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.

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 Alice₁ and Alice₂ 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 codeword is decoded.

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 $K := \{1, \ldots , K\}$ for positive integers $K$. $[x]_+ := \max(x, 0)$. $\mathcal{P}(\mathcal{X})$ are the probability measures on the finite set $\mathcal{X}$, and for measures $\mu_1, \mu_2$ on $\mathcal{X}$, we define the metric $\|\mu_1 - \mu_2\| := \sum_{x \in \mathcal{X}} |\mu_1(x) - \mu_2(x)|$. $\delta(x, \cdot)$ 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 $T^n_{X|U,\delta}(u)$ the $X|U$-typical $n$-sequences conditional on $u$ with constant $\delta$, see [5] for details.

II. SYSTEM MODEL AND MAIN RESULT

The encoders have the finite input alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, Bob’s alphabet is $\mathcal{Z}$, and Eve receives outputs from the alphabet $\mathcal{Z}$. The wiretap channel is memoryless, it is determined by a stochastic matrix $W: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{P}(\mathcal{Z})$ whose marginals are denoted by $W_T$ and $W_Z$, respectively.
The transmission of words \( \mathbf{x} \in \mathcal{X}^n \) and \( \mathbf{y} \in \mathcal{Y}^n \) is governed by the probabilities

\[
W^\otimes n(\mathbf{t}, \mathbf{z}|\mathbf{x}, \mathbf{y}) = \prod_{i=1}^n W(t_i, z_i|x_i, y_i), \quad (\mathbf{t}, \mathbf{z}) \in \mathcal{I}^n \times \mathcal{X}^n.
\]

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. This means that the set \([K_0], [K_1], [K_2]\) for the common and the private messages, respectively, is governed by a stochastic matrix \(G: [K_0] \times [K_1] \times [K_2] \to \mathcal{P}(\mathcal{X}^n \times \mathcal{Y}^n)\) which has the form

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

Here \( \mathcal{J} \) 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

\[
\log K_{\nu} \geq n(R_\nu - \varepsilon) \quad (\nu = 0, 1, 2),
\]

\[
P[\phi(T^n) \neq (M_0, M_1, M_2)] \leq \varepsilon,
\]

\[
I(M_0, M_1, M_2 \land Z^n) \leq \varepsilon,
\]

where the \( M_\nu \) are uniformly distributed on \([K_\nu]\) \((\nu = 0, 1, 2)\), where \( \phi \) 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 \( \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2 \) be finite alphabets and let \( U, (V_1, V_2), (X, Y), (T, Z) \) be a Markov chain with \( U \) taking values in \( \mathcal{X} \), with \( V_1, V_2 \) taking values in \( \mathcal{Y}_1 \) and \( \mathcal{Y}_2 \) and independent conditional on \( U \), with \( X \) only depending on \( V_1 \) and \( Y \) only depending on \( V_2 \) and with \( P_{T,Z|X,Y} = W \).

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 \( I(Z \land U) < H_C \leq \min\{I(Z \land V_1, U), I(Z \land V_2, U)\} \).

For \( H_C > 0 \), let \( \Pi_{H_C} \) be the set of \( p \) that additionally satisfy

\[
I(Z \land V_1, U) \leq I(T \land V_1|V_2, U), \tag{1}
\]

\[
I(Z \land V_2, U) \leq I(T \land V_2|V_1, U), \tag{2}
\]

\[
I(Z \land V_1, V_2|U) \leq I(T \land V_1, V_2|U) + I(Z \land V_2|V_1, U), \tag{3}
\]

\[
I(Z \land V_1, V_2) \leq I(T \land V_1, V_2). \tag{4}
\]

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

\[
R_1 \leq I(T \land V_1|V_2, U) - I(Z \land V_1|U)
\]

\[
- [I(Z \land V_2|V_1, U) - I(T \land V_2|V_1, U)]^+,
\]

\[
R_2 \leq I(T \land V_2|V_1, U) - I(Z \land V_2|U)
\]

\[
- [I(Z \land V_1|V_2, U) - I(T \land V_1|V_2, U)]^+,
\]

\[
R_0 + R_1 \leq I(T \land V_1, V_2|U) - I(Z \land V_1, V_2|U),
\]

\[
R_0 + R_1 \leq I(T \land V_1, V_2) - I(Z \land V_1, V_2).
\]

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

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

where \( \text{conv} \) is the convex hull operator.

**III. THE PROOF**

Using [5, Lemma 2.7], one has

\[
I(Z^n \land M_0, M_1, M_2) \leq -\eta \log \frac{\eta}{|\mathcal{X}|^{K_0K_1K_2}},
\]

where \( \eta = \|P_{Z^n|0} \otimes P_{M_0,M_1,M_2} - P_{Z^n|0} \otimes P_{M_0,M_1,M_2}\| \). Thus if \( \eta \) tends to zero exponentially and if the \( K_\nu \) do not grow faster than exponentially, then \( I(Z^n \land M_0, M_1, M_2) \) also tends to zero exponentially. If there is a measure \( \theta \) on \( \mathcal{X}^n \) satisfying

\[
\|P_{Z^n|0} - \theta\| \leq 2^{-n\beta} \tag{5}
\]

for some \( \beta > 0 \) uniformly in \( k_0, k_1, k_2 \), then \( \eta \) is exponentially small, because

\[
\eta = \frac{1}{K_0K_1K_2} \sum_{k_0,k_1,k_2} \|P_{Z^n|k_0,k_1,k_2} - \theta\| \leq 2 \cdot 2^{-n\beta}. \]

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 \( \{(U^n_{k_0}, X^{l_1}_{k_0,k_1}, Y^{l_2}_{k_0,k_2})\} \) be given, where \( k_0, k_1, k_2 \) are message sets and \( l_\nu \in [L]\), \( \nu = 0, 1, 2 \) are indices needed in stochastic encoding. The \( U^n_{k_0} \) are i.i.d. on \( \mathcal{X}^n \) according to

\[
P_{U^n_{k_0}}(u) := \frac{P_{U^n_{k_0}}(u)}{P_{U^n_{k_0}}(T^n_{U',\delta})},
\]

for some \( \delta > 0 \). For any \( k_0, l_0 \), given \( U^n_{k_0} = u \), the \( X^{l_1}_{k_0,k_1} \) are conditionally i.i.d. on \( \mathcal{X}^n \) according to

\[
P_{X^{l_1}_{k_0,k_1}|U^n_{k_0}}(x|u) := \frac{P_{X^{l_1}_{k_0,k_1}|U^n_{k_0}}(x|u)}{P_{X^{l_1}_{k_0,k_1}|U^n_{k_0}}(x|u)},
\]

Then we define the rate set \( \mathscr{R}(p) \) as the set of triples of
and the $Y^{l_{02}}_{k_{0}k_{2}}$ on $\mathcal{Y}^{n}$ according to $P^{y^{l_{02}}}_{X_{l_{0}}^{l_{02}}|U^{n}}$, which is defined analogously to $P^{x^{l_{02}}}_{X_{l_{02}}^{l_{02}}|U^{n}}$ with $x$ replaced by $y$ and $X$ replaced by $Y$. Following Devetak's approach [7], we obtain the following bounds (6)-(8) on the $L_{\nu}$ that need to be satisfied to establish (5):

$$\log L_{0} \geq n(I(Z \cup U) + 4\tau),$$

$$\log L_{1} \geq n(I(Z \setminus X|Y, U) + 4\tau),$$

$$\log L_{2} \geq n(I(Z \setminus Y|U) + 4\tau).$$

An alternative triple of bounds (6')-(8') can be obtained with $X$ and $Y$ exchanged. $\tau$ depends on $\delta$ and $\tau \xrightarrow{\delta \to 0} 0$. (6)-(8) and (6')-(8') ensure that the probability of obtaining a realization of the random variables $U^{l_{0}}, X^{l_{01}}, Y^{l_{02}}$ 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 $\mu_{i} := \mathbb{E}[X_{i}]$ and $\mu := \frac{1}{L}\sum_{i=1}^{L} \mu_{i}$, one has

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

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 $X^{l_{01}}_{k_{0}l_{1}}$ are i.i.d. given $U^{l_{0}}$, and that $Y^{l_{02}}_{k_{0}k_{2}}$ are i.i.d. given the $U^{l_{0}}$ and the $U^{l_{0}}$ 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 $(k_{0}, l_{1}, k_{2})$, the corresponding random variables exhibit the same behavior. We pick one $(k_{0}, l_{1}, k_{2})$ and omit these indices here. Starting with (7), let $(u, y) \in T_{u}^{n}Y_{Z_{2}}$ and

$$E_{1}(u, x, y) := \{ z \in T_{Z_{2}}^{n}Y_{Z_{2}}x: |z - y| \leq 2^{-n(I(Z|X, Y) - \tau)} \},$$

This will give a bound on the random variables corresponding to the $b$ from Lemma 2, $\tau > 0$ is chosen later when $\|P_{Z_{k_{0}l_{1}k_{2}}|X_{k_{0}l_{1}k_{2}} - \theta}\|$ is estimated. Define

$$\theta^{u}_{xy}(z) := \mathbb{E}[W^{\mu}_{Z_{k_{0}}|X_{k_{0}}, Y_{k_{0}}}|x, u, X_{k_{0}}, Y_{k_{0}}]_{u, x, y} \mu_{1} = u, \mu_{2} = u],$$

$$F_{1}(u, y) := \{ z \in T_{Z_{2}}^{n}Y_{Z_{2}}x: |z - y| \leq 2^{-n(I(Z|X, Y) - \tau)} \}$$

and $U_{xy} := \{ z \in F_{1}(u, y) \}$ This will provide a lower bound on the mean of the random variables used. We set $E_{2}(u, x, y) := E_{1}(u, x, y) \cap F_{1}(u, y)$. For every $z \in \mathbb{Z}^{n}$ and every $(l_{0}, l_{2})$, let $A_{1}(l_{0}, l_{2}, z)$ be the event that

$$\frac{1}{L_{1}} \sum_{l_{2}} W_{Z}^{n}(z: X^{l_{01}}_{l_{0}}, Y^{l_{02}}_{l_{2}})_{1}E_{2}(U^{l_{0}}, X^{l_{01}}, Y^{l_{02}})(z) \in [(1 \pm \varepsilon)\theta^{u}_{U^{l_{0}}, Y^{l_{02}}}(z)].$$

Then, conditioning on all possible realizations of $U^{l_{0}}, Y^{l_{02}}$ adn applying the law of total probability, one obtains with Lemma 2 for $n$ sufficiently large

$$\mathbb{P}[A_{1}(l_{0}, l_{2}, z)] \leq 2 \exp\left(-L_{1} \cdot \frac{\varepsilon^{3}2^{n-2n(I(Z|X, Y, U) + 2\tau)} - 2\ln 2}{2\ln 2}\right).$$

We denote the intersection of all $A_{1}(l_{0}, l_{2}, z)$ as $l_{0}, l_{2}$ and $z$ are varied by $A_{1}$.

Next we turn to (8). Define

$$\theta_{u}(z) := \mathbb{E}[W^{\mu}_{Z_{k_{0}}|X_{k_{0}}, Y_{k_{0}}}|x, u, X_{k_{0}}, Y_{k_{0}}]_{u, x, y} \mu_{1} = u, \mu_{2} = u],$$

$$F_{2}(u, y) := \{ z \in T_{Z_{2}}^{n}Y_{Z_{2}}y: |z - y| \leq 2^{-n(I(Z|X, Y) + 2\tau)} \}.$$
Here we again use the law of total probability. The first two terms in (11) come from the bound on $\mathbb{P}[A_2(l_0, x)']$. The third term results from an application of Lemma 2 to the $L_0$ random variables appearing in the definition of $A_0(z)$ which are i.i.d. conditional on $A_2(z)$ with respect to $\mathbb{P}_x$. We denote the intersection of all $A_0(z)$ 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 $A_s(l_0, l_2)$ be defined by

$$A_s(l_0, l_2) := \{ (l_0, l_1) : (X^{l_0 l_1}, Y^{l_0 l_2}, U^{l_0}) \} \geq (1 - \varepsilon)(1 - 2 \cdot 2^{-n\beta})L_1 \}.$$ 

Then

$$\mathbb{P}[A_s(l_0, l_2)] \leq \exp \left(-L_1 \cdot \frac{\varepsilon^2(1 - 2 \cdot 2^{-n\beta})}{2 \ln 2} \right). \tag{12}$$

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

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 $\mathcal{R}(p)$ defined by

$$\tilde{R}_1 \leq I(T \cup X \cup Y, U),$$

$$\tilde{R}_2 \leq I(T \cup Y \cup X, U),$$

$$\tilde{R}_1 + \tilde{R}_2 \leq I(T \cup X, Y, U).$$

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

In particular, this requires $(1/n)(\log(L_0) + \eta, \log(L_1) + \eta, \log(L_2) + \eta) \in \mathcal{R}(p)$. This does not have to be true for the vector $I^{(1)} := I(Z \cup U, I(Z \cup X | Y, U), I(Z \cup Y | U))$ nor its analog $I^{(2)}$ with the roles of $X$ and $Y$ exchanged. However, a convex combination of the two might be contained in $\mathcal{R}(p)$. 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 $[K^{(1)}_0; K^{(1)}_0]$ and $[K^{(2)}_0; L^{(2)}_0]$, respectively ($\nu = 0, 1, 2$). For the first of these families, we know $A_s \cap A_0 \cap A_1 \cap A_2$ 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 $G^{(1)}_0, G^{(2)}_0$. They are defined analogously. For $G^{(\nu)}_0$ set $\mathcal{G}^{(\nu)}_0 = \{L^{(\nu)}_0\}$ and $G^{(\nu)}_0(T^{(\nu)}_0, k^{(\nu)}_0) := 1/L^{(\nu)}_0$. Given $k^{(\nu)}_0, l^{(\nu)}_0, n^{(\nu)}_0$, Alice 1 chooses the codeword $X^{l^{(\nu)}_0}$ with probability $1/L^{(\nu)}_0$ and Alice 2 independently of Alice 1 chooses $Y^{l^{(\nu)}_0}$ with probability $1/L^{(\nu)}_0$. For $\delta$ small and $L_0 = L^{(\nu)}_0$, close to its bound (6), the encoder satisfies the common randomness restriction because of $I(Z \cup U) < H_{\nu}$. Bob can still decode all messages from the Alice 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

$$R_1 \approx I(T \cup X | Y, U) - \alpha I(Z \cup X | Y, U)$$

$$- (1 - \alpha)I(Z \cup Y | U),$$

$$R_2 \approx I(T \cup Y | X, U) - \alpha I(Z \cup Y | U)$$

$$- (1 - \alpha)I(Z \cup X | Y, U),$$

$$R_1 + R_2 \approx I(T \cup X, Y | U) - I(Z \cup X, Y | U),$$

$$R_1 + R_2 \approx I(T \cup X, Y | U) - I(Z \cup X, Y | U).$$

We denote the rate region defined by the bounds on the right-hand side by $\mathcal{R}_{\alpha}(p)$. 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 $Y^{\nu} := (1/L_0, L_0) \sum$ and $W := W_{\nu}^{Z,n}$ for brevity. We have for every $(k_0, k_1, k_2)$

$$\|P_{Z^n | k_0 k_1 k_2} - \theta\|_{\text{TV}} \leq \|\theta - \sum_{l_0, l_1, l_2} W(\cdot | x^{l_0 l_1}, y^{l_0 l_2}) \| E_0(u^{l_0 l_1}_0, x^{l_0 l_2}_0, y^{l_0 l_2}_0) F_0^l \|

+ \sum_{l_0, l_1, l_2} W(\cdot | x^{l_0 l_1}, y^{l_0 l_2}) \| E_0(u^{l_0 l_1}_0, x^{l_0 l_1}_0, y^{l_0 l_2}_0) F_0^l \|

+ \sum_{l_0, l_1, l_2} W(\cdot | x^{l_0 l_1}, y^{l_0 l_2}) \| E_2(u^{l_0 l_1}_0, y^{l_0 l_1}_0, x^{l_0 l_2}_0) F_2(u^{l_0 l_2}_0) \|

+ \sum_{l_0, l_1, l_2} W(\cdot | x^{l_0 l_1}, y^{l_0 l_2}) \| E_2(u^{l_0 l_1}_0, y^{l_0 l_2}_0, x^{l_0 l_2}_0) F_2(u^{l_0 l_2}_0) \|

+ \sum_{l_0, l_1, l_2} W(\cdot | x^{l_0 l_1}, y^{l_0 l_2}) \| E_2(u^{l_0 l_1}_0, y^{l_0 l_2}_0, x^{l_0 l_2}_0) - P_{Z^n | k_0 k_1 k_2} \|

We denote the five terms by $I-V$ in that order. $I$ is at most $\varepsilon$ 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 $A_s$ is satisfied. Altogether this gives an upper bound on (5) of $20 \cdot \varepsilon + 5 \cdot 2^{-n\beta}$. 


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 \( \mathcal{R}_{\alpha}(p) \) is achievable for those \( \alpha \) satisfying

\[
\alpha I^{(1)} + (1 - \alpha) I^{(2)} \in \mathcal{R}(p).
\]

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

\[
\begin{align*}
R_1 &\leq I(T \wedge X|Y,U) - \alpha_0 I(Z \wedge X|Y,U) \\
&\quad - (1 - \alpha_0) I(Z \wedge X|U), \quad (13) \\
R_2 &\leq I(T \wedge Y|X,U) - \alpha_1 I(Z \wedge Y|U) \\
&\quad - (1 - \alpha_1) I(Z \wedge Y|U), \quad (14) \\
R_1 + R_2 &\leq I(T \wedge X,Y|U) - I(Z \wedge X,Y|U), \quad (15) \\
R_0 + R_1 + R_2 &\leq I(T \wedge X,Y) - I(Z \wedge X,Y), \quad (16)
\end{align*}
\]

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

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

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

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 \( I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2) \leq 0 \) 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 \( \mathcal{X} = \mathcal{Y} = \{0,1\} \), \( \mathcal{Z} = GF(3) \), \( \mathcal{X} = \{0, 2, \ldots, 3 \} \), 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

\[
t = x + y + N_1, \quad z = 2x - 2y + N_2.
\]

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