \alpha_1$. The extremal alphas can be determined to be

$$\begin{aligned} \alpha_0 &= \left[\frac{I(T \wedge V_2|V_1,U) - I(Z \wedge V_2|V_1,U)}{I(Z \wedge V_2|U) - I(Z \wedge V_2|V_1,U)} \right]_+, \\ \alpha_1 &= \min\left(\frac{I(T \wedge V_1|V_2,U) - I(Z \wedge V_1|U)}{I(Z \wedge V_1|V_2,U) - I(Z \wedge V_1|U)}, 1 \right). \end{aligned}$$

Inserting these in (13) and (14), one obtains $\mathscr{R}(p)$.

IV. Discussion

Here we show that $H_C > 0$ may be necessary for secret transmission. In an easy generalization of van Dijk's result [17], one sees that $I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2) \le 0$ for every input-p where V_1 and V_2 are independent, meaning that transmission at $H_C = 0$ is impossible, if and only if this difference is concave in both P_{V_1} and P_{V_2} (not necessarily jointly). This is satisfied for the following channel: let $\mathscr{X} = \mathscr{Y} = \{0,1\}$, $\mathscr{T} = GF(3)$, $\mathscr{Z} = \{-2, \ldots, 3\}$, and let N_1, N_2 be random variables uniformly distributed on $\{0,1\}$. Let the outputs t of W_T and the outputs z of W_Z be given by

$$t = x + y + N_1, \qquad z = 2x - 2y + N_2.$$

The concavity of the above difference of mutual information terms can be shown by elementary analysis. If sufficient common randomness is available to the encoders, however, the joint input distribution giving probability $1/2$ to both $(0,0)$ and $(1,1)$ can be obtained. If V_1, V_2 denote the corresponding input random variables, then $I(T \wedge V_1, V_2) = 1/2$ and $I(Z \wedge V_1, V_2) = 0$, so $R_0 + R_1 + R_2$ may be positive.

We conjecture this behavior to also be observable for the true capacity region of wiretap MACs. The relation to the wiretap MAC with conferencing encoders mentioned in the introduction will then imply that base station cooperation may enable secret transmission where this is not possible without.

Acknowledgment

This work was partly supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050 and by the German Research Foundation (DFG) under Grant BO 1734/25-1.

References

[1] I. Bjelaković, H. Boche, J. Sommerfeld, "Secrecy Results for Compound Wiretap Channels", achievable at http://arxiv.org/abs/1106.2013, 2011.

[2] M.R. Bloch, J.N. Laneman, "Secrecy from Resolvability", submitted to *IEEE Trans. Inf. Theory*, achievable at http://arxiv.org/abs/1105.5419, 2011.

[3] N. Cai, A. Winter, R.W. Yeung, "Quantum Privacy and Quantum Wiretap Channels", *Probl. Inf. Transm*, vol. 40, no. 4, pp. 318–336, 2004.

[4] I. Csiszár, "Almost Independence and Secrecy Capacity", *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, 1996.

[5] I. Csiszár, J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd edition, Cambridge: Cambridge University Press, 2011.

[6] I. Csiszár, J. Körner, "Broadcast Channels with Confidential Messages", *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, 1978.

[7] I. Devetak, "The Private Classical Capacity and Quantum Capacity of a Quantum Channel", *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[8] E. Ekrem, S. Ulukus, "Effects of Cooperation on the secrecy of Multiple Access Channels with Generalized Feedback", *Proc. Conf. on Inf. Sciences and Systems (CISS)*, pp. 791–796, Princeton, NJ, March 2008.

[9] E. Ekrem, S. Ulukus, "On the Secrecy of Multiple Access Wiretap Channel", *Proc. Allerton Conference*, pp. 1014–1021, Allerton House, UIUC, IL, USA, Sept. 2008.

[10] R. Liu, Y. Liang, H.V. Poor, "Fading Cognitive Multiple-Access Channels With Confidential Messages", submitted to *IEEE Trans. Inf. Theory*, achievable at http://arxiv.org/abs/0910.4613, 2009.

[11] Y. Liang, H.V. Poor, "Multiple-Access Channels With Confidential Messages", *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[12] R. Liu, I. Marić, R.D. Yates, P. Spasojević, "The Discrete Memoryless Multiple-Access Channel with Confidential Messages", *Proc. Int. Symp. Inf. Theory*, pp. 957–961, Seattle, USA, July 2006.

[13] U.M. Maurer, S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free", *Advances in Cryptology – Eurocrypt 2000, Lecture Notes in Computer Science*, vol. 1807, pp. 351–368, 2000.

[14] O. Simeone, A. Yener, "The Cognitive Multiple Access Wire-Tap Channel", *Proc. Conf. on Inf. Sciences and Systems (CISS)*, Baltimore, NJ, USA, March 2009.

[15] D. Slepian and K. Wolf, "A coding theorem for multiple access channels with correlated sources", *Bell System Techn. J.*, vol. 52, no. 7, 1037–1076, 1973.

[16] X. Tang, R. Liu, P. Spasojević, H. V. Poor, "Multiple Access Channels with Generalized Feedback and Confidential Messages", *Proc. Inf. Theory Workshop*, pp. 608–613, Lake Tahoe, CA, USA, Sept. 2007.

[17] M. van Dijk, "On a Special Class of Broadcast Channels with Confidential Messages", *IEEE Trans. Inf. Theory*, vol. 43, no. 2, 1997.

[18] F.M.J. Willems, "The Discrete Memoryless Multiple Access Channel with Partially Cooperating Encoders", *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 441–445, 1983.

[19] A. Wyner, "The Wire-Tap Channel", *The Bell System Tech. J.*, vol. 54, no. 8, pp 1355–1387, 1975.