

Information-Theoretic Key Agreement of Multiple Terminals - Part II: Channel Model

Amin Aminzadeh Gohari and Venkat Anantharam

Department of Electrical Engineering and Computer Science

University of California, Berkeley

{aminzade, ananth}@eecs.berkeley.edu

Abstract

This is the second part of a two-part paper on information-theoretically secure secret key agreement. This part covers the secret key capacity under the *channel model*. In this model, multiple terminals wish to create a shared secret key that is secure from an eavesdropper with unlimited computational resources. The terminals are all connected to a noiseless and authenticated but insecure channel, called the “public channel”. Furthermore, the terminals have access to a secure but noisy discrete memoryless broadcast channel (DMBC). The first terminal can choose a sequence of inputs to the DMBC, which has outputs at the other terminals and at the eavesdropper. After each channel use, the terminals can engage in arbitrarily many rounds of interactive authenticated communication over the public channel. At the end, each legitimate terminal should be able to generate the secret key. In this paper, we derive new lower and upper bounds on the secrecy capacity. In each case, an example is provided to show that the new bound represents a strict improvement over the previously best known bound.

This part of the paper is not standalone, and is written under the assumption that the reader has access to Part I, which is published in the same issue.

Keywords: Secret key agreement, unconditional security, communication for omniscience, secret key capacity, common randomness, public discussion, source model, channel model, security.

I. INTRODUCTION

In this paper, we study the problem of determining the maximum information-theoretically secure secret key rate against a passive eavesdropper in a well-known setting in the information-theoretic security literature, called the *channel model*. The history of the development of the model dates back to an early work by Wyner [16], who considered the setting in which Alice is connected to Bob by a discrete

memoryless channel. The eavesdropper, Eve, receives a noisy version of the output at Bob's end. This work was subsequently generalized by Csiszár and Körner [3] and later by Maurer [10] who recognized the value of public discussion (see the introduction of the first part of the paper for a more detailed treatment of the development of the model). The recognition of the value of public discussion led to the formulation of the two main models in this area, introduced by the works of Ahlswede and Csiszár [1], Csiszár and Narayan [5] and Maurer [10], the *source model* and *channel model*. This part of the paper covers the secret key capacity under the channel model.

In the channel model, there are m terminals interested in secret key generation against an adversary Eve. The terminals are all connected to a noiseless and authenticated but public communication channel. In addition, the terminals have access to a secure but noisy discrete memoryless broadcast channel (DMBC), $q(x_2, x_3, \dots, x_m, z|x_1)$. The input to the DMBC is governed by the first terminal while the other terminals, as well as Eve, observe the outputs of the broadcast channel at their respective ends. In what is traditionally called the channel model, after each use of the channel by the first terminal, all the m terminals are allowed to engage in arbitrary many rounds of interactive authenticated communication over the public channel. The public channel is noiseless. The eavesdropper is assumed to remain passive throughout the public discussion, but hears the messages sent over the public channel. We consider a generalization of this where only the first u terminals ($1 \leq u \leq m$) are allowed such communication; terminals $u + 1 \leq i \leq m$ listen and must participate in secret key generation, but cannot talk. This generalization is motivated by the desire to put one-way capacity and interactive capacity on the same footing, and fits naturally with the corresponding generalization that we made in the source model in the first part of the paper. Note that we assume, mostly for notational convenience, that the first terminal is allowed to participate in the interactive authenticated public communication.

Note that each input to the broadcast channel by the first terminal is allowed to depend on the past inputs and on the public communication so far. At the end of the entire process, i.e. of the n uses of the DMBC and of the interactive public communication after each use, each terminal $1 \leq i \leq m$ generates random variable S_i as its secret key. All S_i 's should with high probability be equal to each other and they should be approximately independent of Eve's whole information after the communication, i.e. the n outputs at Eve's end of the broadcast channel, and the entire public discussion. The achieved secret key rate would then be roughly $\frac{1}{n}H(S_1)$. The highest achievable secret key rate, asymptotically in n , is called the secret key capacity. For a precise formulation see the first part of the paper.

In this paper, we prove new lower and upper bounds on the secret key capacity. In each case, an example is provided to show that the new bound is strictly better than the previous one. For the case

of $m = 2$, the best known upper bound explicitly mentioned in the literature, as far as we are aware, is $\min[\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2|Z)]$, which was proposed by Maurer [10]. This can however be easily generalized to $\inf_{\bar{Z} \rightarrow Z \rightarrow X_1 X_2} [\sup_{p(x_1)} I(X_1; X_2|\bar{Z})]$. The best known lower bound, as far as we are aware, is

$$\sup_{p(x_1)} \max \left\{ \sup_{V \rightarrow U \rightarrow X_1 \rightarrow X_2 Z} [I(U; X_2|V) - I(U; Z|V)], \sup_{V \rightarrow U \rightarrow X_2 \rightarrow X_1 Z} [I(U; X_1|V) - I(U; Z|V)] \right\}, \quad (1)$$

which one can find in [5], [10].

The technique used for deriving the upper bounds can be described as follows. Take an arbitrary secret key generation scheme that uses the DMBC for say n times. During the simulation of the protocol, the “secret key reservoir” (representing the amount of secret key bits built up so far)¹ of the legitimate terminals gradually increases until it reaches its final state where the legitimate terminals create the common secret key. Each use of the DMBC increases the “secret key reservoir” of the terminals, whereas the public discussion that follows after each use of the DMBC allows for coordination and processing of the “secret key reservoir”, but does not increase the amount of secret key bits, since the public discussion is observed by the eavesdropper. The idea is to quantify this gradual evolution of the “secret key reservoir”, bound the derivative of its growth at each stage from above by showing that one use of the DMBC can buy us at most a certain amount of secret bits (use of the public channel does not increase the “secret key reservoir”), and conclude that the final size of the “secret key reservoir” is not bigger than n times the upper bound on its derivative per use of the DMBC. An implementation of this idea requires quantification of the “secret key reservoir” of the m terminals at a given stage of the process. To that end, we take a real-valued function of joint distributions, and evaluate it at the joint distribution of $m + 1$ random variables that represent, roughly speaking, the knowledge of the m legitimate terminals and the eavesdropper at the given stage of the secret key generation protocol. Properties that such a function would need to satisfy are identified. The new upper bound is then proved by a verification argument.

We have divided the presentation of results into two parts, one for source model and one for channel model. In order to minimize duplication, we have decided to include in part I a unified introduction which sets out all the common notation, discussion and fundamentals. This part of the paper is therefore not standalone, and is written under the assumption that the reader has access to Part I. Table I summarizes the notation used throughout the paper.

The outline of this paper is as follows. Section II illustrates the technique used for proving the upper

¹We do not need to define “secret key reservoir” formally.

TABLE I
NOTATIONS(SEE THE DEFINITION SECTION OF THE FIRST PART OF THE PAPER)

Variable	Description
$\mathbb{R}_{\geq 0}$	Non-negative real numbers.
$[k], [m]$	The sets $\{1, 2, 3, \dots, k\}$ and $\{1, 2, 3, \dots, m\}$.
m	Number of legitimate terminals.
u	Number of legitimate terminals that participate in public discussion.
$q(x_2, \dots, x_m, z x_1)$	A secure but noisy discrete memoryless broadcast channel (DMBC) exploited for secret key generation.
$C_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z x_1))$	The capacity channel ϵ -secret key capacity when the first u terminals talk.
$C_{CH}(u, q(x_2, x_3, \dots, x_m, z x_1))$	The channel model secret key capacity when the first u terminals talk.
$S(X_1; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} Z)$	The source model secret key capacity when the first u terminals talk.
SK_C	<p>Secret key generation scheme. Parameters are</p> <p>n: the number of uses of the DMBC</p> <p>ϵ: an upper bound on the probability of key mismatch, and secret key rate leak out.</p> <p>S_1, S_2, \dots, S_m: The secret keys generated by the m terminals at the final stage.</p> <p>$\mathbf{C} = (\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_n)$: Interactive public discussions among the parties with \mathbf{C}_i being conducted following the i-th use of the DMBC.</p> <p>M_1, M_2, \dots, M_u: Private randomness available to the first u parties.</p> <p>$X_1^n, X_2^n, \dots, X_m^n, Z^n$: $X_1^n = (X_1(1), \dots, X_1(n))$ is the n inputs to the DMBC; X_2^n, \dots, X_m^n, Z^n are the n outputs.</p>
$\phi(\cdot)$	a real-valued function, and a place holder for an upper bound on the channel model secret key capacity.
$\varphi(\cdot)$	a real-valued function that intuitively takes the knowledge available to the legitimate terminals as well as the eavesdropper, at a given stage in the key generation process, and maps it to a number quantifying the secret bits accumulated so far.
$\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m, \hat{Z}$	Represents the <i>total</i> information available to the m terminals and the eavesdropper terminal at a given stage during the secret key generation scheme.

bounds at an intuitive level. Section III contains the main results of this paper. This is followed by section IV and two appendices which give proofs for the results.

II. THE TECHNIQUE FOR PROVING UPPER BOUNDS

In this section, we illustrate the main proof technique we use for proving the upper bounds at an intuitive level. Consider the special case of $u = m = 2$ and take an arbitrary secret key generation

protocol $\text{SK}_C(n, \epsilon, S_1, S_2, \mathbf{C}, M_1, M_2, X_1^n, X_2^n, Z^n)$ (see the first part of the paper for definitions).

During the simulation of the protocol, the “secret key reservoir” of the legitimate terminals gradually evolves until it reaches its final state where the terminals know enough to create the common secret key. We can represent the state of the system at a given stage of the process by the joint distribution of three random variables that represent, roughly speaking, the knowledge of the two legitimate terminals and the eavesdropper at that stage. The state of the system therefore evolves as follows:

$$\begin{aligned}
& \rightarrow (X_1(1), X_2(1), Z(1)) \rightarrow (X_1(1)M_1, X_2(1)M_2, Z(1)) \rightarrow (X_1(1)M_1C_{1,1}, X_2(1)M_2C_{1,1}, Z(1)C_{1,1}) \\
& \rightarrow (X_1(1)M_1C_{1,1}C_{1,2}, X_2(1)M_2C_{1,1}C_{1,2}, Z(1)C_{1,1}C_{1,2}) \rightarrow \dots \rightarrow (X_1(1)M_1\mathbf{C}_1, X_2(1)M_2\mathbf{C}_1, Z(1)\mathbf{C}_1) \\
& \quad \rightarrow (X_1(1)X_1(2)M_1\mathbf{C}_1, X_2(1)X_2(2)M_2\mathbf{C}_1, Z(1)Z(2)\mathbf{C}_1) \\
& \quad \rightarrow (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}, Z(1)Z(2)\mathbf{C}_1C_{2,1}) \\
& \quad \rightarrow (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}C_{2,2}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}C_{2,2}, Z(1)Z(2)\mathbf{C}_1C_{2,1}C_{2,2}) \\
& \quad \rightarrow \dots \rightarrow (X_1(1)X_1(2)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)\mathbf{C}_1\mathbf{C}_2) \\
& \quad \rightarrow (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2) \\
& \quad \rightarrow (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2C_{3,1}, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2C_{3,1}, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2C_{3,1}) \\
& \quad \rightarrow \dots \rightarrow (X_1^n M_1\mathbf{C}, X_2^n M_2\mathbf{C}, Z^n \mathbf{C}) \rightarrow (S_1, S_2, Z^n \mathbf{C})
\end{aligned}$$

Formally speaking, we can represent the state by three finite sets and a joint distribution on these finite sets, i.e. a four-tuple $(\hat{\mathcal{X}}_1, \hat{\mathcal{X}}_2, \hat{\mathcal{Z}}, p(\hat{x}_1, \hat{x}_2, \hat{z}))$. Please note that here we have used random variables \hat{X}_1 , \hat{X}_2 and \hat{Z} to represent the total information available to the terminals at a given stage of the key generation process (whereas random variables X_1 , and X_2 , Z were representing the input and outputs to the broadcast channel).

A. The functions $\phi(\cdot)$ and $\varphi(\cdot)$, and properties imposed on them

To quantify the evolution of the “secret key reservoir” of the legitimate parties, we use a function φ defined from the set of all four tuples $(\hat{\mathcal{X}}_1, \hat{\mathcal{X}}_2, \hat{\mathcal{Z}}, p(\hat{x}_1, \hat{x}_2, \hat{z}))$ to non-negative real numbers. We sometimes use the notation $\varphi(\hat{X}_1; \hat{X}_2 \| \hat{Z})$ to refer to $\varphi(p(\hat{x}_1, \hat{x}_2, \hat{z}))$ when $(\hat{X}_1, \hat{X}_2, \hat{Z})$ has the law $p(\hat{x}_1, \hat{x}_2, \hat{z})$.²

Suppose we would like to prove that some given non-negative function $\phi(q(x_2, z|x_1))$ is an upper bound on the secret key capacity. It would be enough to prove that each use of the DMBC in each stage,

²As in the source model notation, we have separated the legitimate parties and the eavesdropper via the symbol $\|$.

cannot buy us more than $\phi(q(x_2, z|x_1))$ secret bits. This would imply that n uses of the DMBC does not buy us more than $n \times \phi(q(x_2, z|x_1))$ secret bits, and therefore the secret key rate achieved will be less than or equal to $\phi(q(x_2, z|x_1)) \frac{\text{secret bits}}{\text{DMBC use}}$.

Motivated by the above discussion, let us assume that the system is in the state $(\hat{\mathcal{X}}_1, \hat{\mathcal{X}}_2, \hat{\mathcal{Z}}, p(\hat{x}_1, \hat{x}_2, \hat{z}))$, and the terminals decide to use the DMBC. The first terminal would create X_1 as a function of \hat{X}_1 , and puts it at the input of the DMBC $q(x_2, z|x_1)$. The second terminal and the eavesdropper will receive X_2 and Z . The state of the system will evolve to $(\hat{\mathcal{X}}_1 \times \mathcal{X}_1, \hat{\mathcal{X}}_2 \times \mathcal{X}_2, \hat{\mathcal{Z}} \times \mathcal{Z}, p(\hat{x}_1 x_1, \hat{x}_2 x_2, \hat{z} z))$. Note that the following statements are true about the joint distribution of $\hat{X}_1, X_1, \hat{X}_2, X_2, \hat{Z}, Z$:

$$H(X_1|\hat{X}_1) = 0, \quad (2)$$

$$\hat{X}_1 \hat{X}_2 \hat{Z} \rightarrow \hat{X}_1 \rightarrow X_1 \rightarrow X_1 X_2 Z, \quad (3)$$

$$p(x_2, z|x_1) = q(x_2, z|x_1). \quad (4)$$

We then expect the quantified state does not increase by more than $\phi(\cdot)$. In other words, we would like to have the following property:

- 1) Whenever equations (2), (3) and (4) hold, we require:

$$\varphi(\hat{X}_1 X_1; \hat{X}_2 X_2 \| \hat{Z} Z) \leq \varphi(\hat{X}_1; \hat{X}_2 \| \hat{Z}) + \phi(q(x_2, z|x_1)).$$

Next, we expect the public discussion that follows each use of the DMBC does not increase the “secret key reservoir” (since the public discussion is heard by the eavesdropper). Let us assume that the system is in the state $(\hat{\mathcal{X}}_1, \hat{\mathcal{X}}_2, \hat{\mathcal{Z}}, p(\hat{x}_1, \hat{x}_2, \hat{z}))$, and the i -th legitimate terminal ($1 \leq i \leq 2$) decides to use the public channel. This terminal creates random variable F , so we must have $H(F|\hat{X}_i) = 0$. Random variable F is made public and the state of the system evolves to $(\hat{\mathcal{X}}_1 \times \mathcal{F}, \hat{\mathcal{X}}_2 \times \mathcal{F}, \hat{\mathcal{Z}} \times \mathcal{F}, p(\hat{x}_1 f, \hat{x}_2 f, \hat{z} f))$. We then expect the quantified state to stay the same or to decrease. In other words, we would like to have the following property:

- 2) For any random variable F such that $\exists i : H(F|\hat{X}_i) = 0$, we require:

$$\varphi(\hat{X}_1; \hat{X}_2 \| \hat{Z}) \geq \varphi(\hat{X}_1 F; \hat{X}_2 F \| \hat{Z} F);$$

Next, since $\varphi(\cdot)$ is quantifying the “secret key reservoir”, and reducing the information available to the legitimate terminals should not increase their “secret key reservoir”, we impose the following constraint:

- 3) For any random variables \hat{X}'_1, \hat{X}'_2 such that $\forall i : H(\hat{X}'_i|\hat{X}_i) = 0$, we require:

$$\varphi(\hat{X}_1; \hat{X}_2 \| \hat{Z}) \geq \varphi(\hat{X}'_1; \hat{X}'_2 \| \hat{Z}).$$

Next, consider the special case of $\hat{X}_1 \cong \hat{X}_2$, and \hat{Z} being almost independent of (\hat{X}_1, \hat{X}_2) . In this case, we expect $\varphi(\hat{X}_1; \hat{X}_2 \| \hat{Z})$ to be approximately equal to $H(\hat{X}_1)$. In order to ensure this property, and

inspired by the lower bound $I(\widehat{X}_1; \widehat{X}_2) - I(\widehat{X}_1; \widehat{Z})$ on the source model secret key capacity, we impose the following constraint:

$$4) \quad \varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq H(\widehat{X}_1 | \widehat{Z}) - H(\widehat{X}_1 | \widehat{X}_2) = I(\widehat{X}_1; \widehat{X}_2) - I(\widehat{X}_1; \widehat{Z}).$$

Since $\varphi(\cdot)$ is quantifying the “secret key reservoir”, providing the legitimate terminals with private external randomness should not increase their “secret key reservoir”. We therefore impose the following constraint:

5) Whenever random variables M_1, M_2 satisfy

$$p(M_1, M_2, \widehat{X}_1, \widehat{X}_2, \widehat{Z}) = p(M_1)p(M_2)p(\widehat{X}_1, \widehat{X}_2, \widehat{Z}),$$

we require

$$\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq \varphi(\widehat{X}_1 M_1; \widehat{X}_2 M_2 \| \widehat{Z}).$$

Lastly, we assume the following constraint: for any conditional distribution $q(x_2, z|x_1)$,

$$\sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, z|x_1)) < \infty. \quad (5)$$

B. Implication of the properties imposed on $\phi(\cdot)$ and $\varphi(\cdot)$

Claim: Assume that the above conditions 1-5, and equation (5) are satisfied for some functions $\varphi(\cdot)$ and $\phi(\cdot)$. Then the channel model secret key capacity, $C_{CH}(2, q(x_2, z|x_1))$, must be bounded from above by $\phi(q(x_2, z|x_1))$ for any channel $q(x_2, z|x_1)$.

Intuitive Proof: Take some DMBC channel $q(x_2, z|x_1)$, and a secret key generation protocol $\text{SK}_C(n, \epsilon, S_1, S_2, \mathbf{C}, M_1, M_2, X_1^n, X_2^n, Z^n)$ whose secret key rate is approximately equal to $C_{CH}^\epsilon(2, q(x_2, z|x_1))$. Then we have (here we are using the notation X_1^1 to represent $X_1(1)$, and $X_1^{1:k}$ to represent $X_1(1) \dots X_1(k)$):

$$\begin{aligned} (n-1)\phi(q(x_2, z|x_1)) + \sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, z|x_1)) &\geq \\ (n-1)\phi(q(x_2, z|x_1)) + \varphi(X_1^1; X_2^1 \| Z^1) & \\ \geq (n-1)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^1; M_2 X_2^1 \| Z^1) & \end{aligned} \quad (6)$$

$$\geq (n-1)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^1 C_{1,1}; M_2 X_2^1 C_{1,1} \| Z^1 C_{1,1}) \quad (7)$$

$$\geq (n-1)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^1 C_{1,1} C_{1,2}; M_2 X_2^1 C_{1,1} C_{1,2} \| Z^1 C_{1,1} C_{1,2}) \quad (8)$$

$\geq \dots$

$$\geq (n-1)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^1 \mathbf{C}_1; M_2 X_2^1 \mathbf{C}_1 \| Z^1 \mathbf{C}_1)$$

$$\geq (n-2)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^{1:2} \mathbf{C}_1; M_2 X_2^{1:2} \mathbf{C}_1 \| Z^{1:2} \mathbf{C}_1) \quad (9)$$

$$\geq (n-2)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^{1:2} \mathbf{C}_{1:2}; M_2 X_2^{1:2} \mathbf{C}_{1:2} \| Z^{1:2} \mathbf{C}_{1:2}) \quad (10)$$

$$\geq (n-3)\phi(q(x_2, z|x_1)) + \varphi(M_1 X_1^{1:3} \mathbf{C}_{1:2}; M_2 X_2^{1:3} \mathbf{C}_{1:2} \| Z^{1:3} \mathbf{C}_{1:2}) \quad (11)$$

$$\geq \dots$$

$$\begin{aligned} &\geq \varphi(M_1 X_1^{1:n} \mathbf{C}_{1:n}; M_2 X_2^{1:n} \mathbf{C}_{1:n} \| Z^{1:n} \mathbf{C}_{1:n}) \\ &\geq \varphi(S_1; S_2 \| Z^{1:n} \mathbf{C}_{1:n}) \end{aligned} \quad (12)$$

$$\geq H(S_1 | Z^{1:n} \mathbf{C}_{1:n}) - H(S_1 | S_2) \quad (13)$$

$$\cong nC_{CH}^\epsilon(2, q(x_2, z|x_1)) - 0, \quad (14)$$

where equation (6) holds because of condition 5; equation (7) holds because of condition 2 and the fact that $H(C_{1,1}|M_1 X_1^1) = 0$; equation (8) holds because of condition 2 and the fact that $H(C_{1,2}|M_2 X_2^1 C_{1,1}) = 0$; equation (9) holds because of condition 1; equation (10) is true because we can repeatedly invoke condition 2 for the individual communications within \mathbf{C}_2 ; equation (11) holds because of condition 1; equation (12) holds because of condition 3, and the fact that $H(S_1|M_1 X_1^{1:n} \mathbf{C}_{1:n}) = H(S_2|M_2 X_2^{1:n} \mathbf{C}_{1:n}) = 0$; equation (13) holds because of condition 4; and equation (14) holds since the secret key rate of the protocol is approximately equal to $C_{CH}^\epsilon(2, q(x_2, z|x_1))$, and S_1 is approximately equal to S_2 .

Intuitively, the above chain of inequalities imply that $\frac{n-1}{n}\phi(q(x_2, z|x_1)) + \frac{1}{n} \sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, z|x_1))$ is greater than or equal to $C_{CH}^\epsilon(2, q(x_2, z|x_1))$. Letting $n \rightarrow \infty$ and then $\epsilon \rightarrow 0$, we would get that $\phi(q(x_2, z|x_1))$ is greater than or equal to $C_{CH}(2, q(x_2, z|x_1))$.

C. Discussion

As the above proof indicates, as one moves along a given protocol, the expression $\frac{1}{n}((n-i)\phi(q(x_2, z|x_1)) + \varphi(\text{current state}))$ (where i denotes the number of uses of the DMBC so far) is non-increasing. This quantity starts from the upper bound $\phi(q(x_2, z|x_1))$ and decreases as we move along the protocol, and eventually becomes equal to the secret key rate of the protocol. Thus, it is justified to view the expression as a *potential function*. The reader may compare this section with section III of the first part of the paper where the idea of a potential function is discussed in the context of the source model.

In order to show the effectiveness of the technique, and show that it could make the converse proofs systematic, we provide an example:

Example. Prove that $\sup_{p(x_1)} I(X_1; X_2 | Z)$ is an upper bound on $C_{CH}(2, q(x_2, z|x_1))$.

Proof. Let $\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) = I(\widehat{X}_1; \widehat{X}_2 | \widehat{Z})$ and $\phi(q(x_2, z|x_1)) = \sup_{p(x_1)} I(X_1; X_2 | Z)$. Clearly equation (5) is satisfied. We need to verify the five properties: the first property holds since whenever equations

(2), (3) and (4) are hold, we have

$$\begin{aligned}
I(\widehat{X}_1 X_1; \widehat{X}_2 X_2 | \widehat{Z} Z) &= H(\widehat{X}_2 X_2 | \widehat{Z} Z) - H(\widehat{X}_2 X_2 | \widehat{Z} Z \widehat{X}_1 X_1) \\
&= H(\widehat{X}_2 X_2 | \widehat{Z} Z) - H(\widehat{X}_2 | \widehat{Z} \widehat{X}_1) - H(X_2 | Z X_1) \\
&\leq H(\widehat{X}_2 | \widehat{Z}) + H(X_2 | Z) - H(\widehat{X}_2 | \widehat{Z} \widehat{X}_1) - H(X_2 | Z X_1) = I(\widehat{X}_1; \widehat{X}_2 | \widehat{Z}) + I(X_1; X_2 | Z) \\
&= \varphi(\widehat{X}_1; \widehat{X}_2 | \widehat{Z}) + \varphi(X_1; X_2 | Z) \leq \varphi(\widehat{X}_1; \widehat{X}_2 | \widehat{Z}) + \phi(q(x_2, z | x_1)).
\end{aligned} \tag{15}$$

Equation (15) holds because

$$\begin{aligned}
H(\widehat{X}_2 X_2 | \widehat{Z} Z \widehat{X}_1 X_1) &= H(\widehat{X}_2 | \widehat{Z} Z \widehat{X}_1 X_1) + H(X_2 | \widehat{Z} Z \widehat{X}_1 X_1 \widehat{X}_2) = \\
&H(\widehat{X}_2 | \widehat{Z} \widehat{X}_1) - I(\widehat{X}_2; Z X_1 | \widehat{Z} \widehat{X}_1) + H(X_2 | Z X_1) - I(X_2; \widehat{Z} \widehat{X}_1 \widehat{X}_2 | Z X_1).
\end{aligned}$$

But equation (3) implies that $I(\widehat{X}_2; Z X_1 | \widehat{Z} \widehat{X}_1) \leq I(\widehat{Z} \widehat{X}_2; Z X_1 | \widehat{X}_1) = 0$, and $I(X_2; \widehat{Z} \widehat{X}_1 \widehat{X}_2 | Z X_1) \leq I(X_2 Z; \widehat{Z} \widehat{X}_2 \widehat{X}_1 | X_1) = 0$.

The second property holds because assuming that $H(F | \widehat{X}_1) = 0$, $I(\widehat{X}_1; \widehat{X}_2 | \widehat{Z}) = I(\widehat{X}_1 F; \widehat{X}_2 | \widehat{Z}) = I(F; \widehat{X}_2 | \widehat{Z}) + I(\widehat{X}_1; \widehat{X}_2 | \widehat{Z} F) \geq I(\widehat{X}_1 F; \widehat{X}_2 F | \widehat{Z} F)$. The other properties can be easily verified. \blacksquare

In order to find a new upper bound, one can think of a given functions $\varphi(\widehat{X}_1; \widehat{X}_2 | \widehat{Z})$ and $\phi(q(x_2, z | x_1))$ as a point in the set of all functions that satisfy the properties, and try to slightly perturb the expression so that all the properties remain satisfied.

III. STATEMENT OF THE RESULTS

In this section we state the main results of this paper. All the results are proved in detail in section 4 and the appendices. Following the formal statement of each result, a brief informal discussion is provided to clarify the statement.

A. Sufficient conditions for being an upper bound on the SK_C capacity

Let $\varphi(p(\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_m, \widehat{z}))$ be a real-valued function from the set of *all* probability distributions defined on a product of *any* $m + 1$ finite sets. We sometimes use the notation $\varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m | \widehat{Z})$ to refer to $\varphi(p(\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_m, z))$ when $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z})$ has the law $p(\widehat{x}_1, \dots, \widehat{x}_m, \widehat{z})$.³ Furthermore, let $\phi(\cdot)$ be a real-valued function from the set of *all* conditional laws $q(x_2, x_3, \dots, x_m, z | x_1)$ defined on a product of $m + 1$ finite sets. Further assume that for any channel $q(x_2, x_3, \dots, x_m, z | x_1)$,

$$\sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, x_3, \dots, x_m, z | x_1)) < \infty. \tag{16}$$

³Inspired by the source model notation, we have separated the legitimate parties and the eavesdropper via the symbol $||$.

The following theorem formalizes the ideas discussed in section II:

Theorem 1: Given functions $\phi(\cdot)$ and $\varphi(\cdot)$ satisfying equation (16) for any channel $q(x_2, x_3, \dots, x_m, z|x_1)$, the function $\phi(q(x_2, x_3, \dots, x_m, z|x_1))$ will be an upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ (the channel model secret key capacity assuming that only the first u terminals are permitted to talk) if $\varphi(\cdot)$ satisfies the following 5 conditions for all $p(\hat{x}_1, \hat{x}_2, \dots, \hat{x}_m, \hat{z})$:

- 1) For any random variables X_1, X_2, \dots, X_m, Z jointly distributed with $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m, \hat{Z}$ such that

$$\begin{aligned} H(X_1|\hat{X}_1) &= 0, \\ \hat{X}_1\hat{X}_2\dots\hat{X}_m\hat{Z} &\rightarrow \hat{X}_1 \rightarrow X_1 \rightarrow X_1X_2\dots X_mZ, \text{ and} \\ p(x_2, x_3, \dots, x_m, z|x_1) &= q(x_2, x_3, \dots, x_m, z|x_1) \end{aligned}$$

hold, we have:

$$\varphi(\hat{X}_1X_1; \hat{X}_2X_2; \dots; \hat{X}_mX_m\|\hat{Z}Z) \leq \varphi(\hat{X}_1; \hat{X}_2; \dots; \hat{X}_m\|\hat{Z}) + \phi(q(x_2, x_3, \dots, x_m, z|x_1));$$

- 2) For any random variable F such that $\exists i \leq u : H(F|\hat{X}_i) = 0$, we have:

$$\varphi(\hat{X}_1; \hat{X}_2; \dots; \hat{X}_m\|\hat{Z}) \geq \varphi(\hat{X}_1F; \hat{X}_2F; \dots; \hat{X}_mF\|\hat{Z}F);$$

- 3) For any random variables $\hat{X}'_1, \hat{X}'_2, \dots, \hat{X}'_m$ such that $\forall i : H(\hat{X}'_i|\hat{X}_i) = 0$, we have:

$$\varphi(\hat{X}_1; \hat{X}_2; \dots; \hat{X}_m\|\hat{Z}) \geq \varphi(\hat{X}'_1; \hat{X}'_2; \dots; \hat{X}'_m\|\hat{Z});$$

- 4) $\varphi(\hat{X}_1; \hat{X}_2; \dots; \hat{X}_m\|\hat{Z}) \geq H(\hat{X}_1|\hat{Z}) - \sum_{i=2}^m H(\hat{X}_1|\hat{X}_i)$;

- 5) Whenever random variables M_1, M_2, \dots, M_u satisfy

$$p(M_1, M_2, \dots, M_u, \hat{X}_1, \hat{X}_2, \dots, \hat{X}_m, \hat{Z}) = p(M_1)p(M_2)\dots p(M_u)p(\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m, \hat{Z}),$$

we have:

$$\varphi(\hat{X}_1; \hat{X}_2; \dots; \hat{X}_m\|\hat{Z}) \geq \varphi(M_1\hat{X}_1; M_2\hat{X}_2; \dots; M_u\hat{X}_u; \hat{X}_{u+1}; \dots; \hat{X}_m\|\hat{Z}).$$

B. New upper bound on the SK_C capacity

Before stating the theorem, we make a few definitions. The intuitive meaning of the definitions and of the new upper bound are provided in the discussion that follows the statement of the theorem.

Definitions. Let $[m]$ and $[u]$ respectively denote the sets $\{1, 2, \dots, m\}$, $\{1, 2, \dots, u\}$. For any subset B of $[m]$, let λ_B be a non-negative real number, and $\Lambda = (\lambda_B, B \subseteq [m])$ denote a vector of dimension 2^m whose elements are λ_B for various subsets of $[m]$. Let V denote the set of vectors $\Lambda = (\lambda_B, B \subseteq [m])$ satisfying the following equation for any $(R_1, R_2, \dots, R_u) \in \mathbb{R}_{\geq 0}^u$:

$$\sum_{B: B \subseteq [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B \sum_{j \in B \cap [u]} R_j = \sum_{j=1}^u R_j. \quad (17)$$

For any subset B of $[m] = \{1, 2, 3, \dots, m\}$, we use the notation \hat{X}_B in reference to the set of random variables $(\hat{X}_k, k \in B)$. Note that unlike λ_B , \hat{X}_B is a set of random variables.

We then have the following theorem:

Theorem 2: For any $\Lambda = (\lambda_B, B \subseteq [m]) \in V$, the secret key capacity $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ is bounded from above by

$$\sup_{p(x_1)} \{ \inf_J ([H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} || J) + I(X_1 X_2 \dots X_m; J | Z)]) \}.$$

In this expression $(X_1, X_2, \dots, X_m, J, Z)$ have the law $p(x_1)q(x_2, x_3, \dots, x_m, z|x_1)p(j|x_1, \dots, x_m, z)$; the infimum is taken over finite random variables J arbitrarily distributed with X_1, X_2, \dots, X_m, Z ; and

$$\tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} || J) \doteq \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(X_{B \cap [u]} | X_{B^c} J). \quad (18)$$

Discussion: This upper bound was derived in an attempt to imitate the source model upper bound. In the first part of the paper we showed that

$$S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)} \dots; (X_m)^{(s)} || Z) \leq \inf_J [S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)} \dots; (X_m J)^{(s)} || J) + I(X_1 X_2 \dots X_m; J | Z)], \quad (19)$$

where the infimum is taken over finite random variables J arbitrarily distributed with X_1, X_2, \dots, X_m and Z . Theorem 6 of the first part of this paper provides a single letter expression for the first term in the right hand side of equation (19). This upper bound on the secret key capacity in the source model suggests the following upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$:

$$\sup_{p(x_1)} \{ \inf_J [S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)} \dots; (X_m J)^{(s)} || J) + I(X_1 X_2 \dots X_m; J | Z)] \}. \quad (20)$$

In order to prove that this expression is an upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$, one simply needs to define appropriate functions $\phi(\cdot)$ and $\varphi(\cdot)$, and then verify the properties of Theorem 1. We were not however able to complete the proof. So, we modified the expression of equation (20) for the proof to go through. We first provide an alternative characterization of the expression of equation (20), and then mention our modification.

Note that Theorem 6 of the first part of this paper provides the following expression:

$$S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)}; \dots; (X_m J)^{(s)} || J) = H(X_1 X_2 \dots X_u | J) - \min_{(R_1, R_2, \dots, R_u) \in \mathfrak{R}} \left(\sum_{i=1}^u R_i \right)$$

where

$$\mathfrak{R} = \{ (R_1, \dots, R_u) : \forall B : B \subset [m], B \cap [u] \neq \emptyset, B \neq [m] : \sum_{j \in B \cap [u]} R_j \geq H(X_{B \cap [u]} | X_{B^c} Z) \}.$$

The intuitive meaning of the quantity R_i is to be found in the context of the problem of communication for omniscience (CFO) discussed in the first part of the paper, or in [5]. The above expression can be rewritten using the duality theory as follows:

$$\begin{aligned} & S(X_1 J; X_2 J; \dots; X_u J; (X_{u+1} J)^{(s)}; \dots; (X_m J)^{(s)} \| J) = \\ & H(X_1 X_2 \dots X_u | J) - \max_{\Lambda \in V} (\tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J)) = \\ & \min_{\Lambda \in V} [H(X_1 X_2 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J)]. \end{aligned} \quad (21)$$

Therefore we can write the expression in equation (20) as follows:

$$\sup_{p(x_1)} \left\{ \inf_J \min_{\Lambda \in V} (H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J) + I(X_1 X_2 \dots X_m; J | Z)) \right\}.$$

We modified this expression by swapping $\min_{\Lambda \in V}$ with $\sup_{p(x_1)} \inf_J$ as follows:

$$\begin{aligned} & \min_{\Lambda \in V} \sup_{p(x_1)} \left\{ \inf_J (H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J) \right. \\ & \left. + I(X_1 X_2 \dots X_m; J | Z)) \right\}. \end{aligned} \quad (22)$$

The statement of Theorem 2 implies that equation (22) is an upper bound on $C_{CH}(u, q(x_2, x_3, \dots, x_m, z | x_1))$, since it states that for any arbitrary $\Lambda \in V$,

$$\begin{aligned} & C_{CH}(u, q(x_2, x_3, \dots, x_m, z | x_1)) \leq \\ & \sup_{p(x_1)} \left\{ \inf_J (H(X_1 \dots X_u | J) - \tau^\Lambda(X_1, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J) + I(X_1 \dots X_m; J | Z)) \right\}. \end{aligned}$$

■

Corollary. In the case of $m = u = 2$, the new upper bound on $C_{CH}(2, q(x_2, z | x_1))$ equals

$$\sup_{p(x_1)} \inf_J [I(X_1; X_2 | J) + I(X_1 X_2; J | Z)],$$

where the infimum is taken over finite random variables J arbitrarily distributed with X_1, X_2, Z . This is because the only possible value for $\lambda_{\{1\}}$ and $\lambda_{\{2\}}$ in the case of $m = u = 2$ is one. In order to intuitively understand this upper bound, assume that instead of the broadcast channel $q(x_2, z | x_1)$, we have an extended broadcast channel $q(x_2, z, j | x_1)$ where a fictitious terminal receiving J is introduced. The total secret key is “split” into two parts: one that is independent of with J , and one that is shared of J . These two parts correspond with the terms $I(X_1; X_2 | J)$ and $I(X_1 X_2; J | Z)$ respectively.

The new upper bound is always less than or equal to $\inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} \sup_{p(x_1)} I(X_1; X_2 | \overline{Z})$ (which in turn is less than or equal to $\min[\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2 | Z)]$). This is because in the new upper bound, the minimum is over finite random variables J arbitrarily distributed with X_1, X_2, Z ; if

one takes $J = \overline{Z}$ for some $\overline{Z} \rightarrow Z \rightarrow X_1 X_2$, $I(X_1 X_2; J|Z)$ will be zero, and $I(X_1; X_2|J)$ will be equal to $I(X_1; X_2|\overline{Z})$. Therefore

$$\sup_{p(x_1)} \inf_J [I(X_1; X_2|J) + I(X_1 X_2; J|Z)] \leq \sup_{p(x_1)} \inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} I(X_1; X_2|\overline{Z})$$

Lastly, note that $\sup_{p(x_1)} \inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} I(X_1; X_2|\overline{Z}) \leq \inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} \sup_{p(x_1)} I(X_1; X_2|\overline{Z})$.

Remark: One can use the strengthened Carathéodory theorem of Fenchel and Eggleston to get the cardinality bound of $|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|$ on the size of the alphabet set of J . One can therefore express the new upper bound as

$$\sup_{p(x_1)} \min_J [I(X_1; X_2|J) + I(X_1 X_2; J|Z)],$$

where the infimum is replaced with a minimum.

Theorem 3: The new upper bound represents a strict improvement over the previously best known upper bound for the case of $u = m = 2$: there exists an example for which the new upper bound is strictly smaller than $\sup_{p(x_1)} \inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} I(X_1; X_2|\overline{Z})$ which in turn is always less than or equal to $\inf_{\overline{Z} \rightarrow Z \rightarrow X_1 X_2} \sup_{p(x_1)} I(X_1; X_2|\overline{Z})$.

C. New lower bound on the SK_C capacity

Theorem 4: Assume that $a \leq b$ are two arbitrary natural numbers and (U_1, U_2, \dots, U_b) are arbitrary finite random variables satisfying the following properties:

- $p(U_1, U_2, \dots, U_b | X_1, X_2, X_3, \dots, X_m, Z) = \prod_{k=1}^b p(U_k | U_{1:k-1} X_{j_k})$ where $1 \leq j_k \leq m$ is such that $j_k = k$ modulo m ;
- $U_k = 0$ whenever $u + 1 \leq j_k \leq m$ where j_k is defined as above.⁴

$C_{CH}(u, q(x_2, x_3, \dots, x_m, z | x_1))$ is bounded from below by

$$\sup_{p(x_1)} \sum_{j=a}^b [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$$

where $(X_1, X_2, \dots, X_m, Z, U_1, \dots, U_b)$ inside the supremum has joint distribution

$$p(x_1) q(x_2, x_3, \dots, x_m, z | x_1) p(u_1, u_2, \dots, u_b | x_1, x_2, x_3, \dots, x_m, z).$$

In the case of $m = 2$, the new lower bound on $C_{CH}(2, q(x_2, z | x_1))$ derived by taking supremum over all valid $(a, b, U_1, U_2, \dots, U_b)$ strictly improves the $\sup_{p(x_1)} [\max(S(X_1; X_2^{(s)} \| Z), S(X_1^{(s)}; X_2 \| Z))]$ lower bound, where in this expression, $S(X_1; X_2^{(s)} \| Z)$ is the source model one-way secret key capacity from X_1 to X_2 in the presence of Z .

⁴By $U_k = 0$, we mean $P(U_k = 0) = 1$, in effect meaning that the alphabet set for U_k is of size one.

Discussion: $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ is bounded from below by (see the first part of the paper for the definition of the source model secret key capacity)

$$\sup_{p(x_1)} S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z),$$

because given any $p(x_1)$ and a source model key generation scheme for $S(X_1; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z)$, one can simulate the scheme in the channel model [10]. More specifically, let $\text{SK}(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \mathbf{C})$ denote the secret key generation scheme. Let the first terminal insert i.i.d. copies of X_1 at the input of the DMBC for n stages, and let the first $n - 1$ public discussions $\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{n-1}$ be vacuous, and let \mathbf{C}_n to be equal to the source model discussion \mathbf{C} . The same secret keys $S_1, S_2, S_3, \dots, S_m$ are then created at the end of the scheme.

We can then apply Theorem 7 of the first part of the paper to bound $S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z)$ from below by

$$\sum_{j=a}^b [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})].$$

The proof will establish that in the case of $u = m = 2$, this new lower bound represents an strict improvement over the

$$\sup_{p(x_1)} [\max(S(X_1; X_2^{(s)} \| Z), S(X_1^{(s)}; X_2 \| Z))]$$

lower bound. ■

IV. PROOFS OF THEOREMS

Proof: [Proof of Theorem 1] Fix a probability distribution $q(x_2, x_3, \dots, x_m, z|x_1)$ and assume that X_1, X_2, \dots, X_m and Z take values from finite sets $\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_m, \mathcal{Z}$. For every $\delta > 0$ and $\epsilon > 0$, one can find a valid secret key generation scheme, $\text{SK}_C(n, \epsilon, S_1, S_2, S_3, \dots, S_m, \mathbf{C}, M_1, M_2, \dots, M_u, X_1^n, X_2^n, \dots, X_m^n, Z^n)$, whose secret key rate is within δ of $C_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z|x_1))$. Furthermore without loss of generality we can add the uniformity condition $\frac{1}{n} \log |\mathcal{S}_1| < \frac{1}{n} H(S_1) + \epsilon$.⁵ Following the

⁵This point is argued in [10], or Lemma 5 of [13]. Please see the discussion following definition 2 of the first part of the paper for details.

secret key generation scheme, we can write the following chain of inequalities:

$$\begin{aligned}
& (n-1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, x_3, \dots, x_m, z|x_1)) \\
& \geq (n-1)\phi(q(x_2, \dots, x_m, z|x_1)) + \varphi(X_1^1; X_2^1; \dots; X_m^1 \| Z^1) \\
& \geq (n-1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) + \varphi(M_1 X_1^1; M_2 X_2^1; \dots; M_u X_u^1; X_{u+1}^1 \dots X_m^1 \| Z^1) \quad (23)
\end{aligned}$$

$$\begin{aligned}
& \geq (n-1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) \\
& + \varphi(M_1 X_1^1 C_{1,1}; M_2 X_2^1 C_{1,1}; \dots; M_u X_u^1 C_{1,1}; X_{u+1}^1 C_{1,1} \dots X_m^1 C_{1,1} \| Z^1 C_{1,1}) \quad (24) \\
& \geq (n-1)\phi(q(x_2, x_3, \dots, x_m, z|x_1))
\end{aligned}$$

$$\begin{aligned}
& + \varphi(M_1 X_1^1 C_{1,1} C_{1,2}; \dots; M_u X_u^1 C_{1,1} C_{1,2}; X_{u+1}^1 C_{1,1} C_{1,2} \dots X_m^1 C_{1,1} C_{1,2} \| Z^1 C_{1,1} C_{1,2}) \quad (25) \\
& \geq \dots
\end{aligned}$$

$$\begin{aligned}
& \geq (n-1)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) \\
& + \varphi(M_1 X_1^1 \mathbf{C}_1; M_2 X_2^1 \mathbf{C}_1; \dots; M_u X_u^1 \mathbf{C}_1; X_{u+1}^1 \mathbf{C}_1 \dots X_m^1 \mathbf{C}_1 \| Z^1 \mathbf{C}_1) \\
& \geq (n-2)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) \\
& + \varphi(M_1 X_1^{1:2} \mathbf{C}_1; M_2 X_2^{1:2} \mathbf{C}_1; \dots; M_u X_u^{1:2} \mathbf{C}_1; X_{u+1}^{1:2} \mathbf{C}_1 \dots X_m^{1:2} \mathbf{C}_1 \| Z^{1:2} \mathbf{C}_1) \quad (26)
\end{aligned}$$

$$\begin{aligned}
& \geq (n-2)\phi(q(x_2, x_3, \dots, x_m, z|x_1)) \\
& + \varphi(M_1 X_1^{1:2} \mathbf{C}_{1,2}; M_2 X_2^{1:2} \mathbf{C}_{1,2}; \dots; M_u X_u^{1:2} \mathbf{C}_{1,2}; X_{u+1}^{1:2} \mathbf{C}_{1,2} \dots X_m^{1:2} \mathbf{C}_{1,2} \| Z^{1:2} \mathbf{C}_{1,2}) \quad (27) \\
& \geq (n-3)\phi(q(x_2, x_3, \dots, x_m, z|x_1))
\end{aligned}$$

$$\begin{aligned}
& + \varphi(M_1 X_1^{1:3} \mathbf{C}_{1,2}; M_2 X_2^{1:3} \mathbf{C}_{1,2}; \dots; M_u X_u^{1:3} \mathbf{C}_{1,2}; X_{u+1}^{1:3} \mathbf{C}_{1,2} \dots X_m^{1:3} \mathbf{C}_{1,2} \| Z^{1:3} \mathbf{C}_{1,2}) \quad (28) \\
& \geq \dots
\end{aligned}$$

$$\begin{aligned}
& \geq \varphi(M_1 X_1^{1:n} \mathbf{C}_{1,n}; M_2 X_2^{1:n} \mathbf{C}_{1,n}; \dots; M_u X_u^{1:n} \mathbf{C}_{1,n}; X_{u+1}^{1:n} \mathbf{C}_{1,n} \dots X_m^{1:n} \mathbf{C}_{1,n} \| Z^{1:n} \mathbf{C}_{1,n}) \quad (29) \\
& \geq \varphi(S_1; S_2; \dots; S_m \| Z^{1:n} \mathbf{C}_{1,n}) \quad (30)
\end{aligned}$$

$$\geq H(S_1 | Z^{1:n} \mathbf{C}_{1,n}) - \sum_{j=2}^m H(S_1 | S_j) \quad (31)$$

$$\geq nC_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z|x_1)) - n\delta - (m-1)[h(\epsilon) + \epsilon \cdot \log |S_1|], \quad (32)$$

where equation (23) holds because of condition 5 of Theorem 1; equation (24) holds because of condition 2 and the fact that $H(C_{1,1} | M_1 X_1^1) = 0$; equation (25) holds because of condition 2 and the fact that $H(C_{1,2} | M_2 X_2^1 C_{1,1}) = 0$; equation (26) holds because of condition 1; equation (27) is true because we can repeatedly invoke condition 2 for the individual communications of \mathbf{C}_2 ; equation (28) holds because

of condition 1; equation (29) holds because of condition 3; equation (30) holds because of condition 4; and equation (31) is a consequence of Fano's inequality and the fact that the secret key rate of the protocol is within δ of $C_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z|x_1))$.

The above inequalities show that

$$\frac{n-1}{n} \phi(q(x_2, x_3, \dots, x_m, z|x_1)) \geq C_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z|x_1)) - \delta - \frac{m-1}{n} h(\epsilon) - (m-1)\epsilon \frac{1}{n} \log |\mathcal{S}_1| - \frac{1}{n} \sup_{q(x_1)} \varphi(q(x_1) \cdot q(x_2, x_3, \dots, x_m, z|x_1)).$$

Note that $\frac{1}{n} \log |\mathcal{S}_1| < \frac{1}{n} H(\mathcal{S}_1) + \epsilon < C_{CH}^\epsilon(u, q(x_2, x_3, \dots, x_m, z|x_1)) + \delta + \epsilon$. The theorem is proved by first taking the limit as $n \rightarrow \infty$, and then letting ϵ and δ converge zero. ■

Proof: [Proof of Theorem 2] Fix a $\Lambda = (\lambda_B, B \subseteq [m])$ in the set V . In order to prove this theorem, it is enough to verify the five conditions of Theorem 1 when we set:

$$\begin{aligned} \varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m \| \widehat{Z}) &= \inf_J \left(H(\widehat{X}_1 \dots \widehat{X}_m | J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J) \right. \\ &\quad \left. + I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J \| \widehat{Z}) \right), \end{aligned} \quad (33)$$

$$\phi(p(x_2, x_3, \dots, x_m, z|x_1)) = \sup_{p(x_1)} \varphi(p(x_1) \cdot p(x_2, x_3, \dots, x_m, z|x_1)), \quad (34)$$

where the infimum is over finite random variables J arbitrarily distributed with $\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z}$, and $\tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J)$ is defined as in the statement of the Theorem. In Appendix I, we show that this choice satisfies the five conditions of Theorem 1, thus completing the proof. ■

Proof: [Proof of Theorem 3] Since $m = 2$, for simplicity we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. In order to prove that this bound strictly improves $\sup_{p(x)} \inf_{\overline{Z} \rightarrow Z \rightarrow XY} I(X; Y | \overline{Z})$ we use the example of Renner and Wolf in [7]. X and Y take values from the set $\{0, 1, 2, 3\}$. Assuming that $P(X = i) = p_i$, Table (II) characterizes the conditional probability distribution of Y given X . The conditional distribution of Z given X and Y is specified by the following equation:

$$Z = \begin{cases} (X + Y) \bmod 2 & \text{if } X \in \{0, 1\} \\ X \bmod 2 & \text{if } X \in \{2, 3\} \end{cases}$$

Renner and Wolf proved that for the choice of $p_i = \frac{1}{4}$ for $i = 0, 1, 2, 3$ and $U = \lfloor \frac{X}{2} \rfloor$, one has

$$I(X; Y \downarrow Z) = \frac{3}{2} \quad I(X; Y \downarrow ZU) = 0$$

where $I(X; Y \downarrow Z)$, known as the intrinsic information is defined as $\inf_{\overline{Z} \rightarrow Z \rightarrow XY} I(X; Y | \overline{Z})$ [7].

Therefore

$$\sup_{p(x)} [I(X; Y \downarrow Z)] \geq \frac{3}{2}$$

TABLE II
JOINT PROBABILITY DISTRIBUTION OF X AND Y

X Y	0	1	2	3
0	$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
1	$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
2	0	0	p_2	0
3	0	0	0	p_3

The proof will be completed if we can show that $\sup_{p(x)} \min_J [I(X; Y|J) + I(XY; J|Z)] < \frac{3}{2}$. We show that $\sup_{p(x)} \min_J [I(X; Y|J) + I(XY; J|Z)]$ is in fact less than or equal to one.

Let

$$J_0 = \begin{cases} U & \text{if } U=0 \\ UZ & \text{if } U=1 \end{cases}$$

We can upper bound $\sup_{p(x)} \min_J [I(X; Y|J) + I(XY; J|Z)]$ by $\sup_{p(x)} [I(X; Y|J_0) + I(XY; J_0|Z)]$.

Since $I(X; Y|J_0) = 0$ and $I(XY; J_0|Z) \leq 1$ for all $p(x)$, $\sup_{p(x)} \min_J [I(X; Y|J) + I(XY; J|Z)]$ is less than or equal to one. ■

Proof: [Proof of Theorem 4] $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ is bounded from below by

$$\sup_{p(x_1)} S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z).$$

This is argued in the discussion following the statement of Theorem 4. We apply Theorem 7 of the first part of this paper to bound

$S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z)$ from below by

$\sum_{j=a}^b [\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$. Therefore $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ is bounded from below by

$$\sup_{p(x_1)} \left[\sum_{j=a}^b \left[\min_{1 \leq r \leq m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1}) \right] \right]. \quad (35)$$

For the case of $u = m = 2$, for simplicity we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. We first prove that the new lower bound on $C_{CH}(2, q(y, z|x))$ is always greater than or equal to $\sup_{p(x)} [\max(S(X; Y^{(s)} \| Z), S(X^{(s)}; Y \| Z))]$.

Take some arbitrary $p(x)$, and consider random variables X , Y and Z with the joint distribution $p(x)q(y, z|x)$. Take arbitrary random variables V_1 and V_2 satisfying the Markov chain $V_2 \rightarrow V_1 \rightarrow X \rightarrow YZ$. Specializing equation (35) to $a = b = 3$, the chosen $p(x)$, and $(U_1, U_2, U_3) = (V_2, 0, V_1)$ ⁶, one can show that $C_{CH}(2, q(y, z|x)) \geq I(V_2; Y|V_1) - I(V_2; Z|V_1)$. Therefore the new lower bound is always greater than or equal to $\sup_{p(x)} S(X; Y^{(s)}||Z)$. By symmetry, it is greater than or equal to $\sup_{p(x)} S(X; Y^{(s)}||Z)$. Thus,

$$C_{CH}(2, q(y, z|x)) \geq \sup_{p(x)} [\max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z))].$$

Next, we construct an example to show that there are cases in which the new lower bound outperforms $\sup_{p(x)} [\max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z))]$. Our example is in part motivated by example and proof technique of Ahlswede and Csiszár in [1].

Assume that $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$, $Z = (Z_1, Z_2)$. The conditional distribution of (Y_1, Y_2, Z_1, Z_2) given X_1 and X_2 is defined in Figure 1 in terms of ϵ , a parameter in the interval of $[0, 1]$. We prove that the new lower bound and the upper bound $\sup_{p(x)} I(X; Y|Z)$ match in this case, implying that $C_{CH}(2, q(y, z|x)) = \sup_{p(x)} I(X; Y|Z)$. But on the other hand, we show that

$$\sup_{p(x)} I(X; Y|Z) > \sup_{p(x)} [\max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z))], \quad (36)$$

meaning that the previously known lower bound does not close the gap.

We begin by showing that the supremum $\sup_{p(x)} I(X; Y|Z)$ is *uniquely* achieved at a uniform distribution on X , i.e. when $p(x) = \frac{1}{4}$ for all $x = (x_1, x_2) \in \{0, 1\} \times \{0, 1\}$. In other words, the supremum is uniquely achieved when X_1 and X_2 are independent uniform binary random variables. In Appendix II, with reference to Figure 1 with $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$ and $Z = (Z_1, Z_2)$, it is shown that for any $0 < \epsilon < 1$, $I(X; Y|Z)$ *strictly increases* when

- X_1 and X_2 are not independent and we replace $p(X_1, X_2)p(Y, Z|X)$ with $p(X_1)p(X_2)p(Y, Z|X)$, i.e. replacing the joint distribution of X_1, X_2 with the product of their marginal distributions;
- we change the marginal distribution of X_1 to a uniform distribution if X_1 and X_2 are independent, but X_1 is not uniform;
- we change the marginal distribution of X_2 to a uniform distribution if X_1 and X_2 are independent, but X_2 is not uniform.

Therefore the supremum $\sup_{p(x)} I(X; Y|Z)$ is uniquely achieved when X_1 and X_2 are independent uniform binary random variables.

⁶By $U_2 = 0$, we mean that the finite random variable U_2 takes on the value 0 with probability one.

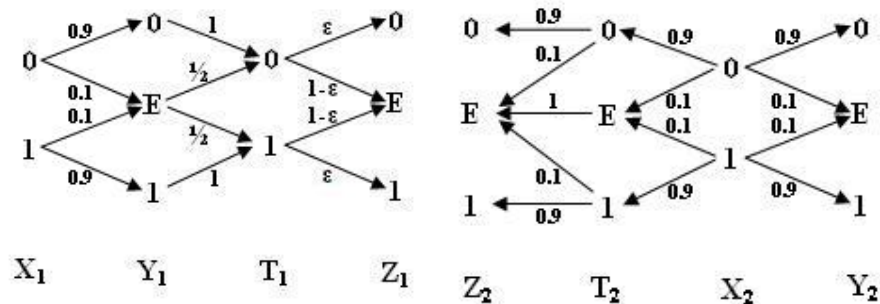


Fig. 1. The conditional distribution of (Y_1, Y_2, Z_1, Z_2) given X_1 and X_2 .

When X_1 and X_2 are independent, the pairs (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) will become independent, and we will have: $I(X; Y|Z) = I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$. Since $X_1 \rightarrow Y_1 \rightarrow Z_1$ and $Y_2 \rightarrow X_2 \rightarrow Z_2$, the sum $I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$ will be equal to $I(X_1; Y_1) - I(X_1; Z_1) + I(Y_2; X_2) - I(Y_2; Z_2)$. The latter secrecy rate can be seen to be achievable via the choice of $a = 1$, $b = 2$, $(U_1, U_2) = (X_1, Y_2)$ in equation (35).

Now, we will prove equation (36). Since

$$\forall p(x), \quad I(X; Y|Z) \geq \max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z)),$$

and that the supremum $\sup_{p(x)} I(X; Y|Z)$ is *uniquely* achieved when X_1 and X_2 are independent uniform binary random variables, it suffices to show that $I(X; Y|Z) > \max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z))$ when X_1 and X_2 are independent uniform binary random variables. In the proof of Theorem 7 of the first part of this paper, we have considered exactly the same joint distribution on X , Y and Z , and have shown that $I(X; Y|Z)$ strictly exceeds $\max(S(X; Y^{(s)}||Z), S(X^{(s)}; Y||Z))$. In order to avoid duplication, the argument is not repeated here. ■

V. RELATION OF THE SECRET KEY CAPACITY SOURCE MODEL AND CHANNEL MODEL

The exact relation of the secret key capacity under the channel model and source model remains an open problem. Both the new lower bound and the new upper bound have the generic form of

$$\sup_{p(x_1)} F(p(x_1)q(x_2, x_3, \dots, x_m, z|x_1))$$

for some upper bound $F(p(x_1, x_2, x_3, \dots, x_m, z))$ on $S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)}||Z)$.

One can then conjecture that $C_{CH}(u, q(x_2, x_3, \dots, x_m, z|x_1))$ equals

$$\sup_{p(x_1)} S(X_1; X_2; \dots; X_u; X_{u+1}^{(s)}; \dots; X_m^{(s)} \| Z).$$

If true, using the Theorem 5 of the first part of this paper for $m = 2$, one can bound $C_{CH}(2, q(y, z|x))$ from above by

$$\sup_{p(x_1)} \inf_J f^{-1}\{f(S(X_1; X_2; \dots; X_u; (X_{u+1})^{(s)}; \dots; (X_m)^{(s)} \| J)) + S_{f\text{-one-way}}(X_1 X_2 \dots X_m; J^{(s)} \| Z)\}$$

$f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$ is an arbitrary strictly increasing convex function, and $f\text{-one-way secrecy rate}$ is defined as

$$S_{f\text{-one-way}}(X; Y^{(s)} \| Z) = \sup_{V \rightarrow U \rightarrow X \rightarrow YZ} [f(H(U|ZV)) - f(H(U|YV))].$$

We do not know if this expression actually serves as an upper bound on $C_{CH}(2, q(y, z|x))$ for all appropriate choices of f , or less ambitiously for the particular choice of $f(x) = x$. If it does, it may represent a strict improvement over previous bounds. Otherwise, it will be evidence against the original conjecture.

APPENDIX I

In this Appendix, we prove that $\varphi(\cdot)$, proposed in equation (33) satisfies the five properties of Theorem

1. Recall that the elements of the vector $\Lambda = (\lambda_B, B \subseteq [m])$ satisfy equation (17). Let

$$\begin{aligned} \theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J \| \widehat{Z}) &\doteq \\ H(\widehat{X}_1 \dots \widehat{X}_u | J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J) + I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J \| \widehat{Z}), \end{aligned}$$

where $\tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J)$ is as in the statement of Theorem 2. We can then re-express equation (33) as

$$\varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m \| \widehat{Z}) = \inf_J (\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J \| \widehat{Z})),$$

where the infimum is over finite random variables J arbitrarily distributed with $\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z}$.

Property 1.

It is required to verify that:

$$\begin{aligned} \inf_{\tilde{J}} (\theta^\Lambda(\widehat{X}_1 X_1; \widehat{X}_2 X_2; \widehat{X}_3 X_3; \dots; \widehat{X}_m X_m; \tilde{J} \| \widehat{Z})) &\leq \\ \inf_{\tilde{J}'} (\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; \tilde{J}' \| \widehat{Z})) + \phi(q(x_2, x_3, \dots, x_m, z|x_1)). \end{aligned} \quad (37)$$

$\phi(q(x_2, x_3, \dots, x_m, z|x_1))$ is by definition greater than or equal to $\varphi(X_1; X_2; \dots; X_m \| Z)$ which is equal to

$$\inf_{\tilde{J}''} (\theta^\Lambda(X_1; X_2; X_3; \dots; X_m; \tilde{J}'' \| Z)).$$

In order to show equation (37), it suffices to prove that for any J'' , the following inequality holds:

$$\begin{aligned} & \inf_{\tilde{J}} \theta^\Lambda(\widehat{X}_1 X_1; \widehat{X}_2 X_2; \widehat{X}_3 X_3; \dots; \widehat{X}_m X_m; \tilde{J} \| \widehat{Z} Z) \leq \\ & \inf_{\tilde{J}'} \theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; \tilde{J}' \| \widehat{Z}) + \theta^\Lambda(X_1; X_2; X_3; \dots; X_m; J'' \| Z). \end{aligned} \quad (38)$$

Without loss of generality, we can further assume that

$$\tilde{J}' \rightarrow \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m \widehat{Z} \rightarrow \widehat{X}_1 \rightarrow X_1 \rightarrow X_1 X_2 \dots X_m Z \rightarrow J''$$

because the two terms on the right hand side of equation (38) depend only on $p(\tilde{J}' | \widehat{X}_1 \dots \widehat{X}_m \widehat{Z})$ and $p(J'' | X_1 \dots X_m Z)$.

In order to prove equation (38), it would be enough to show that for any arbitrary J' satisfying

$$J' \rightarrow \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m \widehat{Z} \rightarrow \widehat{X}_1 \rightarrow X_1 \rightarrow X_1 X_2 \dots X_m Z \rightarrow J'',$$

the following inequality holds:

$$\begin{aligned} & \theta^\Lambda(\widehat{X}_1 X_1; \widehat{X}_2 X_2; \widehat{X}_3 X_3; \dots; \widehat{X}_m X_m; J' J'' \| \widehat{Z} Z) \leq \\ & \theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J' \| \widehat{Z}) + \theta^\Lambda(X_1; X_2; X_3; \dots; X_m; J'' \| Z). \end{aligned}$$

We claim that the following two inequalities hold:

$$\begin{aligned} & H(\widehat{X}_1 \dots \widehat{X}_u X_1 \dots X_u | J', J'') - \tau^\Lambda(\widehat{X}_1 X_1, \dots, \widehat{X}_u X_u, (\widehat{X}_{u+1} X_{u+1})^{(s)}, \dots, (\widehat{X}_m X_m)^{(s)} \| J' J'') \\ & \leq H(\widehat{X}_1 \dots \widehat{X}_u | J') - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J') + \\ & H(X_1 \dots X_u | J'') - \tau^\Lambda(X_1, X_2, \dots, X_u, X_{u+1}^{(s)}, \dots, X_m^{(s)} \| J''), \end{aligned} \quad (39)$$

and

$$I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m X_1 X_2 \dots X_m; J' J'' | \widehat{Z} Z) \leq I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J' | \widehat{Z}) + I(X_1 X_2 \dots X_m; J'' | Z). \quad (40)$$

Starting from the last inequality:

$$\begin{aligned} & I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m X_1 X_2 \dots X_m; J' J'' | \widehat{Z} Z) = H(J' J'' | \widehat{Z} Z) - H(J' J'' | \widehat{Z} Z \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m X_1 X_2 \dots X_m) \leq \\ & H(J' | \widehat{Z} Z) + H(J'' | \widehat{Z} Z) - H(J' | \widehat{Z} Z \widehat{X}_1 \dots \widehat{X}_m X_1 \dots X_m) - H(J'' | J' \widehat{Z} Z \widehat{X}_1 \dots \widehat{X}_m X_1 \dots X_m) \leq^i \\ & H(J' | \widehat{Z}) + H(J'' | Z) - H(J' | \widehat{Z} \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m) - H(J'' | Z X_1 X_2 \dots X_m) = \\ & I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J' | \widehat{Z}) + I(X_1 X_2 \dots X_m; J'' | Z) \end{aligned}$$

In step i , we have used the Markov property

$$J' \rightarrow \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m \widehat{Z} \rightarrow \widehat{X}_1 \rightarrow X_1 \rightarrow X_1 X_2 \dots X_m Z \rightarrow J''.$$

It remains to prove the inequality (39). We first prove that for every set $B \subseteq [m]$:

$$\begin{aligned} & H(\widehat{X}_{B \cap [u]} X_{B \cap [u]} | \widehat{X}_{B^c} X_{B^c} J' J'') - H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') = \\ & (H(\widehat{X}_{B \cap [u]} | \widehat{X}_{B^c} J') - H(\widehat{X}_1 | \widehat{X}_{B^c} J')) + (H(X_{B \cap [u]} | X_{B^c} J'') - H(X_1 | X_{B^c} J'')). \end{aligned}$$

This equality is true because

$$\begin{aligned}
& H(\widehat{X}_{B \cap [u]} X_{B \cap [u]} | \widehat{X}_{B^c} X_{B^c} J' J'') = \\
& H(\widehat{X}_{B \cap [u]} X_{B \cap [u]} \widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') = \\
& H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') + H(\widehat{X}_{B \cap [u]} X_{B \cap [u]} | \widehat{X}_1 \widehat{X}_{B^c} X_{B^c} J' J'') =^i \\
& H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') + H(\widehat{X}_{B \cap [u]} | \widehat{X}_1 \widehat{X}_{B^c} X_{B^c} J' J'') + \\
& H(X_{B \cap [u]} | \widehat{X}_1 X_1 \widehat{X}_{B \cap [u]} \widehat{X}_{B^c} X_{B^c} J' J'') =^{ii} \\
& H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') + H(\widehat{X}_{B \cap [u]} | \widehat{X}_1 \widehat{X}_{B^c} J') + H(X_{B \cap [u]} | X_1 X_{B^c} J'') = \\
& H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') + H(\widehat{X}_{B \cap [u]} | \widehat{X}_{B^c} J') - H(\widehat{X}_1 | \widehat{X}_{B^c} J') + H(X_{B \cap [u]} | X_{B^c} J'') - H(X_1 | X_{B^c} J'').
\end{aligned}$$

In step i , we have used the fact that $H(X_1 | \widehat{X}_1) = 0$ and in step ii , we have used the Markov property

$$J' \rightarrow \widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m \widehat{Z} \rightarrow \widehat{X}_1 \rightarrow X_1 \rightarrow X_1 X_2 \dots X_m Z \rightarrow J''.$$

This property lets us to rewrite the inequality we would like to prove in a new form:

$$\begin{aligned}
& H(\widehat{X}_1 | J', J'') - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J', J'') \leq \\
& H(\widehat{X}_1 | J') - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(\widehat{X}_1 | \widehat{X}_{B^c} J') + \\
& H(X_1 | J'') - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(X_1 | X_{B^c} J'')
\end{aligned}$$

Further, we can restrict the summation on those sets B such that $1 \in B$ (otherwise the term in question would be zero).

Using equation (17), and by setting $R_1 = 1$, and $R_j = 0$ for $1 < j \leq u$, one can get:

$$\sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], 1 \in B} \lambda_B = 1$$

Therefore

$$\begin{aligned}
& H(\widehat{X}_1 | J', J'') - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], 1 \in B} \lambda_B H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'') = \\
& \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], 1 \in B} \lambda_B [H(\widehat{X}_1 | J', J'') - H(\widehat{X}_1 | \widehat{X}_{B^c} X_{B^c} J' J'')] = \\
& \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], 1 \in B} \lambda_B I(\widehat{X}_1; \widehat{X}_{B^c} X_{B^c} | J' J'').
\end{aligned}$$

Similarly we can rewrite the two other expressions. It would be then enough to prove that

$$I(\widehat{X}_1; \widehat{X}_{B^c} X_{B^c} | J' J'') \leq I(\widehat{X}_1; \widehat{X}_{B^c} | J') + I(X_1; X_{B^c} | J'')$$

for all $B \subseteq [m]$ such that $B \neq [m]$ and $1 \in B$.

We have:

$$\begin{aligned}
& I(\widehat{X}_1; \widehat{X}_{B^c} X_{B^c} | J' J'') = H(\widehat{X}_{B^c} X_{B^c} | J' J'') - H(\widehat{X}_{B^c} X_{B^c} | J' J' \widehat{X}_1) \leq \\
& H(\widehat{X}_{B^c} | J') + H(X_{B^c} | J'') - H(\widehat{X}_{B^c} X_{B^c} | J' J' \widehat{X}_1) =^i \\
& H(\widehat{X}_{B^c} | J') + H(X_{B^c} | J'') - H(\widehat{X}_{B^c} | J' \widehat{X}_1) - H(X_{B^c} | J'' X_1) = \\
& I(\widehat{X}_1; \widehat{X}_{B^c} | J') + I(X_1; X_{B^c} | J'').
\end{aligned}$$

In step i , we have used $H(X_1|\widehat{X}_1) = 0$ and the Markov property

$$J' \rightarrow \widehat{X}_1\widehat{X}_2\dots\widehat{X}_m\widehat{Z} \rightarrow \widehat{X}_1 \rightarrow X_1 \rightarrow X_1X_2\dots X_mZ \rightarrow J''.$$

Property 2.

Let $1 \leq i \leq u$ and let $H(F|\widehat{X}_i) = 0$. We need to prove that:

$$\inf_{\tilde{J}}(\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; \tilde{J}|\widehat{Z})) \geq \inf_{\tilde{J}'}(\theta^\Lambda(\widehat{X}_1F; \widehat{X}_2F; \widehat{X}_3F; \dots; \widehat{X}_mF; \tilde{J}'|\widehat{Z}F))$$

It is enough to prove that for any J , there is a J' such that:

$$\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J|\widehat{Z}) \geq \theta^\Lambda(\widehat{X}_1F; \widehat{X}_2F; \widehat{X}_3F; \dots; \widehat{X}_mF; J'|\widehat{Z}F)$$

Let $J' = JF$. Since $I(F; J | \widehat{Z}) \geq 0$, one can show that the above inequality would hold if:

$$H(F|J) - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(F|\widehat{X}_{B^c}J) \geq 0.$$

Since $H(F|\widehat{X}_i) = 0$, we can rewrite the above inequality as follows:

$$H(F|J) - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], i \in B} \lambda_B H(F|\widehat{X}_{B^c}J) \geq 0.$$

$H(F|\widehat{X}_{B^c}J)$ is bounded from above by $H(F|J)$ hence

$$\begin{aligned} H(F|J) - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], i \in B} \lambda_B H(F|\widehat{X}_{B^c}J) &\geq \\ H(F|J) \cdot (1 - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], i \in B} \lambda_B) & \end{aligned}$$

But $1 - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], i \in B} \lambda_B = 0$. This could be proved by setting $R_i = 1$, and $R_j = 0$ for any $1 \leq j \leq u$, $j \neq i$ in equation (17). ■

Property 3.

We need to prove that:

$$\inf_{\tilde{J}}(\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; \tilde{J}|\widehat{Z})) \geq \inf_{\tilde{J}'}(\theta^\Lambda(\widehat{X}'_1; \widehat{X}'_2; \widehat{X}'_3; \dots; \widehat{X}'_m; \tilde{J}'|\widehat{Z})).$$

It is enough to prove that for any J :

$$\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J|\widehat{Z}) \geq \theta^\Lambda(\widehat{X}'_1; \widehat{X}'_2; \widehat{X}'_3; \dots; \widehat{X}'_m; J|\widehat{Z})$$

It is clear that $I(\widehat{X}_1\widehat{X}_2\dots\widehat{X}_m; J|\widehat{Z}) \geq I(\widehat{X}'_1\widehat{X}'_2\dots\widehat{X}'_m; J|\widehat{Z})$. It remains to show that the first two terms of the expression, that is $H(\widehat{X}_1\dots\widehat{X}_u|J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)}|J)$, does not increase when we replace $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z}, J)$ with $(\widehat{X}'_1, \widehat{X}'_2, \dots, \widehat{X}'_m, \widehat{Z}, J)$.

Since we can replace the components of $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m)$ with $(\widehat{X}'_1, \widehat{X}'_2, \dots, \widehat{X}'_m)$ one at a time, it is enough to consider the case that we only change one component, that is we replace $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m)$ by

$$(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_{j-1}, \widehat{X}'_j, \widehat{X}_{j+1}, \dots, \widehat{X}_m).$$

The proof can be completed by considering the two cases of $j > u$ and $j \leq u$ separately. In the case $j > u$, we note that $\tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J)$ increases term by term while $H(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_u | J)$ remains constant. In case $j \leq u$, we note that for every set B that does not contain j , the term $-\lambda_B H(\widehat{X}_{B \cap [u]} | \widehat{X}_{B^c} J)$ decreases as we replace \widehat{X}_j by \widehat{X}'_j . If the set B includes j , we have:

$$\begin{aligned} H(\widehat{X}_{B \cap [u]} | \widehat{X}_{B^c} J) &= H(\widehat{X}_{B \cap [u] - \{j\}} \widehat{X}_j | \widehat{X}_{B^c} J) = H(\widehat{X}_{B \cap [u] - \{j\}} \widehat{X}'_j | \widehat{X}_{B^c} J) = \\ H(\widehat{X}_{B \cap [u] - \{j\}} \widehat{X}'_j | \widehat{X}_{B^c} J) &+ H(\widehat{X}_j | \widehat{X}'_j \widehat{X}_{B^c} \widehat{X}_{B \cap [u] - \{j\}} J) \leq \\ H(\widehat{X}_{B \cap [u] - \{j\}} \widehat{X}'_j | \widehat{X}_{B^c} J) &+ H(\widehat{X}_j | \widehat{X}'_j \widehat{X}_{[u] - \{j\}} J) \end{aligned}$$

So, in order to prove the inequality, it would be enough to prove that

$$H(\widehat{X}_j | \widehat{X}'_j \widehat{X}_{[u] - \{j\}} J) - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], j \in B} \lambda_B H(\widehat{X}_j | \widehat{X}'_j \widehat{X}_{[u] - \{j\}} J) \geq 0.$$

But the left hand side is zero since $\sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m], j \in B} \lambda_B = 1$. ■

Property 4.

Equation (21) implies that for any random variable J arbitrarily correlated with $\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m$ and \widehat{Z} we have:

$$\begin{aligned} S(\widehat{X}_1 J; \widehat{X}_2 J; \dots; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)}; \dots; (\widehat{X}_m J)^{(s)} \| J) &\leq \\ H(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_u | J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J). \end{aligned}$$

Therefore

$$\begin{aligned} \inf_J (S(\widehat{X}_1 J; \widehat{X}_2 J; \dots; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)}; \dots; (\widehat{X}_m J)^{(s)} \| J) &+ I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J \| \widehat{Z})) \leq \\ \inf_J (H(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_u | J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \| J) &+ I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J \| \widehat{Z})) \\ = \varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m \| \widehat{Z}). \end{aligned}$$

Thus,

$$\begin{aligned} \varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m \| \widehat{Z}) &\geq \\ \inf_J (S(\widehat{X}_1 J; \widehat{X}_2 J; \dots; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)} \dots; (\widehat{X}_m J)^{(s)} \| J) &+ I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J^{(s)} \| \widehat{Z})). \end{aligned} \quad (41)$$

According to Theorem 5 of the first part of the paper,

$$\begin{aligned} \inf_J (S(\widehat{X}_1 J; \widehat{X}_2 J; \dots; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)} \dots; (\widehat{X}_m J)^{(s)} \| J) &+ I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J^{(s)} \| \widehat{Z})) \\ \geq S(\widehat{X}_1; \widehat{X}_2; \dots; \widehat{X}_u; \widehat{X}_{u+1}^{(s)} \dots; \widehat{X}_m^{(s)} \| \widehat{Z}) \end{aligned} \quad (42)$$

Since Theorem 1 of the first part of the paper shows that $S(\widehat{X}_1; \widehat{X}_2; \dots; \widehat{X}_u; \widehat{X}_{u+1}^{(s)}; \dots; \widehat{X}_m^{(s)} \parallel \widehat{Z})$ satisfies the condition 4 of the same theorem, we have

$$S(\widehat{X}_1; \widehat{X}_2; \dots; \widehat{X}_u; \widehat{X}_{u+1}^{(s)}; \dots; \widehat{X}_m^{(s)} \parallel \widehat{Z}) \geq H(\widehat{X}_1 \parallel \widehat{Z}) - \sum_{i=2}^m H(\widehat{X}_1 \parallel \widehat{X}_i) \quad (43)$$

Equations (41), (42) and (43) imply that $\varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m \parallel \widehat{Z}) \geq H(\widehat{X}_1 \parallel \widehat{Z}) - \sum_{i=2}^m H(\widehat{X}_1 \parallel \widehat{X}_i)$. ■

Property 5.

We need to prove that

$$\inf_{\widetilde{J}} (\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; \widetilde{J} \parallel \widehat{Z})) \geq \inf_{\widetilde{J}'} (\theta^\Lambda(\widehat{X}_1 M_1; \widehat{X}_2 M_2; \dots; \widehat{X}_u M_u; \widehat{X}_{u+1} \dots; \widehat{X}_m; \widetilde{J}' \parallel \widehat{Z})),$$

where the first infimum is taken over finite random variable \widetilde{J} arbitrarily distributed with $\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m$ and \widehat{Z} ; and the second infimum is taken over finite random variable \widetilde{J}' arbitrarily distributed with $\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z}, M_1, M_2, \dots, M_u$.

It is enough to prove that for any J , there is a J' such that:

$$\theta^\Lambda(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; \dots; \widehat{X}_m; J \parallel \widehat{Z}) \geq \theta^\Lambda(\widehat{X}_1 M_1; \widehat{X}_2 M_2; \dots; \widehat{X}_u M_u; \widehat{X}_{u+1} \dots; \widehat{X}_m; J' \parallel \widehat{Z})$$

We define J' in a way that it has the same joint distribution with $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z})$ as J has, and furthermore $(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_m, \widehat{Z}, J')$ is independent of $M_1 M_2 \dots M_u$. One can then prove that:

$$\begin{aligned} & H(\widehat{X}_1 M_1 \dots \widehat{X}_u M_u \parallel J') - \tau^\Lambda(\widehat{X}_1 M_1, \widehat{X}_2 M_2, \dots, \widehat{X}_u M_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \parallel J') + \\ & I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m M_1 \dots M_u; J' \parallel \widehat{Z}) = \\ & H(\widehat{X}_1 \dots \widehat{X}_u \parallel J) - \tau^\Lambda(\widehat{X}_1, \widehat{X}_2, \dots, \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, \dots, \widehat{X}_m^{(s)} \parallel J) + I(\widehat{X}_1 \widehat{X}_2 \dots \widehat{X}_m; J \parallel \widehat{Z}) + \\ & H(M_1) + \dots + H(M_u) - \\ & \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B \sum_{i \in B \cap [u]} H(M_i) \end{aligned}$$

But $H(M_1) + H(M_2) + \dots + H(M_u) - \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B \sum_{i \in B \cap [u]} H(M_i)$ is zero. This could be proved using equation (17) and by setting $R_j = H(M_j)$ for $1 \leq j \leq u$. ■

APPENDIX II

In this Appendix, we will prove that with reference to Figure 1 with $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$ and $Z = (Z_1, Z_2)$, for any $0 < \epsilon < 1$, $I(X; Y \parallel Z)$ strictly increases when

- X_1 and X_2 are not independent and we replace $p(X_1, X_2)p(Y, Z \parallel X)$ with $p(X_1)p(X_2)p(Y, Z \parallel X)$, i.e. replacing the joint distribution of X_1, X_2 with the product of their marginal distributions;
- we change the marginal distribution of X_1 to a uniform distribution if X_1 and X_2 are independent, but X_1 is not uniform;

- we change the marginal distribution of X_2 to a uniform distribution if X_1 and X_2 are independent, but X_2 is not uniform.

Case 1:

$$I(X; Y|Z) = I(X_1 X_2; Y_1 Y_2 | Z_1 Z_2) = H(Y_1 Y_2 | Z_1 Z_2) - H(Y_1 Y_2 | Z_1 Z_2 X_1 X_2).$$

Since $Y_1 Z_1 \rightarrow X_1 \rightarrow X_2 \rightarrow Y_2 Z_2$, we can work out the second term

$$H(Y_1 Y_2 | Z_1 Z_2 X_1 X_2) = H(Y_1 | Z_1 Z_2 X_1 X_2) + H(Y_2 | Z_1 Z_2 X_1 X_2 Y_1) = H(Y_1 | Z_1 X_1) + H(Y_2 | X_2 Z_2).$$

The first term can be bounded from above as follows:

$$H(Y_1 Y_2 | Z_1 Z_2) = H(Y_2 | Z_1 Z_2) + H(Y_1 | Z_1 Z_2 Y_2) \leq H(Y_2 | Z_2) + H(Y_1 | Z_1).$$

Therefore $I(X; Y|Z) \leq I(X_1; Y_1 | Z_1) + I(X_2; Y_2 | Z_2)$. This would mean that if we replace $p(X_1, X_2)p(Y, Z|X)$ with $p(X_1)p(X_2)p(Y, Z|X)$, $I(X; Y|Z)$ does not decrease.

We prove that $I(X; Y|Z)$ strictly increases by contradiction. Assume $I(X; Y|Z)$ does not increase. In this case, $H(Y_1 | Z_1 Z_2 Y_2)$ must be equal to $H(Y_1 | Z_1)$ implying that $I(Y_1; Y_2 | Z_1) = 0$. Since $Z_1 \rightarrow Y_1 \rightarrow Y_2$ form a Markov chain, the $I(Y_1; Y_2 | Z_1) = 0$ constraint implies that $I(Y_2; Z_1) = I(Y_2; Y_1)$. But since

$$I(Y_2; Y_1) \geq I(Y_2; T_1) \geq I(Y_2; Z_1),$$

we get $I(Y_2; T_1) = I(Y_2; Z_1)$.

$$I(Y_2; Z_1) = I(Y_2; Z_1, \mathbb{1}[Z_1 = E]) =$$

$$I(Y_2; \mathbb{1}[Z_1 = E]) + I(Y_2; Z_1 | \mathbb{1}[Z_1 = E]) = 0 + \epsilon \cdot I(Y_2; T_1).$$

Since $\epsilon < 1$, $I(Y_2; T_1) = I(Y_2; Z_1)$ can hold only when $I(Y_2; T_1) = I(Y_2; Z_1) = I(Y_2; Y_1) = 0$.

$$0 = I(Y_2; Y_1) = I(Y_2, \mathbb{1}[Y_2 = E]; Y_1, \mathbb{1}[Y_1 = E]) \geq$$

$$I(Y_2; Y_1 | \mathbb{1}[Y_2 = E], \mathbb{1}[Y_1 = E]) \geq$$

$$p(Y_2 \neq E) \cdot p(Y_1 \neq E) \cdot I(Y_2; Y_1 | Y_2 \neq E, Y_1 \neq E) = 0.81 I(X_1; X_2).$$

Therefore $I(X_1; X_2) = 0$ meaning that X_1 and X_2 are independent. This is a contradiction. ■

Case 2:

$I(X_1; Y_1 | Z_1) = I(X_1; Y_1) - I(X_1; Z_1) = H(Y_1) - H(Y_1 | X_1) - H(Z_1) + H(Z_1 | X_1)$ can be thought of as a function of $p(X_1 = 0) = a$. $H(Y_1 | X_1)$ and $H(Z_1 | X_1)$ are constant not depending on a . The marginal distribution of Z_1 equals $(\epsilon \cdot (0.9a + 0.05), 1 - \epsilon, \epsilon \cdot (-0.9a + 0.95))$, and the marginal distribution of Y_1 equals $(0.9a, 0.1, 0.9 - 0.9a)$. Therefore it is enough to show that $H(Y_1) - H(Z_1)$ reaches its maximum at and only at $a = 0.5$. This can be seen by noting that the derivative of $\frac{1}{0.9}(H(Y_1) - H(Z_1))$ with respect to a equals: $\log \frac{0.5 - (a - 0.5)}{0.5 + (a - 0.5)} - \epsilon \log \frac{0.5 - 0.9(a - 0.5)}{0.5 + 0.9(a - 0.5)}$ which is zero only at $a = 0.5$. ■

Case 3:

$$\begin{aligned} I(X_2; Y_2 | Z_2) &= I(X_2; (Y_2, \mathbb{1}[Y_2 = E]) | Z_2) = I(X_2; \mathbb{1}[Y_2 = E] | Z_2) + I(X_2; Y_2 | \mathbb{1}[Y_2 = E], Z_2) = \\ &= 0 + P(Y_2 = E) \cdot 0 + P(Y_2 \neq E) \cdot H(X_2 | Z_2) = 0.9 H(X_2 | Z_2). \end{aligned}$$

But $H(X_2|Z_2) = P(Z_2 = 0).0 + P(Z_2 = 1).0 + P(Z_2 = E).H(X_2)$. Therefore

$$I(X_2; Y_2|Z_2) = 0.9 * 0.19H(X_2).$$

We are done by noting that $H(X_2)$ strictly increases when the distribution of X_2 is changed to uniform.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments. The authors would like to thank TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies, for their support of this work. The research was also partially supported by NSF grant numbers CCF-0500234, CCF-0635372 and CNS-0627161.

REFERENCES

- [1] R. Ahlswede and I. Csiszár, “Common Randomness in Information Theory and Cryptography. Part I: Secret sharing”, *IEEE Trans. Inform. Theory*, Vol. 39, No. 4, July 1993, pp. 1121 -1132.
- [2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.
- [3] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages”, *IEEE Trans. Inform. Theory*, Vol. 24, No. 3, May 1978, pp. 339-348.
- [4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1982.
- [5] I. Csiszár and P. Narayan, “Secrecy Capacities for Multiple Terminals”, *IEEE Trans. Inform. Theory*, Vol. 50, No. 12, Dec 2004, pp. 3047-3061.
- [6] I. Csiszár and P. Narayan, “Secrecy Capacities for Multiterminal Channel Models”, *IEEE Trans. Inform. Theory*, Vol. 54, No. 6, June 2008, pp. 2437-2452.
- [7] R. Renner and S. Wolf, “New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction”, *Proceedings of EUROCRYPT 2003*, LNCS, Springer-Verlag, Vol. 2656, May 2003, pp.562577.
- [8] A. A. Gohari and V. Anantharam, “Communication for Omniscience by a Neutral Observer and Information-Theoretic Key Agreement of Multiple Terminals”, *Proceedings of the International Symposium on Information Theory (ISIT)*, 2007, pp. 2056-2060.
- [9] U. M. Maurer, R. Renner and S. Wolf, “Unbreakable Keys from Random Noise”, *Security with Noisy Data*, Springer-Verlag, 2007, pp. 21-44.
- [10] U. M. Maurer, “Secret Key Agreement by Public Discussion From Common Information”, *IEEE Trans. Inform. Theory*, Vol. 39, No.3, May 1993, pp. 733-742.
- [11] U. M. Maurer and S. Wolf, “The Intrinsic Conditional Mutual Information and Perfect Secrecy”, *Proceedings of the International Symposium on Information Theory (ISIT)*, 1997, p.88.
- [12] U. M. Maurer and S. Wolf, “Unconditionally Secure Key Agreement and the Intrinsic Conditional Information”, *IEEE Trans. Inform. Theory*, Vol. 45, No.2, March 1999, pp. 499-514.
- [13] U. M. Maurer and S. Wolf, “From Weak to Strong Information-Theoretic Key Agreement”, *Proceedings of the International Symposium on Information Theory (ISIT)*, 2000, p. 18.

- [14] A. A. Gohari and V. Anantharam, "An outer bound to the admissible source region of broadcast channels with arbitrarily correlated sources and channel variations", *Proceedings of the 46th Annual Allerton Conference on Communications, Control and Computing*, 2008, pp. 301-308.
- [15] A. A. Gohari and V. Anantharam, "A Generalized Cut-Set Bound", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2009, p. 99-103.
- [16] A. D. Wyner, "The Wiretap Channel", *Bell System Technical Journal*, Vol. 54, No. 8, Oct. 1975, pp. 1355-1387.
- [17] M. Christandl, R. Renner and S. Wolf, "A property of the intrinsic mutual information", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2003, p.258.
- [18] C.E. Shannon, "Communication Theory of Secrecy", *Bell System Technical Journal*, Vol. 28, Oct. 1949, pp. 656-715.