Secret Key Capacity For Multipleaccess Channel With Public Feedback

Himanshu Tyagi*

Shun Watanabe†

***Abstract*—We consider the generation of a secret key (SK) by the inputs and the output of a secure multipleaccess channel (MAC) that additionally have access to a noiseless public communication channel. Under specific restrictions on the protocols, we derive various upper bounds on the rate of such SKs. Specifically, if the public communication consists of only the feedback from the output terminal, then the rate of SKs that can be generated is bounded above by the maximum symmetric rate R_f^* in the capacity region of the MAC with feedback. On the other hand, if the public communication is allowed only before and after the transmission over the MAC, then the rate of SKs is bounded above by the maximum symmetric rate R^* in the capacity region of the MAC without feedback. Furthermore, for a symmetric MAC, we present a scheme that generates an SK of rate R_f^*, improving the best previously known achievable rate R^*. An application of our results establishes the SK capacity for adder MAC, without any restrictions on the protocols.**

I. INTRODUCTION

What is the largest rate of a *secret key* (SK) that can be generated by the inputs and the output of a secure *multipleaccess channel* (MAC) with a public feedback from the output? We show that this rate is bounded above by

$$R_f^* = \max \{R : (R, R) \in \mathcal{C}_{\mathtt{MACFB}}\}, \tag{1}$$

where $\mathcal{C}_{\mathtt{MACFB}}$ denotes the capacity region[1] of the MAC with feedback. In fact, for a MAC that is symmetric with respect to its inputs, this largest SK rate is equal to R_f^*.

Previously, Csiszár and Narayan [6] presented two different protocols to establish SKs of rate

$$R^* = \max \{R : (R, R) \in \mathcal{C}_{\mathtt{MAC}}\}, \tag{2}$$

where $\mathcal{C}_{\mathtt{MAC}}$ denotes the capacity region of the MAC without feedback. In both the protocols, the inputs of the MAC were selected without any knowledge of the previous outputs. Such protocols are reminiscent of SK generation in source models [4] and will be collectively referred to as source emulation[2]. We show that R^* is the best rate of an SK that can be generated using such simple protocols. Since for symmetric MACs we generate an SK of rate R_f^*, it follows that complex protocols that select inputs of the MAC based on the feedback from the output can outperform source emulation. This answers a question raised in [6, Section VII].

In general, the inputs of the MAC can be selected based on interactive public communication from all the terminals after each transmission over the secure MAC. For this set-up, Csiszár and Narayan established an upper bound for the largest rate of an SK [6], termed the SK capacity and denoted by C. Moreover, for the special case of MACs in the Willem's class [12], this upper bound was improved and it was shown that $C \leq R_f^*$. Therefore, for symmetric MACs in the Willem's class, our aforementioned results imply $C = R_f^*$. This class of channels includes adder MAC, which settles an open problem posed in [6, Example 2].

One of the rate R^*-achieving schemes in [6] involves transmitting messages M_1, M_2 of rates (R^*, R^*) over the MAC and communicating the modulo sum $M_1 \oplus M_2$ over the public channel, resulting in an SK of rate R^*; either M_1 or M_2 constitutes the SK. It was remarked in [6, page 21] that an SK generation protocol with "*full feedback is ruled out as the feedback communication is public. Still, if a coding scheme with partial feedback could be found by which the gain in transmission rates exceeds the information leakage due to feedback, it would lead to an SK rate greater than*" R^*. Following this clue, our achievability scheme for symmetric MACs entails communicating compressed output sequences over the public channel and then extracting an SK of rate R_f^* from the output sequence. One difficulty is the lack of a single-letter expression for R_f^*. However, this is circumvented by converting the transmission schemes for MAC directly into SK generation protocols, without recourse to the single-letter rate achieved. In fact, our approach implies that any message transmission scheme of rates (R, R) for a symmetric MAC can be used to generate an SK of rate R, with appropriate modifications.

Our converse proofs rely on a general converse[3] for the SK generation problem in a multiterminal source model, which in

*Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. Email: tyagi@umd.edu

†Department of Information Science and Intelligent Systems, University of Tokushima, Tokushima 770-8506, Japan, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. Email: shun-wata@is.tokushima-u.ac.jp

Himanshu Tyagi was supported by the U.S. National Science Foundation under Grants CCF0830697 and CCF1117546.

[1]Throughout this paper, the capacity region of the MAC is for the average probability of error criterion.

[2]Our source emulation protocols include the generalized source emulation of [6], [3] as a special case; the latter restricts the MAC inputs for different channel uses to be *independent and identically distributed* (i.i.d.).

[3]This general converse is due to Prakash Narayan, who agreed to publish it in this paper.

turn is a simple consequence of a basic property of interactive communication that was established in [5, Lemma B.1] (see, also, [8]). Here, too, the challenge posed by the lack of single-letter expressions is handled by working directly with n-letter expressions.

The problem formulation and our main results are stated formally in the following section. Sections III and IV contain the necessary tools that are used in our converse proofs in Section V. The final section contains a discussion of our results and the properties of interactive communication that are used to derive them.

II. Problem Formulation and Main Results

Consider a MAC with two inputs[4] $\mathcal{X}_1$ and $\mathcal{X}_2$, and an output $\mathcal{X}_3$, specified by a DMC $W : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{X}_3$. We study a secrecy generation problem for three terminals: terminals 1 and 2 govern the inputs to the DMC over which they transmit, respectively, sequences $\mathbf{x}_1$ and $\mathbf{x}_2$ of length n, while terminal 3 observes the corresponding n length output $\mathbf{x}_3$. Between two consecutive transmissions, the terminals communicate with each other interactively over a noiseless public communication channel of unlimited capacity. While the transmissions over the DMC W are secure, the public communication is observed by all the terminals as well as a (passive) eavesdropper. This model is a special case of a general model for secrecy generation over channels introduced by Csiszár and Narayan in [6] (see also [5]). In the manner of [6], the messages sent over W will be referred to as transmissions and those sent over the public channel will be referred to as communication.

Formally, assume that at the outset terminal i generates rv U_i, $i = 1, 2, 3$, to be used for (local) randomization; the rvs U_1, U_2, U_3 are mutually independent. The *communication-transmission protocol* can be divided into $n+1$ time slots. In the first n time slots, the terminals communicate interactively over the public channel, followed by a transmission over the secure DMC. The protocol ends with a final round of interactive public communication in slot $n+1$. Specifically, in time slot t, $1 \leq t \leq n$, the terminals communicate interactively using their respective local randomization U_1, U_2, U_3 and observations upto time slot $t-1$; the overall interactive communication in slot t is denoted by

$$F_t = F_t\left(U_1, U_2, U_3, X_3^{t-1}, F^{t-1}\right) \tag{3}$$

Subsequently, the inputs $X_{1t} = X_{1t}(F^t, U_1)$ and $X_{2t} = X_{2t}(F^t, U_2)$ are transmitted by terminals 1 and 2, respectively, and X_{3t} is observed by terminal 3. Finally, the last round of interactive communication $F_{n+1} = F_{n+1}\left(U_1, U_2, U_3, X_3^n, F^n\right)$ is sent over the public channel. For convenience, we denote $\mathbf{F} = (F_1, ..., F_{n+1})$.

After the communication-transmission protocol ends, the terminals 1, 2, 3, respectively, form estimates K_1, K_2, K_3 as follows:

$$K_i = K_i(U_1, \mathbf{F}), \quad i = 1, 2, 3. \tag{4}$$

[4]Our results in this paper can be extended to the multiple input case. See Section VII.

An rv K with range $\mathcal{K}$ constitutes an ϵ-SK if the following two conditions are satisfied (c.f. [4]):

$$\mathrm{P}\left(K_1 = K_2 = K_3 = K\right) \geq 1 - \epsilon, \tag{5}$$

$$\begin{aligned} s_{in}(K; \mathbf{F}) &:= \log|\mathcal{K}| - H(K \mid \mathbf{F}) \\ &= D\left(\mathrm{P}_{K\mathbf{F}} \| \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}}\right) \\ &\leq \epsilon, \end{aligned} \tag{6}$$

where $\mathrm{P}_{\mathtt{unif}}$ is the uniform distribution on $\mathcal{K}$. The first condition above represents reliable *recoverability* of the SK and the second guarantees its *security*. While our achievability proofs establish SKs that satisfy the "strong secrecy" condition (6), our converse results are valid for SKs satisfying the weaker secrecy condition given below:

$$\frac{1}{n} s_{in}(K; \mathbf{F}) \leq \epsilon. \tag{7}$$

Definition 1. A number $R \geq 0$ is an achievable SK rate if for every $\epsilon > 0$, there exist local randomization U_1, U_2, U_3, communication-transmission protocol $\mathbf{F}$ and ϵ-SK K with

$$\frac{1}{n}\log|\mathcal{K}| \geq R,$$

for all n sufficiently large.

The supremum of all achievable SK rates is called the SK capacity, denoted by C.

The general problem of characterizing C remains open. In [6], general lower bounds and upper bounds for C were given; we state the former next, specialized for the case of two input MAC.

Theorem 1. *[6] The SK capacity for a MAC is bounded below as*

$$C \geq R^*. \tag{8}$$

For the special case $W(x_3 \mid x_1, x_2) = \mathbb{1}\left(x_3 = x_1 \oplus x_2\right)$, the lower bound above is tight and $C = R^*$ [6, Example 1]. Also, for the case when W is in the Willem's class of MACs [12], an upper bound for C was derived in [6]. Willem's class consists of MAC where one of the inputs, say input 1, is determined by the output and the other input, i.e., for some mapping $\phi : \mathcal{X}_2 \times \mathcal{X}_3 \to \mathcal{X}_1$, $W(x_3 \mid x_1, x_2) = 0$ if $x_1 \neq \phi(x_2, x_3)$. The following result holds.

Theorem 2. *[6] For a MAC in the Willem's class,*

$$C \leq R_f^*. \tag{9}$$

In this paper, we show that the bounds (8) and (9) are tight under various restrictions imposed on the MAC and the communication-transmission protocols. We first describe the specific restrictions we place. As in Definition 1, define the SK capacity with *source emulation* [5], [6], [3], denoted by $C_{\mathtt{SE}}$, as the supremum of all achievable SK rates with the additional restriction that

$$F_t = \text{constant}, \quad 2 \leq t \leq n,$$

i.e., the transmission input sequences for the MAC are selected solely based on the initial interactive communication F_1 and local randomization at the input terminals, without any feedback from the output. Next, define the SK capacity with *no input communication*, denoted by $C_{\texttt{NIC}}$, as the supremum of all achievable SK rates with the additional restriction that following the first round interactive communication F_1, the subsequent communication $F_2, ..., F_n$ are only from the output terminal, i.e.,

$$F_t = F_t\left(U_3, X_3^{t-1}, F^{t-1}\right), \quad 2 \leq t \leq n.$$

The following inequalities ensue:

$$C_{\texttt{SE}} \leq C_{\texttt{NIC}} \leq C.$$

We now state our main results. First, we show a general upper bound on $C_{\texttt{NIC}}$.

Theorem 3. *The SK capacity with no input communication is bounded above as*

$$C_{\texttt{NIC}} \leq R_f^*.$$

Next, we show that for the class of symmetric MACs, this upper bound is tight.

Theorem 4. *For a symmetric MAC with $\mathcal{X}_1 = \mathcal{X}_2$ and*

$$W(x_3 \mid x_1, x_2) = W(x_3 \mid x_2, x_1),$$

the SK capacity with no input communication is given by

$$C_{\texttt{NIC}} = R_f^*.$$

As a corollary, we characterize C for adder MAC, for which lower and upper bounds were reported in [6, Example 2].

Corollary. *For $W(x_3|x_1, x_2) = \mathbb{1}(x_3 = x_1 + x_2)$, the SK capacity is given by*

$$C = R_f^*.$$

Since adder MAC is in the Willem's class and is symmetric, the corollary follows from Theorem 2 and Theorem 4.

Finally, the following result implies that source emulation does not suffice to generate SKs of rate R_f^* and the complex communication-transmission protocols above are needed necessarily in Theorem 4.

Theorem 5. *The SK capacity with source emulation is given by*

$$C_{\texttt{SE}} = R^*.$$

The inequality $C_{\texttt{SE}} \geq R^*$ was shown in [6]. We show the reverse inequality in Section V.

Remark. Theorem 5 is a further strengthening of [6, Proposition 5] where this result was established for source emulation protocols that restrict the inputs of the MAC for different channel uses to be i.i.d. We show that the inequality $C_{\texttt{SE}} \leq R^*$ holds even when this restriction is dropped.

III. A General Converse for SK Capacity of a Multiterminal Source

In this section, we present a converse for an SK generation problem in a multiterminal source model with m sources (c.f. [4]) that does not require the underlying sources to be i.i.d. This converse result is due to Prakash Narayan and it relies on a basic property of interactive communication in multiterminal models.

Terminals $1, ..., m$ observe correlated rvs $Y_1, ..., Y_m$, respectively; for brevity we denote by $\mathcal{M}$ the set $\{1, ..., m\}$ and by Y_A the rvs $\{Y_i, i \in A\}$ for $A \subseteq \mathcal{M}$. The terminals communicate over a public channel, possibly interactively in several rounds. Specifically, terminal i sends communication F_{ij} in the jth round, $1 \leq j \leq r$, where F_{ij} depends on the observation Y_i and the previously received communication

$$F_{11}, ..., F_{m1}, ..., F_{1j}, ..., F_{(i-1)j}.$$

We denote the overall interactive communication by $\mathbf{F}$. Consider an rv K taking values in $\mathcal{K}$ such that

$$\mathrm{P}\left(K = K_i(Y_i, \mathbf{F}),\, i \in \mathcal{M}\right) \geq 1 - \epsilon, \tag{10}$$

for $0 < \epsilon < 1$ and some mappings K_i of $(Y_i, \mathbf{F})$, i.e., the terminals form estimates of K using their respective observations Y_i and the interactive communication $\mathbf{F}$ that agree with K with probability greater than $1 - \epsilon$. We present below an upper bound on $\log|\mathcal{K}|$. The following notations will be used: Let $\mathcal{B}$ be a collection of subsets of $\mathcal{M}$ given by

$$\mathcal{B} = \{B : B \subsetneq \mathcal{M}, B \neq \emptyset\}.$$

A collection $\lambda = \{\lambda_B : B \in \mathcal{B}\}$ constitutes a fractional partition of $\mathcal{M}$ (c.f. [5]) if

$$\sum_{B \in \mathcal{B}: i \in B} \lambda_B = 1, \quad \text{for all } i \in \mathcal{M}.$$

Consider a partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\mathcal{M}$. Corresponding to this partition, we define a fractional partition λ^π as follows:

$$\lambda_B^\pi = \begin{cases} \frac{1}{k-1}, & B = \pi_i^c,\ 1 \leq i \leq k, \\ 0, & \text{otherwise}. \end{cases} \tag{11}$$

First, we present a key property of interactive communication that underlies all the converse proofs of this paper.

Lemma 6 (*Interactive Communication Property*)**.** *[5] For an interactive communication $\mathbf{F}$, we have*

$$H(\mathbf{F}) \geq \sum_{B \in \mathcal{B}} \lambda_B H\left(\mathbf{F} \mid Y_{B^c}\right),$$

for every fractional partition λ of $\mathcal{M}$.

The following result is, in effect, a "single-shot" converse for the SK generation problem.

Theorem 7. *[9] For an rv K and interactive communication $\mathbf{F}$ satisfying (10), we have*

$$\log|\mathcal{K}| \leq H\left(Y_{\mathcal{M}}\right) - \sum_{B \in \mathcal{B}} \lambda_B H\left(Y_B \mid Y_{B^c}\right) + s_{in}(K; \mathbf{F}) + \nu,$$

for every fractional partition λ of $\mathcal{M}$, where $\nu = (m+2)(\epsilon \log |\mathcal{K}| + h(\epsilon))$.

Proof. It follows from [5, Lemma A.2] that

$$\begin{aligned} H(K \mid \mathbf{F}) &\leq H\left(Y_{\mathcal{M}} \mid \mathbf{F}\right) - \sum_{B\in\mathcal{B}} \lambda_B H\left(Y_B \mid Y_{B^c}, \mathbf{F}\right) + \nu, \\ &= H\left(Y_{\mathcal{M}}\right) - \sum_{B\in\mathcal{B}} \lambda_B H\left(Y_B \mid Y_{B^c}\right) \\ &\quad - \left[H(\mathbf{F}) - \sum_{B\in\mathcal{B}} \lambda_B H\left(\mathbf{F} \mid Y_{B^c}\right)\right] + \nu, \end{aligned}$$

which, along with Lemma 6 and the definition of $s_{in}(K;\mathbf{F})$ in (6), completes the proof. □

Corollary. *For K and $\mathbf{F}$ as in Theorem 7, we get*

$$\log|\mathcal{K}| \leq \frac{1}{k-1} D\left(\mathrm{P}_{Y_{\mathcal{M}}} \middle\| \prod_{i=1}^{k} \mathrm{P}_{Y_{\pi_i}}\right) + s_{in}(K;\mathbf{F}) + \nu,$$

for every partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\mathcal{M}$.

The corollary follows upon choosing $\lambda = \lambda^\pi$ in Theorem 7, where λ^π is given by (11).

IV. Maximum Symmetric Rate for MAC

While a single-letter expression for R^* is known [1], [7], for R_f^* such an expression is available only in special cases [12]. In this section, we will present n-letter characterizations for R^* and R_f^*, which will be used in our proofs in the next section.

Lemma 8. *For MAC with two inputs,*

$$\begin{aligned} R^* = \overline{\lim_n} \sup \min \Big\{ &\frac{1}{n} I\left(X_1^n \wedge X_3^n \mid X_2^n\right), \\ &\frac{1}{n} I\left(X_2^n \wedge X_3^n \mid X_1^n\right), \\ &\frac{1}{2n} I\left(X_1^n, X_2^n \wedge X_3^n\right) \Big\}, \end{aligned}$$

where the sup *is over all distributions $\mathrm{P}_{X_1^n X_2^n X_3^n} = \mathrm{P}_{X_1^n} \mathrm{P}_{X_2^n} W^n$.*

We omit the proof, which is a simple consequence of the capacity region for a MAC [1], [7].

Lemma 9. *For MAC with two inputs,*

$$\begin{aligned} R_f^* = \overline{\lim_n} \sup \min \Big\{ &\frac{1}{n} I\left(U_1 \wedge X_3^n, U_3 \mid U_2\right), \\ &\frac{1}{n} I\left(U_2 \wedge X_3^n, U_3 \mid U_1\right), \\ &\frac{1}{2n} I\left(U_1, U_2 \wedge X_3^n, U_3\right) \Big\}, \end{aligned} \tag{12}$$

where the sup *is over all joint distributions U_1, U_2, U_3, X_3^n of the randomization at the terminals and the output of the MAC that result from communication-transmission protocols with* no input communication *(as in the definition of $C_{\mathtt{NIC}}$).*

Proof. First, we claim that making additional independent common randomness U_3 available to the senders and the receiver does not improve the capacity region of a MAC. Indeed, let $\mathrm{P}_{\mathsf{err}}(u_3)$ be the error probability of the MAC W^n with feedback conditioned on $U_3 = u_3$. Clearly, there exists at least one realization u_3^* such that

$$\mathrm{P}_{\mathsf{err}}(u_3^*) \leq \mathbb{E}[\mathrm{P}_{\mathsf{err}}(U_3)].$$

Thus, using the encoders and decoders with $U_3 = u_3^*$ fixed we can achieve the same rate as that of the original scheme. In the remainder of the proof, without loss of generality, we will assume the availability of rv U_3 to the senders and the receiver of the MAC.

If $(R, R) \in \mathcal{C}_{\mathtt{MACFB}}$, then using standard manipulations and Fano's inequality we get

$$R \leq \frac{1}{n} I\left(U_1 \wedge X_3^n, U_3 \mid U_2\right) + \eta_n,$$

where U_1, U_2 are the messages sent by terminal 1 and 2, respectively, i.i.d. uniform over $\{1, ..., \lfloor 2^n R \rfloor\}$, and $\eta_n \to 0$ as $n \to \infty$. Also,

$$R \leq \frac{1}{n} I\left(U_2 \wedge X_3^n, U_3 \mid U_1\right) + \eta_n,$$

and

$$2R \leq \frac{1}{n} I\left(U_1, U_2 \wedge X_3^n, U_3\right) + \eta_n.$$

Since a code for MAC with feedback constitutes a valid communication-transmission protocol with local randomization U_1, U_2, U_3 at terminals 1, 2, 3, respectively, it follows that R_f^* is bounded above by the right-side of (12).

For the other direction, consider a MAC $W^{(n)} : \mathcal{U}_1 \times \mathcal{U}_2 \to \mathcal{X}_3^n \times \mathcal{U}_3$ given by

$$\begin{aligned} &W^{(n)}\left(x_3^n, u_3 \mid u_1, u_2\right) \\ &= \mathrm{P}\left(X_3^n = x_3^n, U_3 = u_3 \mid U_1 = u_1, U_2 = u_2\right). \end{aligned}$$

Then, by [1] and [7], the right-side of (12) is less than the maximum symmetric rate of the messages that can be transmitted reliably over this MAC (without feedback). To complete the proof we note that we can simulate $W^{(n)}$ by using the MAC W with feedback n times. Specifically, given a communication-transmission protocol with *no input communication* and fixed values u_1, u_2, u_3, choosing

$$\begin{aligned} X_{1t} &= X_{1t}\left(u_1, F^{t-1}\left(x_3^{t-1}, u_3\right)\right), \\ X_{2t} &= X_{2t}\left(u_2, F^{t-1}\left(x_3^{t-1}, u_3\right)\right), \quad 1 \leq t \leq n. \end{aligned}$$

simulates $W^{(n)}$. This is a valid choice of inputs since both the senders know the common randomness U_3 and the feedback signals X_3^{t-1} at time t. □

V. Upper Bounds

In this section, we prove upper bounds on $C_{\mathtt{NIC}}$ and $C_{\mathtt{SE}}$ by applying the results developed in Sections III and IV. We assume that the SK satisfies the "weak secrecy" condition (7).

The following observation from [11] is needed.

Lemma 10. *For mutually independent rvs Y_1, Y_2, Y_3 and an interactive communication $\mathbf{F}$ for the sources Y_1, Y_2, Y_3 described in Section III, we have*

$$\mathrm{P}_{Y_1,Y_2,Y_3|\mathbf{F}}\left(y_1, y_2, y_3 \mid \mathbf{f}\right) = \prod_{i=1}^{3} \mathrm{P}_{Y_i|\mathbf{F}}\left(y_i \mid \mathbf{f}\right), \quad \forall\, \mathbf{f},$$

i.e., independent observations remain independent when conditioned on an interactive communication.

We first remark that the initial round of interactive communication F_1 does not help. Specifically, for an ϵ-SK K recoverable from an interactive communication $\mathbf{F}$, it follows from (5) and (6) that there exists a fixed value f_1 of F_1 such that

$$\begin{aligned} &\mathrm{P}\left(K_1 = K_2 = K_3 = K \mid F_1 = f_1\right) \geq 1 - 2\epsilon, \\ &\log|\mathcal{K}| - H\left(K \mid \mathbf{F}, F_1 = f_1\right) \leq 2\epsilon \end{aligned} \tag{13}$$

Note that by Lemma 10 the rvs U_1, U_2, U_3 are conditionally independent given F_1. Consider a modified protocol obtained by fixing $F_1 = f_1$ and using local randomization $\tilde{U}_1, \tilde{U}_2, \tilde{U}_3$ with the same distribution as the conditional distribution of U_1, U_2, U_3 given $F_1 = f_1$. Then, in view of (13), the modified protocol generates a 2ϵ-SK of rate not less than the original protocol and does not require any initial interactive communication. Thus, without loss of generality, in the remainder of the section we assume that F_1 is constant.

A. Proof of $C_{\mathtt{NIC}} \leq R^*_f$

Let R be an achievable SK rate for a MAC with *no input communication*. Setting $Y_1 = U_1$, $Y_2 = U_2$ and $Y_3 = (X_3^n, U_3)$ and applying the corollary to Theorem 7 with partition $\pi = (\{1\}, \{2, 3\})$, for every $\delta > 0$ and n sufficiently large we have

$$\begin{aligned} R &\leq \frac{1}{n} D\left(\mathrm{P}_{U_1 U_2 X_3^n U_3} \| \mathrm{P}_{U_1} \times \mathrm{P}_{U_2 X_3^n U_3}\right) + \delta \\ &= \frac{1}{n} I\left(U_1 \wedge U_2, X_3^n, U_3\right) + \delta \\ &= \frac{1}{n} I\left(U_1 \wedge X_3^n, U_3 \mid U_2\right) + \delta, \end{aligned} \tag{14}$$

and similarly, using the partition $\pi = (\{2\}, \{1, 3\})$,

$$R \leq \frac{1}{n} I\left(U_2 \wedge X_3^n, U_3 \mid U_1\right) + \delta. \tag{15}$$

Also, for the partition $\pi = (\{1\}, \{2\}, \{3\})$, we get for n large

$$\begin{aligned} R &\leq \frac{1}{2n} D\left(\mathrm{P}_{U_1 U_2 X_3^n U_3} \| \mathrm{P}_{U_1} \times \mathrm{P}_{U_2} \times \mathrm{P}_{X_3^n U_3}\right) + \delta \\ &= \frac{1}{2n} I\left(U_1, U_2 \wedge X_3^n, U_3\right) + \delta, \end{aligned} \tag{16}$$

where the equality uses the independence of U_1 and U_2. Upon combining the bounds in (14) – (16) and taking the limit $n \to \infty$, an application of Lemma 9 yields

$$R \leq R^*_f,$$

since $\delta > 0$ was arbitrary. This proves the claimed upper bound. □

Remark. Choosing $\pi = (\{1, 2\}, \{3\})$, we also get the bound

$$\begin{aligned} R &\leq \frac{1}{n} D\left(\mathrm{P}_{U_1 U_2 X_3^n U_3} \| \mathrm{P}_{U_1 U_2} \times \mathrm{P}_{X_3^n U_3}\right) + \delta \\ &= \frac{1}{n} I\left(U_1, U_2 \wedge X_3^n, U_3\right) + \delta \end{aligned}$$

which is subsumed by (16).

B. Proof of $C_{\mathtt{SE}} \leq R^*$

Let R be an achievable SK rate for a MAC with *source emulation*. Setting $Y_1 = (X_1^n, U_1)$, $Y_2 = (X_2^n, U_2)$ and $Y_3 = (X_3^n, U_3)$, and following the steps of the previous part *mutatis mutandis*, we get

$$\begin{aligned} R^* \leq \overline{\lim_n} \sup \min \Bigg\{ &\frac{1}{n} I\left(X_1^n, U_1 \wedge X_3^n, U_3 \mid X_2^n, U_2\right), \\ &\frac{1}{n} I\left(X_2^n, U_2 \wedge X_3^n, U_3 \mid X_1^n, U_1\right), \\ &\frac{1}{2n} I\left(X_1^n, U_1, X_2^n, U_2 \wedge X_3^n, U_3\right) \Bigg\}. \end{aligned} \tag{17}$$

Note that

$$\begin{aligned} &I\left(X_1^n, U_1 \wedge X_3^n, U_3 \mid X_2^n, U_2\right) \\ &= I\left(X_1^n, U_1 \wedge X_3^n \mid X_2^n, U_2\right) \\ &\leq I\left(X_1^n \wedge X_3^n \mid X_2^n\right), \end{aligned} \tag{18}$$

where the equality follows since U_3 is independent of the rest of the rvs, and the inequality[5] uses $U_1, U_2 \multimap X_1^n, X_2^n \multimap X_3^n$. Similarly,

$$I\left(X_2^n, U_2 \wedge X_3^n, U_3 \mid X_1^n, U_1\right) \leq I\left(X_2^n \wedge X_3^n \mid X_1^n\right),$$

and

$$I\left(X_1, U_1, X_2^n, U_2 \wedge X_3^n, U_3\right) \leq I\left(X_1^n, X_2^n \wedge X_3^n\right),$$

where the rvs $X_1^n = X_1^n(U_1)$ and $X_2^n = X_2^n(U_2)$ are independent. By Lemma 8 and (17), the upper bound on $C_{\mathtt{SE}}$ follows. □

VI. Lower Bounds

In this section, we prove Theorem 4. Suppose (R, R) lies in $\mathcal{C}_{\mathtt{MACFB}}$ for a symmetric MAC. Then, there exist encoder mappings

$$\begin{aligned} &\tau_{1t} : \{1, ..., \lfloor 2^{nR} \rfloor\} \times \mathcal{X}_3^{t-1} \to \mathcal{X}_1, \\ &\tau_{2t} : \{1, ..., \lfloor 2^{nR} \rfloor\} \times \mathcal{X}_3^{t-1} \to \mathcal{X}_2, \quad 1 \leq t \leq n, \end{aligned} \tag{19}$$

and decoder mapping

$$\rho : \mathcal{X}_3^n \to \{1, ..., \lfloor 2^{nR} \rfloor\} \times \{1, ..., \lfloor 2^{nR} \rfloor\} \tag{20}$$

such that when messages M_1, M_2 are sent, where rvs M_1 and M_2 are i.i.d. uniform over $\{1, ..., \lfloor 2^{nR} \rfloor\}$, the error probability satisfies

$$\epsilon_n = \mathrm{P}\left(\rho\left(X_3^n\right) \neq (M_1, M_2)\right) \to 0,$$

in the limit as $n \to \infty$.

[5] In fact, the inequality holds with equality.

Using this n length code, we construct a symmetric code of length $2n$ by applying (19) and (20) twice as follows. Consider rvs $\hat{M}_1$, $\hat{M}_2$, $\tilde{M}_1$, $\tilde{M}_2$ i.i.d. uniform over $\left\{1, ..., \lfloor 2^{nR} \rfloor\right\}$. We send inputs corresponding to messages $\hat{M}_1, \hat{M}_2$ in the odd time instances, and, with the roles of τ_{1t} and τ_{2t} interchanged, send inputs corresponding to messages $\tilde{M}_1, \tilde{M}_2$ in the even time instances. Using the outputs at the odd and even time instances to decode $\hat{M}_1$, $\hat{M}_2$ and $\tilde{M}_1$, $\tilde{M}_2$, respectively, we obtain a code of rate (R, R) with error probability bounded above by $2\epsilon_n$. Denoting by Y_t the rv $(X_{3(2t-1)}, X_{3(2t)})$, $1 \leq t \leq n$, and letting $M_1 = (\hat{M}_1, \tilde{M}_1)$ and $M_2 = (\hat{M}_2, \tilde{M}_2)$, we get

$$\begin{aligned} &H\left(Y_t \mid M_1, Y^{t-1}\right) \\ &= H\left(X_{3(2t-1)} \mid \hat{M}_1, X_{31}, ..., X_{3(2t-3)}\right) \\ &\quad + H\left(X_{3(2t)} \mid \tilde{M}_1, X_{32}, ..., X_{3(2t-2)}\right) \\ &= H\left(X_{3(2t)} \mid \tilde{M}_2, X_{32}, ..., X_{3(2t-2)}\right) \\ &\quad + H\left(X_{3(2t-1)} \mid \hat{M}_2, X_{31}, ..., X_{3(2t-3)}\right) \\ &= H\left(Y_t \mid M_2, Y^{t-1}\right), \end{aligned} \tag{21}$$

where the second equality follows from the symmetry of the MAC.

Next, we replace the feedback Y_t with its compressed version given the observations of the input terminals. To do this, we consider a multiple-blocks extension of the symmetric code above and take recourse to the result of Slepian and Wolf [10]. Specifically, let M_{1i}, M_{2i}, Y_i^n, $i = 1, ..., N$, be N i.i.d. repetitions of rvs M_1, M_2, Y^n above. By Slepian-Wolf theorem [10], there exist mappings

$$F_t = F_t(Y_{t1}, Y_{t2}, ..., Y_{tN}), \quad 1 \leq t \leq n,$$

of rates

$$\begin{aligned} \frac{1}{N}\log\|F_t\| &\leq H\left(Y_t \mid M_1, Y^{t-1}\right) + \epsilon_n, \\ &= H\left(Y_t \mid M_2, Y^{t-1}\right) + \epsilon_n, \end{aligned} \tag{22}$$

such that an observer of $(M_{11}, ..., M_{1N}, Y_1^{t-1}, ..., Y_N^{t-1})$ or $(M_{21}, ..., M_{2N}, Y_1^{t-1}, ..., Y_N^{t-1})$ can recover Y_t^N with probability of error less than ϵ_n/n, for all N sufficiently large. The equality in (22) uses (21). Then, using a union bound on probability of error, the communication-transmission protocol corresponding to $F_1, ..., F_n$ allows all the terminals to recover $(Y_1^n, ..., Y_N^n)$ with probability of error less than ϵ_n. Note that the overall communication-transmission protocol now consists of n rounds of communication from terminal 3 and $2nN$ transmissions over the MAC. In each time slot t, the output terminal observing $Y_{t1}, ..., Y_{tN}$ sends F_t to the input terminals. Using this communication and their local observations M_1^N and M_2^N, the terminals 1 and 2 estimate $Y_{t1}, ..., Y_{tN}$ and use the estimates to select the inputs $X_{1(2t+1)}^N, X_{1(2t+2)}^N$ and $X_{2(2t+1)}^N, X_{2(2t+2)}^N$, respectively.

Finally, we show that for all n, N sufficiently large, there exists a function K of $(Y_1^n, ..., Y_N^n)$ of rate $(1/nN)\log\|K\|$ greater than $R - \delta$, satisfying

$$s_{in}(K; \mathbf{F}) \leq \epsilon.$$

Therefore, K is an ϵ-SK for n, N sufficiently large, where $0 < \epsilon < 1$ is arbitrary. It remains to find a mapping K as above. By [4, Lemma 1], it suffices to show that

$$\|\mathrm{P}_{K\mathbf{F}} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}}\| \leq 2^{-n\tau},$$

for some $\tau > 0$. Indeed, by the "balanced coloring lemma" [4, Lemma B4], for n, N sufficiently large, there exists such a mapping K of rate

$$\begin{aligned} \frac{1}{nN}\log\|K\| &\geq \frac{1}{nN}H(Y_1^n, ..., Y_N^n) - \frac{1}{nN}\log\|\mathbf{F}\| - \epsilon_n \\ &\geq \frac{1}{n}H(Y^n) - \frac{1}{n}\sum_{t=1}^n H\left(Y_t \mid M_1, Y^{t-1}\right) - 2\epsilon_n \\ &= \frac{1}{n}I(Y^n \wedge M_1) - 2\epsilon_n \\ &\geq R - \delta, \end{aligned}$$

where the second inequality is by (22) and the previous inequality uses Fano's inequality. Thus, R is an achievable SK rate.

VII. Discussion

Our proof methodology in this paper is to use the basic properties of SKs and interactive communication to obtain upper bounds on SK rates, and then relate these upper bounds directly to the maximum rates of reliable transmission over a MAC, without reducing them to single-letter forms. In particular, this approach brings out a key property of interactive communication that is instrumental in proving the converse, namely the inequality (see Lemma 6)

$$H(\mathbf{F}) \geq \sum_{B \in \mathcal{B}} \lambda_B H\left(\mathbf{F} \mid Y_{B^c}\right). \tag{23}$$

For the case of two terminals, this inequality can be written as

$$H(\mathbf{F}) \geq H(\mathbf{F} \mid Y_1) + H(\mathbf{F} \mid Y_2), \tag{24}$$

which is well-known in the communication complexity literature (c.f. [2]) as the fact that *external communication cost is at least as much as the communication cost*. Besides (23), the only other property of interactive communication that we use is the fact that independent observations remain so when conditioned on interactive communication (see Lemma 10). However, for a specific choice of λ in (23), upon rearranging the terms we get

$$I\left(Y_B \wedge Y_{B^c} \mid \mathbf{F}\right) \leq I\left(Y_B \wedge Y_{B^c}\right), \quad \text{for all } B \subseteq \mathcal{M},$$

which in turn implies Lemma 10. Thus, (23) is the only property of interactive communication that is used in our converse proofs. Note that (24) is indeed a characteristic of an interactive communication and does not hold for every function of Y_1 and Y_2. For instance, for symmetrically distributed unbiased bits Y_1 and Y_2, and $F = Y_1 \oplus Y_2$,

$$H(F) = 1 < H(F \mid Y_1) + H(F \mid Y_2) = 2.$$

Our results in this paper extend easily to MACs with multiple inputs. In particular, Theorems 3 and 5 hold for a multi-input MAC upon defining R^* and R_f^* as follows:

$$R^* = \max\left\{R : (R, ..., R) \in \mathcal{C}_{\mathtt{MAC}}\right\},$$
$$R_f^* = \max\left\{R : (R, ..., R) \in \mathcal{C}_{\mathtt{MACFB}}\right\}.$$

Also, Theorem 4 holds for a multi-input MAC $W : \mathcal{X}_1 \times ... \times \mathcal{X}_{m-1} \to \mathcal{X}_m$ that satisfies

$$W\left(x_m \mid x_1, ..., x_{m-1}\right) = W\left(x_m \mid x_{\sigma(1)}, ..., x_{\sigma(m-1)}\right),$$

for every permutation σ of $\{1, ..., m-1\}$.

ACKNOWLEDGEMENTS

The authors are indebted to Prakash Narayan for allowing us to include Theorem 7 in this paper. Also, the discussion on interactive communication properties in the last section is based on ideas developed jointly with him.

REFERENCES

[1] R. Ahlswede, "Multiway communication channels," *Proc. IEEE International Symposium on Information Theory*, pp. 23–52, 1973.

[2] M. Braverman, "Coding for interactive computation: progress and challenges," *Proc. Conference on Communication, Control, and Computing (Allerton)*, pp. 1914–1921, October 2012.

[3] C. Chan, "Generating secret in a network," *Ph. D. Dissertation, Massachussetts Institute of Technology*, 2010.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.

[5] ——, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[6] ——, "Secrecy generation for multiaccess channel models," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 17–31, 2013.

[7] H. Liao, "A coding theorem for multipleaccess communications," *Proc. IEEE International Symposium on Information Theory*, 1972.

[8] M. Madiman and P. Tetali, "Information inequalities for joint distributions, with interpretations and applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2699–2713, June 2010.

[9] P. Narayan, *Personal Communication*, 2013.

[10] D. Slepian and J. Wolf, "Noiseless coding of correlated information source," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[11] H. Tyagi and P. Narayan, "How many queries will resolve common randomness?" *To appear, IEEE Trans. Inf. Theory*, 2013.

[12] F. M. J. Willems, "The feedback capacity region of a class of discrete memoryless multiple access channels," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 93–95, January 1982.