Information-Theoretic Key Agreement of Multiple Terminals - Part I: Source Model

Amin Aminzadeh Gohari[1] and Venkat Anantharam[1]

[1] Department of Electrical Engineering and Computer Science

University of California, Berkeley

{aminzade,ananth}@eecs.berkeley.edu

Abstract

This is the first part of a two-part paper on information-theoretically secure secret key agreement. In this part, we study the secrecy problem under the widely studied *source model*. In the source model the terminals wishing to generate a secret key, as well as the eavesdropper, receive the respective coordinates of a block of independent and identically distributed copies of jointly distributed random variables, after which the terminals are allowed interactive authenticated public communication, at the end of which each terminal should be able to generate the key. We derive a new upper bound on the secrecy capacity that strictly improves the currently best upper bound, due to Renner and Wolf. Further, while the Renner-Wolf bound is defined only in the case of two terminals, the new upper bound applies to the general multi-terminal case. The technique used for deriving our bound is to find certain properties of functions of joint probability distributions which will imply that they dominate the secrecy capacity, and then prove the bound by a verification argument. We also define a problem of communication for omniscience by a neutral observer and establish the equivalence between this new problem and the problem of secret key agreement. This generalizes an earlier result of Csiszár and Narayan. Finally, we prove a new lower bound on the secrecy capacity in the general multi-terminal case that in the two terminal case is strictly better than what is essentially the currently best known lower bound, namely the maximum of the two one-way secrecy capacities.

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

I. Introduction

Information-theoretic security is the most desirable form of security as it does not make any assumptions on the computational power of the adversary. Shannon was the first who precisely formulated the problem

of secret key generation by multiple terminals, information-theoretically secure from an eavesdropper [14]. Since then, the work of Shannon has been much developed and modified; see for example [1], [3] and [8]. In an early work, Maurer [8] considered the model in which Alice can send a message over a broadcast channel with one output at the intended recipient, Bob, and the other at the eavesdropper, Eve. He made the interesting observation that even if the channel from Alice to Eve is stronger than the channel from Alice to Bob, Alice and Bob may still be able to generate a common secret key that is information-theoretically secure from Eve, in an asymptotic sense, if we allow Bob to send authenticated but public messages to Alice. In some sense in this result the communication between Alice and Bob is being used to agree about features of the noise realization in the broadcast channel that are independent of Eve's knowledge: this is the secret key. This observation 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 [8], called the *source model* and *channel model*. In this paper, we focus on the source model. In this model there are m terminals interested in secret key generation against an adversary, Eve. The m terminals and Eve have access to n independently and identically distributed (i.i.d.) repetitions of jointly distributed random variables X_i ($i = 1, 2, ..., m$) and Z respectively. Following the reception of the n i.i.d. repetitions of $(X_1, X_2, ..., X_m, Z)$, in the traditional source model the m terminals are allowed to have interactive authenticated public communication. We generalize this model somewhat by allowing such communication only among the first u ($1 \leq u \leq m$) of the terminals; terminals $u+1, u+2, ..., m$ can listen and have to participate in secret key generation, but do not talk. This generalization has the technical advantage of putting one-way secret key generation and interactive secret key generation on the same footing and includes the standard model as a special one. Further, and more importantly, it provides an approach to study the secret key rate by splitting it into parts in a sense that will become clear after understanding the main results of this paper. Following the communication, each terminal generates random variable S_i as its secret key, $i = 1, 2, 3, ..., m$. 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 i.i.d repetitions of Z and the public discussion, becoming asymptotically independent as $n \to \infty$. The achieved secret key rate would then be roughly $\frac{1}{n}H(S_1)$. The highest achievable secret key rate, asymptotic in n, is called the secrecy capacity. For a precise formulation see section 2.

Calculation of the exact secrecy capacity remains an unsolved problem, although some lower and upper bounds on this quantity are known. For the case of $m = 2$, the best know upper bound is that of Renner and Wolf [12]. This bound, known as the *double intrinsic information bound*, is equal to $\inf_U [H(U) +$

$I(X_1; X_2 \downarrow ZU)]$, where $I(X; Y \downarrow Z)$ is defined as $\inf_{XY-Z-\overline{Z}} I(X; Y|\overline{Z})$ and is called the *intrinsic information* [10]. The essentially best known lower bound, proved using random binning arguments, is due to Ahlswede and Csiszár [1]: the maximum of $\sup_{V-U-X-YZ} \big(I(U;Y|V) - I(U;Z|V)\big)$ and $\sup_{V-U-Y-XZ} \big(I(U;X|V) - I(U;Z|V)\big)$. [1]

In some special cases, Csiszár and Narayan [5] derived a single-letter characterization of the secrecy capacity, notably when Z is independent of (X_1, X_2, X_3, ..., X_m). This was done by bringing out a connection between a problem of communication for omniscience (CFO) by the terminals and the secret key generation problem. In the CFO problem, as defined in [5], the requirement at the end of the communication is not a secret key, but that all the terminals become approximately omniscient about each other's random variables. The goal is to minimize the communication rate required to achieve this.

In this paper, we also improve the above mentioned result. We define a broader notion of communication for omniscience, called the problem of communication for omniscience by a neutral observer (still abbreviated as CFO). This includes the one of Csiszár and Narayan as a special case in the cases where their single letter characterization of the secrecy rate is valid. In the CFO problem, as defined in this paper, the m terminals at the end of the communication wish to create a shared random variable which when provided to a neutral observer who has access to the i.i.d. copies of Z seen by Eve, allows the observer to reconstruct the i.i.d. copies of the variables $(X_1, X_2, ..., X_u)$ (where $1 \leq u \leq m$ is as before). The CFO rate is the minimum conditional entropy of the communication, conditioned on the information available to Eve, measured on a per observation basis. We prove that our CFO problem is equivalent to the problem of secret key generation (see section 2 for the precise formulation of the definitions and section 3 for a precise formulation of the results). This result generalizes the one of [5] but does not appear to lead to a single letter characterization of the secrecy rate.

Finally, in this paper we also develop a new single letter lower bound for the secrecy rate which, in the case of two terminals, strictly improves on the one in [1], i.e. the maximum of the two one-way secret key rates. Our bound is proved by following the interactive communication stage by stage and careful bookkeeping of the buildup of the secret-key rate by controlling the amount of reduction of secret key rate built-up in earlier stages due to the communication in later stages.

The outline of this paper is as follows. In section 2, we introduce the basic notation and the definitions.

[1]Maurer provided a different technique for deriving lower bounds on the secret key rate in [8]. He proved, for instance, that even when the maximum of the two one-way communications vanishes, the secret key rate may be positive. This technique however seems to give us a rather low secrecy rate in this case. A generally applicable single letter form of a lower bound based on the ideas in [8] is not known.

Section 3 contains the main results of this paper followed by section 4, which gives the proofs, with some of the details relegated to appendices II and IV. Appendix I contains an example showing that our upper bound for secret key rate is strictly better than the currently best know upper bound from [12]. Appendix III contains a counterexample to the natural conjecture (which we believed for a long time while working on this problem) that the CFO rate is a concave function of the underlying joint probably distribution.

II. Definitions and Notation

Throughout this paper we assume X_1, X_2, ..., X_m and Z are $m+1$ possibly dependent random variables each taking values from a finite set.

We basically use the same multi-terminal model as in [5]. We however relax the uniformity condition on the generated secret key i.e. equation (2) in [5]. Maurer in [8] argued that the assumption of uniformity could always be added without loss of generality. We study the weak notion of secrecy throughout this paper and assume that all m terminals are interested in secret key generation. It is known that the weak and strong secret key rates are equal [11].

Some previous works consider secret key generation in the case where only one terminal is allowed to participate in public discussion, called the *one-way secrecy rate*. Our models more generally include the case in which only a subset of terminals is allowed to participate in the public discussion. Without loss of generality, we assume that terminals $1, 2, ..., u$ ($1 \leq u \leq m$) are allowed to talk while terminals $u+1, u+2, ..., m$ are silent.

Given n i.i.d. repetitions of a random variable X, we denote the i-th of these by $X(i)$. We write $X^{1:i}$ for $(X(1), X(2), ..., X(i))$. For $X^{1:n}$ we will often instead write X^n.

Definition 1: Given n i.i.d repetitions of the jointly distributed random variables $(X_1, X_2, ..., X_m, Z)$, the pair $(n, \overrightarrow{C})$, where $\overrightarrow{C} = (C_1, C_2, ..., C_r)$ is a finite set of discrete random variables, is considered a *valid communication* if:

- $H(C_i | C_1, C_2, ..., C_{i-1}, X_j^n) = 0 \ \ \forall j : 1 \leq j \leq m, \ i = j$ modulo m. This means that the indexing of the communications is done in round-robin order and each communication is adapted to the available information of the communicator;
- For all $u+1 \leq r \leq m$, we have $C_i = 0 \ \ \forall i : i = r$ modulo m. This means that the r-th terminal is not allowed to participate in the communication.

•

Please note that if $(n, \overrightarrow{C})$ is valid, then one has $H(\overrightarrow{C} | X_1^n, X_2^n, ..., X_m^n) = 0$.

Definition 2. Let n be a natural number, ϵ be a positive real number, $\overrightarrow{C} = (C_1, C_2, ..., C_r)$ be a finite set of discrete random variables, and S_1, S_2, ..., S_m be m discrete random variables. Consider the following conditions:

1) the pair $(n, \overrightarrow{C})$ is a valid communication;
2) $H(S_i|C_1, C_2, ..., C_r, X_i^n) = 0$ for all $1 \leq i \leq m$;
3) $P(S_1 = S_2 = S_3 = ... = S_m) > 1 - \epsilon$;
4) $\frac{1}{n} I(S_1; Z^n, C_1, C_2, ..., C_r) < \epsilon$;
5) $\frac{1}{n} H(X_1^n, X_2^n, ..., X_u^n | Z^n, S_1, S_2, ..., S_u) < \epsilon$.

The data typing condition SK(n, ϵ, S_1, S_2, S_3, ..., S_m, $\overrightarrow{C}$) is said to hold iff conditions 1, 2, 3 and 4 are satisfied. To any SK data type, we assign a number called the *gain* of the SK data type which is defined as $\frac{1}{n} H(S_1)$.

The data typing condition CFO(n, ϵ, S_1, S_2, S_3, ..., S_m, $\overrightarrow{C}$) is said to hold iff conditions 1, 2, 3 and 5 are satisfied. To any CFO data type, we assign a number called the *cost* of the CFO data type which is defined as $\frac{1}{n} H(\overrightarrow{C}|Z^n)$. ●

A valid communication $(n, \overrightarrow{C})$ for which, for some $\epsilon > 0$ and some $(S_1, S_2, \ldots, S_m)$ the data typing condition SK(n, ϵ, S_1, S_2, S_3, ..., S_m, $\overrightarrow{C}$) holds is called a *communication for secret key generation in the presence of an eavesdropper*. The intuitive reason for this terminology should be clear from the definition.

A valid communication $(n, \overrightarrow{C})$ for which, for some $\epsilon > 0$ and some $(T_1, T_2, \ldots, T_m)$ the data typing condition CFO(n, ϵ, T_1, T_2, T_3, ..., T_m, $\overrightarrow{C}$) holds is called a *communication for omniscience by a neutral observer*. Intuitively speaking, a communication for omniscience (CFO) protocol works as follows. The terminals will conduct a public discussion in order to agree, with probability close to 1, on a common randomness, but there is no secrecy constraint. We can assume that there is a neutral terminal, say Charles, who receives Z^n from Eve and the common randomness obtained by the terminals. Charles is required to become omniscient about $X_1^n, X_2^n, ..., X_u^n$. The cost of the communication would be the entropy of the overall communication conditioned on Z^n.

Consider the special case in which $u = m$, and Z is independent of $(X_1, X_2, \ldots, X_m)$. Charles will then not learn anything about $X_1^n, X_2^n, \ldots, X_m^n$ from Z^n and thus each T_i should be approximately equal to $X_1^n, X_2^n, \ldots, X_m^n$, meaning that each terminal has learned the random variables of all other terminals. The communication for omniscience by a neutral observer would be transformed to a simple communication for omniscience, as studied by Csiszár and Narayan [5]. The cost of communication in this case is equal to the total entropy of the communication. Since without loss of generality the successive

communications can be made independent of each other, one could have chosen them so that the cost as we measure it is identical to the cost as measured by Csiszár and Narayan. Therefore the communication for omniscience by a neutral observer is a generalization of the communication for omniscience of [5].

Definition 3: $S^{\epsilon}_{no-r}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$, the ϵ-secret key rate when the terminals cannot randomize, is defined as:

$$\limsup_{n\to\infty} \sup_{SK(n,\epsilon,S_1,S_2,S_3,...,S_m\overrightarrow{C})} Gain(SK)$$

Please note that the superscript "(s)" is used to denote the silent terminals. Similarly, $T^{\epsilon}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$ is defined as:

$$\liminf_{n\to\infty} \inf_{CFO(n,\epsilon,T_1,T_2,T_3,...,T_m\overrightarrow{C})} Cost(CFO)$$

$S_{no-r}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$, the secret key rate when the terminals cannot randomize, and $T(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$ are defined as:

$$S_{no-r}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z) = \lim_{\epsilon\to 0} S^{\epsilon}_{no-r}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$$

$$T(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z) = \lim_{\epsilon\to 0} T^{\epsilon}(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$$

$S(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$, the secret key rate when the terminals can randomize, is defined as the supremum of $S_{no-r}(X_1M_1;X_2M_2;X_3M_3;X_uM_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$ over all $(M_1,M_2,...,M_u)$ satisfying:

$$p(M_1,...,M_u,X_1,...,X_m,Z) = p(M_1).p(M_2)...p(M_u).p(X_1,...,X_m,Z)$$

•

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.

Theorem 1. Let $\varphi(X_1;X_2;X_3;...;X_m\|Z)$ be a real-valued function from the set of all probability distributions defined on $(X_1,X_2,X_3,...,X_m,Z)$, where $X_1,X_2,...,X_m$ and Z take values from arbitrary finite sets. $\varphi(X_1;X_2;X_3;...;X_m\|Z)$ is an upper bound on $S(X_1;X_2;X_3;...;X_u;X^{(s)}_{u+1};...;X^{(s)}_m\|Z)$ if

it satisfies all of the following properties. $\varphi(X_1;X_2;X_3;...;X_m\|Z)$ is an upper bound on $S_{no-r}(X_1;X_2;X_3;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|Z)$ if it satisfies properties (1-4):

1) For any natural number n:

$$n\varphi(X_1;X_2;...;X_m\|Z) \geq \varphi(X_1^n;X_2^n;...;X_m^n\|Z^n) \ ;$$

2) For any random variable F such that for some $1 \leq i \leq u$ we have $H(F|X_i)=0$, it holds that:

$$\varphi(X_1;X_2;...;X_m\|Z) \geq \varphi(X_1F;X_2F;...;X_mF\|ZF) \ ;$$

3) For any random variables $X_1', X_2', ..., X_m'$ such that $H(X_i'|X_i)=0$ for all $1 \leq i \leq m$, we have:

$$\varphi(X_1;X_2;...;X_m\|Z) \geq \varphi(X_1';X_2';...;X_m'\|Z) \ ;$$

4) $\varphi(X_1;X_2;...;X_m\|Z) \geq H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)$;

5) For any set of random variables $(M_1, M_2, ..., M_u)$ satisfying

$$p(M_1,M_2,...,M_u,X_1,X_2,...,X_m,Z) = p(M_1)p(M_2)...p(M_u).p(X_1,X_2,...,X_m,Z) \qquad (1)$$

we have

$$\varphi(X_1;X_2;...;X_m\|Z) \geq \varphi(X_1M_1;X_2M_2;...;X_uM_u;X_{u+1};...;X_m\|Z) \ .$$

Further $S(X_1;X_2;X_3;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|Z)$ itself satisfies all of these properties; and $S_{no-r}(X_1;X_2;X_3;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|Z)$ satisfies properties (1-4).

Discussion: The domain of φ in Theorem 1 is the set of *all* probability distributions on *all* products of $m+1$ finite sets. Condition 1 corresponds to the notion of taking blocks of observations. Condition 2 corresponds to the notion of terminal i communicating over the authenticated public channel. Condition 3 corresponds to the notion of each terminal choosing to ignore part of its available information. The right hand side of condition 4 is a choice of an easily proved and technically convenient lower bound on the secret key rate; other such expressions could also have been used instead. Condition 5 is relevant to the case where the speaking terminals are allowed to independently randomize. •

Theorem 2. Let $\psi(X_1;X_2;X_3;...;X_m\|Z)$ be a real-valued function from the set of all probability distributions defined on $(X_1,X_2,X_3,...,X_m,Z)$, where $X_1,X_2,...,X_m$ and Z take values from arbitrary finite sets. $\psi(X_1;X_2;X_3;...;X_m\|Z)$ is a lower bound on $T(X_1;X_2;X_3;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|Z)$ if it satisfies the following properties:

1) For any natural number n:

$$n\psi(X_1;X_2;...;X_m\|Z) \leq \psi(X_1^n;X_2^n;...;X_m^n\|Z^n);$$

2) For any random variable F such that for some $1 \leq i \leq u$ we have $H(F|X_i) = 0$, it holds that:

$$\begin{aligned} \psi(X_1; X_2; ...; X_m \| Z) \quad &\leq \\ \psi(X_1 F; X_2 F; ...; X_m F \| Z F) \quad &+ \quad H(F|Z) \ ; \end{aligned}$$

3) For any random variables $X'_1, X'_2, ..., X'_m$ such that $H(X'_i|X_i) = 0$ for all $1 \leq i \leq m$, we have:

$$\psi(X_1; X_2; ...; X_m \| Z) \leq \psi(X'_1; X'_2; ...; X'_m \| Z) + H(X_1 ... X_u | X'_1 ... X'_u Z);$$

4) $\psi(X_1; X_2; ...; X_m \| Z) \leq H(X_2 ... X_u | X_1 Z) + \sum_{i=2}^{m} H(X_1|X_i)$.

Further $T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ satisfies these properties.

Discussion: As in the case of φ of Theorem 1, here ψ should be thought of as defined on the set of *all* probability distributions on *all* products of $m+1$ finite sets. Condition 1 corresponds to the notion of forming blocks. Condition 2 corresponds to the notion of terminal i communicating over the authenticated public channel and paying the cost $H(F|Z)$ for this. Condition 3 corresponds to each terminal choosing to work with only part of its observation; intuitively the missing part can later be shared by paying a cost of at most $H(X_1 X_2 ... X_u | X'_1 X'_2 ... X'_u Z)$. The right hand side of condition 4 is a convenient choice of an easily proved upper bound on the CFO rate; other such choices could also have been used instead. It should however be noted that the choice in condition 4 is concave over probability distributions and this was important in the proof of some additional properties of the CFO rate given in [7]. •

Theorem 3. For any joint distribution $p(x_1, x_2, ..., x_m, z)$, we have:

$$S_{no-r}(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + T(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) = H(X_1, X_2, ..., X_u | Z).$$

Discussion: This establishes the equivalence between the problems of secret key generation and the problem of communication for omniscience by a neutral observer, generalizing the result of [5]. •

Theorem 4. $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is bounded above by

$$\begin{aligned} \inf_{J_1, J_2, ..., J_t} [\max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i)) + \\ S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ... J_t^{(s)} \| Z)] \end{aligned}$$

where the infimum is taken over all random variables $J_1, J_2, ..., J_t$ and all t.

Discussion: To understand this claim, start with the case $t = 1$. One can think of J_1 as trying to define a "split" in the secret key rate: one looks for a secret key rate among the m terminals that is secret from an entity that gets i.i.d. copies of J_1 (the first term on the right hand side of the upper bound) and then for a secret key that is shared by a terminal getting i.i.d. repetitions of J_1 (who is not allowed to talk)

but is secret from the original eavesdropper (the second term on the right hand side of the upper bound). The claim is that the true secret key can not exceed the sum of the two rates got in this "split" way. The case of general t can be understood in a similar way. ●

Theorem 4 leads to some corollaries that appear to deserve separate statements.

Corollary 1. $S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|Z)$ is bounded above by

$$\inf_J \big(S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)+S(X_1X_2...X_m;J^{(s)}\|Z)\big).$$

A single letter characterization of $S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)$ is given in Theorem 6. ●

Corollary 2. For $m=2$, we have

$$S(X;Y\|Z)\leq \inf_J\big(S(X;Y\|J)+S(XY;J^{(s)}\|Z)\big)\leq$$
$$\inf_J\big(I(X;Y|J)+S(XY;J^{(s)}\|Z)\big).$$

This bound strictly improves the Renner-Wolf double intrinsic information upper bound. ●

Corollary 3. For any random variables $J_1,J_2,...,J_t$, the following inequalities hold (for the notation $valid(1,\overrightarrow{C})$ used in the second and third bullets, please refer to definition 1):

- $S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)\geq$
  $\sup_{X_1'...X_m':p(ZJ_1...J_tX_1...X_m,X_1',...,X_m')=p(ZJ_1...J_tX_1...X_m)p(X_1'|X_1)...p(X_m'|X_m)}[$
  $S(X_1';X_2';...;X_u';X_{u+1}^{'(s)};...;X_m^{'(s)}\|Z)-\max_i(S(X_1';X_2';...;X_u';X_{u+1}^{'(s)};...;X_m^{'(s)}\|J_i))]$;
- $S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)\geq$
  $\sup_{valid(1,\overrightarrow{C})}[S(X_1\overrightarrow{C};X_2\overrightarrow{C};...;X_u\overrightarrow{C};(X_{u+1}\overrightarrow{C})^{(s)};...;(X_m\overrightarrow{C})^{(s)}\|Z\overrightarrow{C})-$
  $\max_i(S(X_1\overrightarrow{C};X_2\overrightarrow{C};...;X_u\overrightarrow{C};(X_{u+1}\overrightarrow{C})^{(s)};...;(X_m\overrightarrow{C})^{(s)}\|J_i\overrightarrow{C}))]$;
- $S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)\geq$
  $\sup_{valid(1,\overrightarrow{C}),X_1'...X_m':p(\overrightarrow{C}ZJ_1...J_tX_1...X_m,X_1',...,X_m')=p(\overrightarrow{C}ZJ_1...J_tX_1...X_m)p(X_1'|X_1\overrightarrow{C})...p(X_m'|X_m\overrightarrow{C})}[$
  $S(X_1'\overrightarrow{C};X_2'\overrightarrow{C};...;X_u'\overrightarrow{C};(X_{u+1}'\overrightarrow{C})^{(s)};...;(X_m'\overrightarrow{C})^{(s)}\|Z\overrightarrow{C})-$
  $\max_i(S(X_1'\overrightarrow{C};X_2'\overrightarrow{C};...;X_u'\overrightarrow{C};(X_{u+1}'\overrightarrow{C})^{(s)};...;(X_m'\overrightarrow{C})^{(s)}\|J_i\overrightarrow{C}))]$.

Discussion: For the special case of $u=m=t=1$, the last formula suggests the inequality:

$$S(X;Y^{(s)}\|Z)\geq \sup_{\overrightarrow{C}-X'\overrightarrow{C}-XYZ}[S(X'\overrightarrow{C}\|Z\overrightarrow{C})-S(X'\overrightarrow{C}\|Y\overrightarrow{C})].$$

$S(X\|Z)$ is not well-defined but if defined as $H(X|Z)$, we get the tight inequality

$$S(X;Y^{(s)}\|Z)\geq \sup_{\overrightarrow{C}-X'\overrightarrow{C}-XYZ}[H(X'|Z\overrightarrow{C})-H(X'|Y\overrightarrow{C})]$$

and the above formula can be understood as a generalization of this lower bound on the (one-way) secrecy rate. ●

A variant of Corollary 1 can be proved by the verification technique that was used to prove Theorem 1. This is stated as the next result.

Theorem 5. Let $\mathbb{R}_{\geq 0}$ denote the set of nonnegative real numbers. Let $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$ be a strictly increasing convex function and let the *f-one-way secrecy rate* be defined as

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

Then $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is bounded above by

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

This upper bound is in turn bounded above by

$\inf_J f^{-1}\big(f(S(X_1 J; ...; X_u J; (X_{u+1} J)^{(s)}; ...; (X_m J)^{(s)} \| J)) + S_{f-one-way}(X_1 X_2 ... X_m; J^{(s)} \| Z)\big)$.

Discussion: The upper bound given in Theorem 5 reduces to that of Corollary 1 in the special case of $f(x) = x$. We don't know if this bound strictly improves that of Corollary 1. The weaker form of the bound given in the statement of the theorem is useful because there is a single letter characterization for $S(X_1 J; X_2 J; ...; X_u J; (X_{u+1} J)^{(s)}; ...; (X_m J)^{(s)} \| J)$, given in Theorem 6. •

Theorem 6. Let $[m]$ and $[u]$ respectively denote the sets $\{1, 2, ..., m\}$, $\{1, 2, ..., u\}$. The following formula on the secret key rate holds:

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

$H(X_1 X_2 ... X_u | Z) - \min_{(R_1, R_2, ..., R_u) \in \Re} (\sum_{i=1}^{u} R_i)$

where:

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

Discussion: This claim is best understood in conjunction with Theorem 3 as giving a natural Slepian-Wolf type characterization of the CFO rate in this special case. When $u = m$ it reduces to the known result proved in [5]. •

Theorem 7. $S(X_1; X_2; ...; X_u; (X_{u+1})^{(s)}; ...; (X_m)^{(s)} \| Z)$ is bounded below by

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

for every $q \leq p$, and $(U_1, U_2, ..., U_p)$ satisfying the following constraints:

- U_i ($i = 1, 2, ..., p$) takes values from a finite set;
- $p(U_1, U_2, ..., U_p | X_1, X_2, X_3, ..., X_m, Z) = \prod_{i=1}^{p} p(U_i | U_{1:i-1} X_{i \mod m})$;
- For all $r > u$, we have $U_i = 0 \ \forall i : i - r \equiv^m 0$.

This lower bound strictly improves what is essentially the currently best known lower bound, namely the maximum of the two one-way secrecy rates.

Discussion: The property that $(U_1, ..., U_p)$ should satisfy is equivalent to the following condition:

$I(U_i; X_{[m]-\{j\}} | U_{1:i-1} X_j) = 0 \ \forall i, j : 1 \leq j \leq m, \ i - j \equiv^m 0$.

Intuitively, assuming that all the X_i's and Z have learnt $U_{1:i-1}$, the $(i \mod m)$-th terminal can create U_i. The individual terms in the lower bound can be understood from the form of the one-way secrecy

rate. ●

IV. PROOFS OF THEOREMS 1-7

Proof of Theorem 1. Fix a probability distribution $p(x_1, x_2, ..., x_m, z)$ on $(X_1, X_2, ..., X_m, Z)$ and assume that $X_1, X_2, ..., X_m$ and Z take values in the discrete finite sets Δ_i, $i = 1...m+1$. We prove that $\varphi(X_1; X_2; X_3; ...; X_m \| Z)$ is an upper bound on $S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ if it satisfies all the properties. Proving that $\varphi(X_1; X_2; X_3; ...; X_m \| Z)$ would be an upper bound on $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ if it satisfies properties (1-4) is similar.

For every $\delta > 0$, $\epsilon > 0$ and M_1, M_2, ..., M_u (satisfying (1)), one can find data type SK(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) whose gain is within δ of $S_{no-r}^{\epsilon}(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$. We have:

$$
\begin{aligned}
& n\varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq^{i} \\
& \varphi(X_1^n; X_2^n; X_3^n; ...; X_m^n \| Z^n) \geq^{ii} \\
& \varphi(X_1^n M_1; X_2^n M_2; X_3^n M_3; ...; X_u^n M_u; X_{u+1}^n ...; X_m^n \| Z^n) \geq^{iii} \\
& \varphi(X_1^n M_1 C_1; X_2^n M_2 C_1; ...; X_u^n M_u C_1; X_{u+1}^n C_1; ...; X_m^n C_1 \| Z^n C_1) \geq^{iv} \\
& \varphi(X_1^n M_1 C_1 C_2; X_2^n M_2 C_1 C_2; ...; X_u^n M_u C_1 C_2; X_{u+1}^n C_1 C_2; ...; X_m^n C_1 C_2 \| Z^n C_1 C_2) ... \geq^{v} \\
& \varphi(X_1^n M_1 \overrightarrow{C}; X_2^n M_2 \overrightarrow{C}; ...; X_u^n M_u \overrightarrow{C}; X_{u+1}^n \overrightarrow{C}; ...; X_m^n \overrightarrow{C} \| Z^n \overrightarrow{C}) \geq^{vi} \\
& \varphi(S_1; S_2; ...; S_m \| Z^n \overrightarrow{C}) \geq^{vii} \\
& H(S_1 | Z^n \overrightarrow{C}) - \textstyle\sum_{j=2}^{m} H(S_1 | S_j) \geq^{viii} \\
& n S_{no-r}^{\epsilon}(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)\} - n\delta - (m-1)[h(\epsilon) + \epsilon . n \log \textstyle\prod_{i=1}^{m} |\Delta_i|]
\end{aligned}
$$

Inequalities i, ii, iii, iv, v, vi, vii are true respectively because of the properties 1, 5, 2, 2, 2, 3, 4. Inequality $viii$ is true because of the Fano inequality, and the fact that the gain of SK(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) is within δ of $S_{no-r}^{\epsilon}(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$.

Therefore we get

$$
\begin{aligned}
& \varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq \\
& S_{no-r}^{\epsilon}(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) - \delta - \tfrac{m-1}{n}[h(\epsilon) + \epsilon . n \log \textstyle\prod_{i=1}^{m} |\Delta_i|].
\end{aligned}
$$

The theorem is proved by taking the limit as ϵ and δ go to zero and noting that the choice of M_1, M_2, ..., M_u was arbitrary.

$S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ and $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ themselves satisfy the five (respectively the first four) properties.

$S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ satisfies properties 1, 2, 3 and 5 and $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ satisfies properties 1, 2 and 3 because every valid SK data

type for the right hand side of the inequalities can be converted to one for the left hand side. In 1, the terminals observing $(X_1, X_2, ..., X_m)$ can first observe n i.i.d. copies of their random variables and then simulate the SK data type for the right hand side. In 2, they can take i.i.d repetitions of F by i-th terminal as the first non-trivial communication and then simulate the SK data type for the right hand side. In 3, they can create X_i''s first and then simulate the SK data type for the right hand side. In 5, the terminals $1 \leq i \leq u$ can respectively create $M_1, M_2, \ldots, M_u$ first and then simulate the SK data type for the right hand side.

For property 4, note that both $S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ and $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ are greater than or equal to the one way secret key rate from X_1 to $X_2, X_3, ..., X_m$ in the presence of Z which in turn is greater than or equal to $\min_{2 \leq i \leq m}(I(X_1; X_i) - I(X_1; Z))$. This expression is greater than or equal to the right hand side of 4. ●

Proof of Theorem 2. Fix the probability distribution $p(x_1, x_2, ..., x_m, z)$ on $(X_1, X_2, ..., X_m, Z)$ and assume that $(X_1, X_2, ..., X_m, Z)$ take values in the discrete finite sets Δ_i, $i = 1...m+1$. For every $\delta > 0$ and $\epsilon > 0$, one can find data type CFO(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) whose cost is within δ of $T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$. We have:

$$
\begin{aligned}
& n\psi(X_1; X_2; X_3; ...; X_m \| Z) \leq^{i} \\
& \psi(X_1^n; X_2^n; X_3^n; ...; X_m^n \| Z^n) \leq^{ii} \\
& \psi(X_1^n C_1; X_2^n C_1; ...; X_m^n C_1 \| Z^n C_1) + H(C_1 | Z^n) \leq^{iii} \\
& \psi(X_1^n C_1 C_2; X_2^n C_1 C_2; ...; X_m^n C_1 C_2 \| Z^n C_1 C_2) + H(C_1 C_2 | Z^n) ... \leq^{iv} \\
& \psi(X_1^n \overrightarrow{C}; X_2^n \overrightarrow{C}; ...; X_m^n \overrightarrow{C} \| Z^n \overrightarrow{C}) + H(\overrightarrow{C} | Z^n) \leq^{v} \\
& \psi(S_1; S_2; ...; S_m \| Z^n \overrightarrow{C}) + H(X_1^n X_2^n ... X_u^n | S_1 S_2 ... S_u Z^n) + H(\overrightarrow{C} | Z^n) \leq^{vi} \\
& H(S_2 S_2 ... S_u | S_1 Z^n \overrightarrow{C}) + \textstyle\sum_{j=2}^{m} H(S_1 | S_j) + H(X_1^n X_2^n ... X_u^n | S_1 S_2 ... S_u Z^n) + H(\overrightarrow{C} | Z^n) \leq^{vii} \\
& h(\epsilon) + \epsilon . n \log \textstyle\prod_{i=1}^{u} |\Delta_i| + (m-1)[h(\epsilon) + \epsilon . n \log \prod_{i=1}^{m} |\Delta_i|] + \\
& + n\epsilon + nT^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + n\delta
\end{aligned}
$$

Inequalities i, ii, iii, iv, v, vi are true respectively because of the properties 1, 2, 2, 2, 3, 4. Inequality vii is true due to the Fano inequality, and the fact that the cost of CFO(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) is within δ of $T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$.

Therefore we get

$$
\begin{aligned}
& \psi(X_1; X_2; X_3; ...; X_m \| Z) \leq \\
& T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + \delta + \tfrac{m}{n}[h(\epsilon) + \epsilon . n \log \textstyle\prod_{i=1}^{m} |\Delta_i|] + \epsilon.
\end{aligned}
$$

The theorem is proved by taking the limit as ϵ and δ go to zero.

$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ itself satisfies the four properties.

For property 1, note that the terminals observing $(X_1, X_2, ..., X_m)$ can first observe n i.i.d. copies of their random variables and then pretend that they are in the situation on the right hand side of 1. For property 2, they can take i.i.d repetitions of F by i-th terminal as the first non-trivial communication, and then pretend that they are in the situation corresponding to the first term on the right hand side of 2. The total cost would be the sum of $H(F|Z)$ and the remaining cost of communication of the CFO data type of the left hand side.

Regarding property number 3, we first intuitively sketch the proof: one possible communication for omniscience for $(X_1, X_2, ..., X_m, Z)$ is to first conduct a communication for omniscience for $(X_1', X_2', ..., X_m', Z)$. The terminal who wants to become omniscient, Charles, would be able to approximately learn $(X_1', X_2', ..., X_u', Z)$ with the cost of $T(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z)$. If Charles exactly knew $(X_1', X_2', ..., X_u', Z)$, the u terminals could use a Slepian-Wolf type communication scheme to reveal $H(X_1 X_2 ... X_u | X_1' X_2' ... X_u' Z)$ bits on the public channel, thereby enabling Charles to receive these bits as a common randomness and become omniscient. The total communication cost is no more than $T(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z) + H(X_1 X_2 ... X_u | X_1' X_2' ... X_u' Z)$. Even though Charles does not exactly know $(X_1', X_2', ..., X_u'; Z)$, this Slepian-Wolf algorithm still works.

We now prove the property more precisely. Fix $\epsilon > 0$ and $\delta > 0$. $T^{\epsilon}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is defined as:

$$\liminf_{n \to \infty} \inf_{CFO(n, \epsilon, T_1, T_2, T_3, ..., T_m, \overrightarrow{C})} Cost(CFO)$$

Therefore we can find a large enough n such that the following requirements are satisfied:

- There is a valid CFO(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) within δ of
  $T^{\epsilon}(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z)$;
- There is a communication with the total entropy of at most $n(H(X_1 .... X_u | X_1' X_2' ... X_u' Z) + \delta)$ for the Slepian-Wolf type problem in which u terminals having i.i.d. repetitions of X_1, X_2, ..., X_u want to transmit their information to a receiver who has i.i.d. repetitions of $X_1' X_2' ... X_u' Z$ as a side information. In this Slepian-Wolf type problem, it is desired to have
  $\frac{1}{n} H(X_1^n .... X_u^n | X_1'^n X_2'^n ... X_u'^n Z^n$, Communication$) \leq \delta$.

The terminals first follow CFO(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) and then the u terminals X_1, X_2, ..., X_u insert the corresponding communications for the Slepian-Wolf problem, on the public channel. Let $\overrightarrow{C'}$ denote the *whole* communication ($\overrightarrow{C'}$ includes $\overrightarrow{C}$).

We prove that the CFO(n, $\epsilon + \delta$, $S_1\overrightarrow{C'}$, $S_2\overrightarrow{C'}$, $S_3\overrightarrow{C'}$,..., $S_m\overrightarrow{C'}$, $\overrightarrow{C'}$) is valid and further the cost of this

CFO is less than or equal to

$$T^{\epsilon}(X'_1; X'_2; X'_3; ...; X'_u; X^{'(s)}_{u+1}; ...; X^{'(s)}_m \| Z) + H(X_1....X_u | X'_1 X'_2 ... X'_u Z) + 2\delta$$

Using the inequality $H(X|YW) \leq H(X|ZW)+H(Z|YW)$ for any four random variables X, Y, Z, W, we have

$$\tfrac{1}{n} H(X_1^n....X_u^n | S_1 S_2 ... S_u \overrightarrow{C'} Z^n) \leq \tfrac{1}{n} H(X_1^n....X_u^n | X_1^{'n} X_2^{'n} ... X_u^{'n} \overrightarrow{C'} Z^n) + \tfrac{1}{n} H(X_1^{'n} X_2^{'n} ... X_u^{'n} | S_1 S_2 ... S_u \overrightarrow{C'} Z^n) \leq \delta + \epsilon$$

The other requirements for CFO to be valid can be easily checked.

The cost of the CFO, i.e. $\frac{1}{n} H(\overrightarrow{C'} | Z^n)$ is bounded above by

$$\tfrac{1}{n} H(\overrightarrow{C} | Z^n) + \tfrac{1}{n} H(\overrightarrow{C'} | \overrightarrow{C}) \leq$$
$$T^{\epsilon}(X'_1; X'_2; ...; X'_u; X^{'(s)}_{u+1}; ...; X^{'(s)}_m \| Z) + \delta + H(X_1 X_2 ... X_u | X'_1 X'_2 ... X'_u Z) + \delta.$$

For property number 4, the idea is that, in the first phase, the first terminal transmits messages to other terminals enabling them find X_1 with high probability. The entropy of the communication from 1^{st} terminal to i-th terminal would be roughly $nH(X_1|X_i)$, and this is an upper bound for the conditional entropy of the communication given Z^n. Now, since all the terminals can include X_1 as a common randomness, Charles would be able to calculate $X_1 Z$. In the second stage, the first u terminals reveal roughly $n.H(X_1 X_2 ... X_u | X_1 Z)$ bits on the public channel. Since this now becomes a common randomness, this can be passed to Charles, enabling him to learn $X_1 X_2 ... X_u$. The total cost of this communication scheme would be bounded above by $\sum H(X_i|X_1) + H(X_1 X_2 ... X_u | X_1 Z)$ on a per observation basis, asymptotically as $n \to \infty$. ●

Proof of Theorem 3. It can be easily shown that $\psi(X_1; X_2; X_3; ...; X_m \| Z)$ satisfies the four properties of Theorem 2 if and only if $H(X_1 X_2 ... X_u | Z) - \psi(X_1; X_2; X_3; ...; X_m \| Z)$ satisfies the four properties of Theorem 1.

$T(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ itself satisfies the four properties of Theorem 2. Hence

$$H(X_1 X_2 ... X_u | Z) - T(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z) \geq$$
$$S_{no-r}(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z).$$

Further since $S_{no-r}(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ itself satisfies the four properties of Theorem 1, we get

$$H(X_1 X_2 ... X_u | Z) - S_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z) \leq T(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z).$$

Therefore $H(X_1 X_2 ... X_u | Z) =$

$$S_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z) + T(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z).$$ ●

Proof of Theorem 4. It is enough to prove that

$$\varphi(X_1;X_2;X_3;...;X_m\|Z) = \inf_{J_1,J_2,...,J_t}[\max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i)) + S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)]$$

satisfies the five properties of Theorem 1.

Property number *1*: It is enough to prove that for any $J_1, J_2, ..., J_t$, there exists $J_1', J_2', ..., J_t'$ such that:

$$n\ \max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i))+S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)$$
$$\geq \max_i(S(X_1^n;X_2^n;...;X_u^n;(X_{u+1}^n)^{(s)};...;(X_m^n)^{(s)}\|J_i')) + S(X_1^n;X_2^n;...;X_u^n;(X_{u+1}^n)^{(s)};...;(X_m^n)^{(s)};J_1^{'(s)};J_2^{'(s)};...;J_t^{'(s)}\|Z^n).$$

We take J_i' to be J_i^n for $1 \leq i \leq t$. The inequality holds since the secret key function itself satisfies the first property of Theorem 1.

Property number *2*: Let $H(F \mid X_i) = 0$, where $1 \leq i \leq u$. It is enough to prove that for any $J_1, J_2, ..., J_t$, there exists $J_1', J_2', ..., J_t'$ such that:

$$\max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i)) + S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)$$
$$\geq \max_i(S(X_1F;X_2F;...;X_uF;X_{u+1}^{(s)}F;...;X_m^{(s)}F\|J_i')) + S(X_1F;X_2F;...;X_uF;(X_{u+1}F)^{(s)};...;(X_mF)^{(s)};J_1^{'(s)};J_2^{'(s)};...;J_t^{'(s)}\|ZF).$$

We take J_i' to be J_iF for $1 \leq i \leq t$. The inequality holds since the secret key function itself satisfies the second property of Theorem 1.

The proof for property *3* is similar to that for the two preceding properties, and is left to the reader.

Property number *4*: It is enough to prove that for any $J_1, J_2, ..., J_t$,

$$\max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)}...;X_m^{(s)}\|J_i)) + S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)$$

is greater than or equal to $H(X_1|Z) - \sum_{k=2}^m H(X_1|X_k)$

We have:

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z) \geq$$
$$S(X_1;X_2^{(s)};X_3^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z) \geq$$
$$\min(\min_{1\leq i\leq t} I(X_1;J_i), \min_{2\leq k\leq m} I(X_1;X_k)) - I(X_1;Z)$$

Since the secret key function itself satisfies the fourth property of Theorem 1, we have:

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i) \geq H(X_1) - I(X_1;J_i) - \textstyle\sum_k H(X_1|X_k).$$

This implies that

$$\max_i S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i) \geq H(X_1) - \min_i I(X_1;J_i) - \textstyle\sum_{k=2}^m H(X_1|X_k)$$

There are two cases:

- If $\min_i I(X_1;J_i) \leq \min_k I(X_1;X_k)$:

  We have:

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z) \geq$$
$$\min_i I(X_1;J_i) - I(X_1;Z) = H(X_1) - \max_i H(X_1|J_i) - I(X_1;Z).$$

Therefore

$$\max_i S(X_1;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i) + S(X_1;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};...J_t^{(s)}\|Z) \geq$$
$$H(X_1) - I(X_1;Z) - \sum_{k=2}^m H(X_1|X_k) = H(X_1|Z) - \sum_{k=2}^m H(X_1|X_k).$$

- If $\min_i I(X_1;J_i) > \min_{2\leq k\leq m} I(X_1;X_k)$:

  We have:

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z) \geq$$
$$\min_{2\leq k\leq m} I(X_1;X_k) - I(X_1;Z) \geq$$
$$H(X_1) - \sum_{k=2}^m H(X_1|X_k) - I(X_1;Z) = H(X_1|Z) - \sum_{k=2}^m H(X_1|X_k).$$

Property number 5: It is enough to prove that for any $J_1, J_2, ..., J_t$, there exists $J_1', J_2', ..., J_t'$ such that:

$$\max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i)) +$$
$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z) \geq$$
$$\max_i(S(X_1M_1;X_2M_2;...;X_uM_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i')) +$$
$$S(X_1M_1;X_2M_2;...;X_uM_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{'(s)};J_2^{'(s)};...J_t^{'(s)}\|Z).$$

We define $J_1', J_2', ..., J_t'$ such that:

- For every $x_1, ..., x_m, z, j_1, ..., j_t$,
  $p(J_1' = j_1, ..., J_t' = j_t|X_1 = x_1, ..., X_m = x_m, Z = z) =$
  $p(J_1 = j_1, ..., J_t = j_t|X_1 = x_1, ..., X_m = x_m, Z = z)$;
- $p(M_1, ..., M_u, X_1, ..., X_m, Z, J_1'..., J_t') = p(M_1).p(M_2)...p(M_u).p(X_1, ..., X_m, Z, J_1'..., J_t')$.

The proof would be done by noting that the secret key function itself satisfies the fifth property of Theorem 1. ●

Proof of Corollary 1. We get the desired result by applying Theorem 4 for the case of $t = 1$ and noting that

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J) \leq S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)$$

and

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J^{(s)}\|Z) \leq S(X_1X_2...X_m;J^{(s)}\|Z).$$ ●

Proof of Corollary 2. This is a straightforward special case of Corollary 1. In the case of two terminals we have:

$$S(X;Y\|Z) \leq \inf_J \left(S(X;Y\|J) + S(XY;J^{(s)}\|Z)\right) \leq \inf_J \left(S(XJ;YJ\|J) + S(XY;J^{(s)}\|Z)\right).$$

We get the desired upper bound by noting that $S(XJ;YJ\|J) = I(X;Y|J)$.

$I(X;Y|J)+S(XY;J^{(s)}\|Z)$ could be further bounded above by $\inf_J\big(I(X;Y|J)+I(XY;J|Z)\big)$. It is enough to prove that $\inf_J\big(I(X;Y|J)+I(XY;J|Z)\big)$ strictly improves the Renner-Wolf double intrinsic information upper bound. In order to prove that the new bound is not worse than the double intrinsic information bound, it is sufficient to prove that for any random variable U, there is a random variable J such that $I(X;Y|J)+I(XY;J|Z)\leq[H(U)+\min_{\overline{Z}:X-Y-ZU-\overline{Z}}I(X;Y|\overline{Z})]$. Choosing $J=\overline{Z}$, we will have $I(X;Y|J)=I(X;Y|\overline{Z})$ and also $I(XY;J|Z)=I(XY;U|Z)-I(XY;U|ZJ)\leq I(XY;U|Z)\leq H(U)$. Therefore $\inf_J\big(I(X;Y|J)+I(XY;J|Z)\big)$ is no worse than the double intrinsic information bound. Appendix I contains an example for which $\inf_J\big(I(X;Y|J)+I(XY;J|Z)\big)$ is strictly better than the double intrinsic information bound. ●

Proof of Corollary 3. The inequality can be proved by noting that for any $(X_1'...X_m')$ such that

$$p(ZJ_1...J_tX_1...X_m,X_1',...,X_m')=p(ZJ_1...J_tX_1...X_m)p(X_1'|X_1)...p(X_m'|X_m)$$

we have

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)\geq$$
$$S(X_1';X_2';...;X_u';X_{u+1}^{'(s)};...;X_m^{'(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)$$

which is true because reducing information can not increase the secret key rate. ●

Proof of Theorem 5. Without loss of generality we can assume $f(0)=0$, because for any positive constant c, $g(x)=f(x)+c$ satisfies the following equations:

- $S_{g-one-way}(X;Y^{(s)}\|Z)=S_{f-one-way}(X;Y^{(s)}\|Z)$;
- $g^{-1}\big(g(a)+b\big)=f^{-1}\big(f(a)+b\big)$ for any non-negative a and b.

Since

$$S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)\geq S(X_1;X_2;...;X_u;(X_{u+1})^{(s)};...;(X_m)^{(s)}\|J)$$

and f is increasing, it suffices to prove the first bound in the statement of the theorem. In order to show this, it is sufficient to verify the five conditions of Theorem 1. This is done in appendix II. The proof uses the standard fact that the convexity of f implies that it is continuous and that $f(x+a)-f(x)$ is an increasing function in x for any fixed a.

●

Proof of Theorem 6.

We first prove that for any $(R_1,R_2,...,R_u)\in\Re$, there are SK data types whose gains asymptotically approach $H(X_1X_2...X_u|Z)-\sum_{i=1}^u R_i$. In order to show this, it is enough to prove that for any $\epsilon>0$, there is n large enough such that the first u terminals, after observing $X_i^nZ^n$ ($1\leq i\leq u$), can insert messages of entropy $n(R_i+\epsilon)$ on the public channel such that all the m terminals would be able to calculate $X_1^n,X_2^n,...,X_u^n,Z^n$ with probability at least $1-\epsilon$: $(X_1,X_2,...,X_u,Z)$ will be a common

randomness for the m terminals, and Eve's whole information about this common randomness is bounded above by the summation of the entropy of Z and the entropy of the communication (i.e. $n(R_i+\epsilon)$).

We use the technique used in appendix A of [5] and apply Theorem 1.1.14 of [4]. We define a normal source network (NSN) without helper as follows: There are m source and m dummy nodes in the first layer of our NSN. The $2i$-th and $(2i-1)$-th node are both connected to X_iZ. The second layer comprises of $m+u$ encoders. The first u encoders are connected to the first $2i$-th nodes for $i=1,2,...,u$. The rest of the m encoders are connected to $(2i-1)$-th nodes for $i=1,2,...,m$. The output rates of the first $u+m$ encoders are R_1, R_2, ..., R_u, $H(X_1)$, $H(X_2)$, ..., $H(X_m)$. The third layer includes m decoders. The i-th decoder is connected to the $(u+i)$-th and the first u nodes of the second layer.

It can be shown that the conditions imposed by Theorem 1.1.14 of [4] would be satisfied if $(R_1,R_2,...,R_u)$ is in $\Re$. This result makes intuitive sense because for every set B, the overall communication of those of the u terminals that are in B is at least equal to their uncertainty with respect to those outside B.

For the converse part, take u arbitrary random variables $M_1,M_2,...,M_u$ jointly independent of each self and of $(X_1,X_2,...,X_m,Z)$. For convenience, let us write $\tilde{X}_i$ for X_iZ for the rest of the proof, $1\leq i\leq m$. Take a valid SK(n, ϵ, S_1, S_2, S_3,..., S_m, $\overrightarrow{C}$) for $(\tilde{X}_1M_1,\tilde{X}_2M_2,...,\tilde{X}_uM_u,\tilde{X}_{u+1},...,\tilde{X}_m,Z)$. The proof technique is similar to one used in Lemma 2 of [5].

$H(\tilde{X}_1^nM_1^n...\tilde{X}_u^nM_u^n|Z^n)=H(\tilde{X}_1^nM_1^n...\tilde{X}_u^nM_u^n\overrightarrow{C}S_1|Z^n)=\sum_i H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1}Z^n)+H(S_1|\overrightarrow{C}Z^n)+$
$\sum_{i=1}^u H(\tilde{X}_i^nM_i^n|\tilde{X}_1^nM_1^n\tilde{X}_2^nM_2^n...\tilde{X}_{i-1}^nM_{i-1}^n\overrightarrow{C}S_1Z^n)$

Let $R'_j=\frac{1}{n}\sum_{i:i-j\equiv^m 0}H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1}Z^n)+\frac{1}{n}H(\tilde{X}_j^nM_j^n|\tilde{X}_1^nM_1^n\tilde{X}_2^nM_2^n...\tilde{X}_{j-1}^nM_{j-1}^n\overrightarrow{C}S_1Z^n)-H(M_j)$ for $j=1,2,...,u$.

Based on this choice of R'_j's, one can observe that $\sum_{j=1}^u R'_j=H(\tilde{X}_1...\tilde{X}_u|Z)-\frac{1}{n}H(S_1|\overrightarrow{C}Z^n)$.

Let $R_j=R'_j+\frac{\epsilon\log(|S_1|)+h(\epsilon)}{n}$. We prove that $(R_1,R_2,...,R_u)\in\Re$.

Let B be some subset of $[m]$ whose intersection with $[u]$ is nonempty and such that $B\neq[m]$. By conditioning on $((\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B))$, we get:

$H(\tilde{X}_1^nM_1^n...\tilde{X}_u^nM_u^n|Z^n(\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B))=$
$\sum_i H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1}Z^n(\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B))+$
$H(S_1|\overrightarrow{C}Z^n(\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B))+$
$\sum_{i=1}^u H(\tilde{X}_i^nM_i|\tilde{X}_1^nM_1^n\tilde{X}_2^nM_2^n...\tilde{X}_{i-1}^nM_{i-1}^n\overrightarrow{C}S_1(\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B)Z^n)$

Noting that

$H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1}Z^n(\tilde{X}_j^n,j\in B^c)(M_j^n,j\in[u]-B))=0$ for $i\in([m]-[u])\bigcup([u]-B)$

and

$$H(\tilde{X}_i^n M_i|\tilde{X}_1^n M_1^n \tilde{X}_2^n M_2^n ... \tilde{X}_{i-1}^n M_{i-1}^n \overrightarrow{C} S_1(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)Z^n) = 0 \text{ for } i \in [u]-B$$

we can rewrite the above expression as:

$$H(\tilde{X}_1^n M_1^n ... \tilde{X}_u^n M_u^n|Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)) =$$
$$\sum_{i \mod m \in B \bigcap [u]} H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1} Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)) +$$
$$H(S_1|\overrightarrow{C} Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)) +$$
$$\sum_{i \in B \bigcap [u]} H(\tilde{X}_i^n M_i|\tilde{X}_1^n M_1^n \tilde{X}_2^n M_2^n ... \tilde{X}_{i-1}^n M_{i-1}^n \overrightarrow{C} S_1(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)Z^n).$$

Hence:

$$H((\tilde{X}_i^n, i \in B \bigcap [u])(M_i^n, i \in B \bigcap [u])|Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B))$$
$$\leq \sum_{i \mod m \in B \bigcap [u]} H(\overrightarrow{C}_i|\overrightarrow{C}_{1:i-1} Z^n) + H(S_1|\overrightarrow{C} Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)) +$$
$$\sum_{i \in B \bigcap [u]} H(\tilde{X}_i^n M_i|\tilde{X}_1^n M_1^n \tilde{X}_2^n M_2^n ... \tilde{X}_{i-1}^n M_{i-1}^n \overrightarrow{C} S_1)$$

But

$$H((\tilde{X}_i^n, i \in B \bigcap [u])(M_i^n, i \in B \bigcap [u])|Z^n(\tilde{X}_j^n, j \in B^c)(M_j^n, j \in [u]-B)) =$$
$$H((\tilde{X}_i^n, i \in B \bigcap [u])|Z^n(\tilde{X}_j^n, j \in B^c)) + nH((M_i^n, i \in B \bigcap [u])).$$

By simplifying the above expression, we get:

$$\sum_{j \in B \bigcap [u]} R'_j \geq H(\tilde{X}_{B \bigcap [u]}|Z\tilde{X}_{B^c}) - \frac{1}{n} H(S_1|S_{B^c})$$

Using Fano inequality, we can upper bound $\frac{1}{n} H(S_1|S_{B^c})$ and show that

$$\sum_{j \in B \bigcap [u]} R_j \geq H(\tilde{X}_{B \bigcap [u]}|Z\tilde{X}_{B^c})$$

We have $\text{Gain}_{SK} = H(X_1 X_2 ... X_u|Z) - \sum_{j=1}^u R'_j$. Letting ϵ go to zero (for any fixed $M_1, ..., M_u$), we get that

$$S_{no-r}(\tilde{X}_1 M_1; \tilde{X}_2 M_2; ... \tilde{X}_u M_u; \tilde{X}_{u+1}^{(s)}; ...; \tilde{X}_m^{(s)} \| Z) \leq$$
$$H(X_1 X_2 ... X_u|Z) - \min_{(R_1, R_2, ..., R_u) \in \Re} (\sum_{i=1}^u R_i).$$

Therefore

$$S(\tilde{X}_1; \tilde{X}_2; ...; \tilde{X}_u; \tilde{X}_{u+1}^{(s)}; ...; \tilde{X}_m^{(s)} \| Z) \leq$$
$$H(X_1 X_2 ... X_u|Z) - \min_{(R_1, R_2, ..., R_u) \in \Re} (\sum_{i=1}^u R_i).$$ ●

Proof of Theorem 7. It is enough to prove the lower bound for the special case of $q = 1$. This is because $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ can be bounded below by

$$S(X_1 U_{1:q-1}; X_2 U_{1:q-1}; ...; X_u U_{1:q-1}; (X_{u+1} U_{1:q-1})^{(s)}; ...; (X_m U_{1:q-1})^{(s)} \| Z U_{1:q-1})$$

since the m terminals can collaboratively create $i.i.d.$ repetitions of $U_{1:q-1}$. Here we are using the following inequality for $k = 1, 2, ..., q-2$:

$$S(X_1 U_{1:k-1}; X_2 U_{1:k-1}; ...; X_u U_{1:k-1}; (X_{u+1} U_{1:k-1})^{(s)}; ...; (X_m U_{1:k-1})^{(s)} \| Z U_{1:k-1}) \geq$$
$$S(X_1 U_{1:k}; X_2 U_{1:k}; ...; X_u U_{1:k}; (X_{u+1} U_{1:k})^{(s)}; ...; (X_m U_{1:k})^{(s)} \| Z U_{1:k})$$

We proceed with the assumption $q = 1$.

For any sequence $(a_1, a_2, ..., a_s)$, let $(a_1, a_2, ..., a_{i-1}, \overbrace{a_i}, a_{i+1}, ..., a_s)$ refers to the subsequence in which a_i is removed. Applying Lemma A4.1 of the appendix IV to the $m+1$-tuple:

$$(U_i, X_1U_{1:i-1}, ..., X_{(i-1) \mod m}U_{1:i-1}, \overbrace{X_{i \mod m}U_{1:i-1}}, X_{(i+1) \mod m}U_{1:i-1}, ..., X_mU_{1:i-1}, ZU_{1:i-1})$$

for $i = 1, 2, ..., p$, one can conclude existence of a natural number n and random variables $C_{1:p}$ satisfying the following four properties (here we use $U^n_{1:i-1}$ as a shorthand for $U^n_1U^n_2U^n_3...U^n_{i-1}$, n i.i.d repetitions of $U_1U_2...U_{i-1}$):

- C_i is a function of U^n_i, $i = 1, 2, 3..., p$;
- U^n_i could be reconstructed from C_i and $X^n_jU^n_{1:i-1}$ for all j with probability $1-\epsilon$ for $i = 1, 2, 3..., p$;
- $\frac{1}{n}I(C_i; Z^nU^n_{1:i-1}) < \epsilon + \max[0, I(U_i; ZU_{1:i-1}) - \min_j I(U_i; X_jU_{1:i-1})] = \epsilon + \max[0, I(U_i; Z|U_{1:i-1}) - \min_j I(U_i; X_j|U_{1:i-1})]$;
- $\frac{1}{n}H(U^n_i|C_iZ^nU^n_{1:i-1}) \geq \max[0, \min_j I(U_i; X_jU_{1:i-1}) - I(U_i; ZU_{1:i-1})] - \epsilon = \max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})] - \epsilon$.

Assume that the m terminals observe n i.i.d repetition of their random variables. At the i-th stage, U^n_i and C_i are created by the $(i \mod m)$-th terminal. C_i is then communicated to other terminals and thereby enabling the other $m-1$ terminals to create U^n_i with probability $1-\epsilon$. The probability that after p stages, all m terminals can not agree on the common randomness $U^n_1U^n_2U^n_3...U^n_p$ will therefore be at most $(m-1)p\epsilon$. In other words, if we let G_i represent the i-th terminal's guess of $U^n_{1:p}$, we will have:

$$P(G_1 = ... = G_m = U^n_{1:p}) = 1 - (m-1)p\epsilon.$$

We can bound from below $S(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ by

$$\frac{1}{n}S(G_1; G_2; ...; G_u; G^{(s)}_{u+1}; ...; G^{(s)}_m \| C_{1:p}Z^n) \geq$$
$$\frac{1}{n}[H(G_1|C_{1:p}Z^n) - \sum_{i=2}^m H(G_1|G_i)].$$

The last inequality was derived using the property 4 of theorem 1. Since

$$P(G_1 = ... = G_m = U^n_{1:p}) = 1 - (m-1)p\epsilon$$

we can work out the last expression as follows:

$$\frac{1}{n}[H(G_1|C_{1:p}Z^n) - \sum_{i=2}^m H(G_1|G_i)] \geq$$
$$\frac{1}{n}[H(U^n_{1:p}|C_{1:p}Z^n) - H(U^n_{1:p}|G_1) - \sum_{i=2}^m H(G_1|G_i)] \geq$$
$$\frac{1}{n}H(U^n_{1:p}|C_{1:p}Z^n) - m(h((m-1)p\epsilon) + (m-1)p\epsilon.c)$$

where c is the sum of the logarithm of the alphabet sizes of U_i and $h(.)$ is the binary entropy function.

We prove that $\frac{1}{n}H(U^n_{1:p}|C_{1:p}Z^n)$ is at least

$$\sum_{i=1}^p [\min_{1 \leq j \leq m} I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})] - 2p\epsilon.$$

If we can show this, the proof would be finished by letting ϵ tend zero.

$H(U_{1:p}^n|C_{1:p}Z^n) = \sum_{i=1}^p H(U_i^n|C_{1:p}Z^nU_{1:i-1}^n) =$

$\sum_{i=1}^p H(U_i^n|C_{1:i}Z^nU_{1:i-1}^n) - \sum_{i=1}^{p-1} I(U_i^n; C_{i+1:p}|C_{1:i}Z^nU_{1:i-1}^n) =$

$\sum_{i=1}^p H(U_i^n|C_iZ^nU_{1:i-1}^n) - \sum_{i=1}^{p-1} I(U_i^n; C_{i+1:p}|C_{1:i}Z^nU_{1:i-1}^n).$

Starting with the second term,

$\sum_{i=1}^{p-1} I(U_i^n; C_{i+1:p}|C_{1:i}Z^nU_{1:i-1}^n) =$

$\sum_{1\le i<j\le p} I(U_i^n; C_j|C_{1:j-1}Z^nU_{1:i-1}^n) =$

$\sum_{j=2}^p I(U_{1:j-1}^n; C_j|C_{1:j-1}Z^n) \le \sum_{j=2}^p I(U_{1:j-1}^nC_{1:j-1}Z^n; C_j) =$

$\sum_{j=2}^p I(U_{1:j-1}^nZ^n; C_j) \le \sum_{j=2}^p n.\big(\epsilon + \max[0, I(U_j; Z|U_{1:j-1}) - \min_r I(U_j; X_r|U_{1:j-1})]\big).$

Where we have used the third above-mentioned property of C_j's in the last step.

The first term in the above expansion of $H(U_{1:p}^n|C_{1:p}Z^n)$ can be bounded below using the fourth property of C_i's:

$\sum_{i=1}^p H(U_i^n|C_iZ^nU_{1:i-1}^n) \ge n.\sum_{i=1}^p \big(\max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})] - \epsilon\big).$

Therefore

$H(U_{1:p}^n|C_{1:p}Z^n) \ge$

$n.\sum_{i=1}^p \big(\max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})]\big) -$

$n.\sum_{i=2}^p \big(\max[0, I(U_i; Z|U_{1:i-1}) - \min_j I(U_i; X_j|U_{1:i-1})]\big) - 2np\epsilon.$

Since for every real number a, $\max[0, a] - \max[0, -a] \ge a$, we can conclude:

$\frac{1}{n}H(U_{1:p}^n|C_{1:p}Z^n) \ge \sum_{j=1}^p[\min_{1\le r\le m} I(U_j; X_r|U_{1:j-1}) - I(U_j; Z|U_{1:j-1})] - 2p\epsilon.$

It remains to prove that, in the case of two terminals, the new lower bound strictly improves the maximum of the two one way secrecy rates. Since $m = 2$, for simplicity we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. We note that for any arbitrary random variables V_1 and V_2 satisfying the Markov chain $V_2 - V_1 - X - YZ$, the choice of $p = q = 3$ and $U_1 = V_2$, $U_2 = 0$, $U_3 = V_1$ would achieve $I(V_2; Y|V_1) - I(V_2; Z|V_1)$. Therefore the new lower bound is no worse than the maximum of the two one way secrecy rates. We use the example and proof technique provided by Ahlswede and Csiszár in [1] to show that there are cases in which the new lower bound outperforms the maximum of the two one way secrecy rates. Assume that X_1 and X_2 are independent binary random variables. The joint conditional distribution of Y_1, Y_2, Z_1, Z_2 given X_1 and X_2 is defined in figure 1. Let $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$, $Z = (Z_1, Z_2)$. Assume further that X_1 has a uniform distribution.

The upper bound $I(X; Y|Z) = I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$ is also a lower bound on $S(X; Y\|Z)$. This is because the above expression is achievable with the choice of $U_1 = X_1$, $U_2 = Y_2$. But this can not be achieved by either of the one-way secrecy rates. As pointed out in [1], the one way secrecy rate $S(X; Y^{(s)}\|Z)$ depends only on $p(X, Y)$ and $p(X, Z)$. But $p((X_1, X_2), (Y_1, Y_2))$ is the

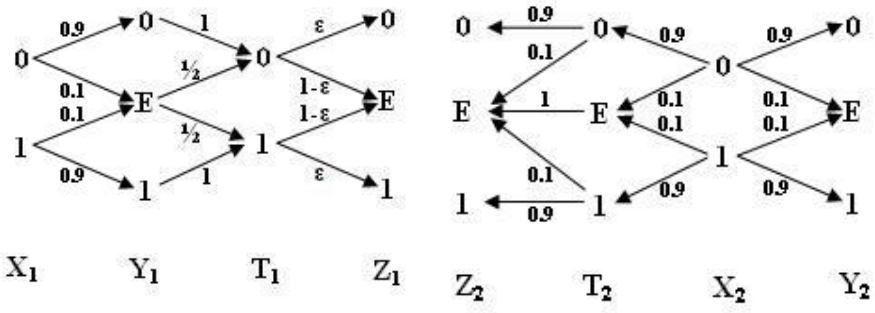

Fig. 1. The conditional distribution of (Y_1, Y_2, Z_1, Z_2) given X_1 and X_2.

same as $p((X_1, X_2), (Y_1, T_2))$. Further $(X_1, X_2) - (Y_1, T_2) - (Z_1, Z_2)$ forms a Markov chain. Therefore $S(X; Y^{(s)} \| Z) = I(X_1; Y_1|Z_1) + I(X_2; T_2|Z_2) < I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$. The last inequality is because $I(Y_2; Z_2) = 0.9I(X_2; Z_2) < I(X_2; Z_2)$.

Similarly, $S(X^{(s)}; Y \| Z) < I(X; Y|Z)$ because $p((Y_1, Y_2), (X_1, X_2))$ is the same as $p((Y_1, Y_2), (T_1, X_2))$ as X_1 has a uniform distribution, and also because $I(X_1; Z_1) < I(Y_1; Z_1)$. The latter inequality is valid because $H(Z_1|X_1) = h(0.95\epsilon, 1-\epsilon, 0.05\epsilon) > H(Z_1|Y_1) = 0.9h(\epsilon, 1-\epsilon) + 0.1h(0.5\epsilon, 1-\epsilon, 0.5\epsilon)$.

•

V. DISCUSSION

We have derived a new upper bound on the secret key rate which generalizes and improves the double intrinsic information bound of [12] to the multi-terminal case. We have also strengthened the results of [5] via a newly formulated problem of communication for omniscience by a neutral observer.

Table (I) contains some properties of $S_{no-r}(.)$ and $T(.)$ suggesting a duality. The inequalities mentioned in each section could be derived from each other by the following transformation:

$$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) =$$
$$H(X_1, X_2, X_3, ..., X_u|Z) - S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$$

In a recent conference paper [7] we proved that

$$T(X_1; X_2; X_3; ...; X_m \| Z) = \inf_r \tfrac{1}{r} T_c(X_1^r; X_2^r; X_3^r; ...; X_m^r \| Z^r)$$

where $T_c(X_1; X_2; X_3; ...; X_m \| Z)$ is the concave hull of $\{T(X_1; X_2; X_3; ...; X_m \| Z)\}$ (this is where the concavity of the choice of the right hand side of condition 4 of Theorem 2 was important). In appendix III, we prove that $T(X_1; X_2; X_3; ...; X_m \| Z)$ is not always concave.

TABLE I

SOME DUAL PROPERTIES OF $T(.)$ AND $S_{no-r}(.)$

$S_{no-r}(.)$:	$S_{..}(X_1;...;X_m^{(s)}\|ZU) \leq S_{..}(X_1U;...;X_m^{(s)}U\|ZU)$
$T(.)$:	$T(X_1;...;X_m^{(s)}\|ZU) \geq T(X_1U;...;X_m^{(s)}U\|ZU)$
$S_{no-r}(.)$:	$S_{..}(X_1;...;X_m^{(s)}\|Z) \geq S_{..}(X_1;...;X_m^{(s)}\|ZU)$
$T(.)$:	$T(X_1;...;X_m^{(s)}\|Z) \leq T(X_1;...;X_m^{(s)}\|ZU)+$ $I(X_1...X_u;U\|Z)$
$S_{no-r}(.)$:	$S_{..}(X_1;...;X_m^{(s)}\|Z) \leq S_{..}(X_1;...;X_m^{(s)}\|ZU)+$ $I(X_1...X_u;U\|Z)$
$T(.)$:	$T(X_1;...;X_m^{(s)}\|Z) \geq T(X_1;...;X_m^{(s)}\|ZU)$

VI. APPENDIX

A. Appendix I

In this appendix we prove existence of a joint probability distribution on X, Y, Z for which the new bound is strictly better than the double intrinsic information bound. In this appendix, we use the notation $\Im(X)$ to refer to the law of the random variable X.

We need the following Lemmas which we will prove at the end of this appendix:

Lemma A1.1 Assume that $\inf_U[H(U) + I(X;Y \downarrow ZU)] = \min_J[I(X;Y|J) + I(XY;J|Z)]$, then there is a sequence of random variables U_i, $i = 1, 2, ...$ taking values in finite sets Ω_i, and a sequence of positive real numbers δ_i converging to zero, such that:

1) $H(U_i) + I(X;Y \downarrow ZU_i) \to \inf_U[H(U) + I(X;Y \downarrow ZU)]$ as $i \to \infty$
2) $H(U_i|XYZ) \to 0$ as $i \to \infty$
3) $I(U_i;Z) \to 0$ as $i \to \infty$
4) $|p(U_i = u_j|X = x, Y = y, Z = z) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i \ \ \forall u_j \in \Omega_i, \ (x,y,z) : \ p(x,y,z) > 0$
5) The variational distance $d(\Im(U_i|Z = z_i), \Im(U_i|Z = z_j)) \to 0$ as $i \to \infty \ \ \forall z_i, z_j : \ p(Z = z_i) > 0, p(Z = z_j) > 0$

• *Lemma A1.2* Continuity of $I(X;Y \downarrow Z)$: $\forall \xi > 0, \exists \delta > 0$ such that for all random variables T having entropy less than δ, we have $|I(X;Y \downarrow ZT) - I(X;Y \downarrow Z)| < \xi$. •

TABLE II

JOINT PROBABILITY DISTRIBUTION OF X AND Y

Y \ **X**	0	1	2	3
0	$\frac{1}{8}$	$\frac{1}{8}$	0	0
1	$\frac{1}{8}$	$\frac{1}{8}$	0	0
2	0	0	$\frac{1}{4}$	0
3	0	0	0	$\frac{1}{4}$

We will perturb the example provided by Renner and Wolf in order to prove that their bound is better than the intrinsic information bound. Table (II) shows the joint probability distribution between X and Y in that example. Z is defined as:

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

Renner and Wolf proved that for the choice of $U = \lfloor \frac{X}{2} \rfloor$, one has

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

And therefore their bound would be less than or equal to $H(U) + I(X;Y \downarrow ZU) = 1$, while $I(X;Y \downarrow Z) = \frac{3}{2} > 1$.

Let V be a binary random variable, satisfying the $V - U - XYZ$ Markov property and defined as follows:

$$p(U=0|V=0) = \alpha_1 \qquad p(U=1|V=0) = 1-\alpha_1$$

$$p(U=0|V=1) = \alpha_2 \qquad p(U=1|V=1) = 1-\alpha_2$$

Clearly, there exists α_1 and α_2 such that:

- $\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\} \bigcap \{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\} = \{0,1\}$

If the constraint is not satisfied for some α_1 and α_2, then it would be enough to perturb α_1 or α_2 by a tiny amount.

Let $\widetilde{X} = X, \widetilde{Y} = Y, \widetilde{Z} = (Z, V)$. We would like to prove that the new bound is strictly better than the double intrinsic information bound for the triple $(\widetilde{X},\ \widetilde{Y}, \widetilde{Z})$.

We have:

$p(X = x, Y = y|\widetilde{Z} = (0,0)) =$

$\frac{1}{2}\alpha_1 \mathbb{1}[(x,y) = (0,0)] + \frac{1}{2}\alpha_1 \mathbb{1}[(x,y) = (1,1)] + (1-\alpha_1)\mathbb{1}[(x,y) = (2,2)]$

and,

$p(X = x, Y = y|\widetilde{Z} = (0,1)) =$

$\frac{1}{2}\alpha_2 \mathbb{1}[(x,y) = (0,0)] + \frac{1}{2}\alpha_2 \mathbb{1}[(x,y) = (1,1)] + (1-\alpha_2)\mathbb{1}[(x,y) = (2,2)]$

Assuming that the new bound is not better than the double intrinsic information bound, we can apply Lemma A1.1 to get a sequence U_i having the five properties given in Lemma A1.1. Using the property number 4, we have

$$|p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i$$
$$|p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i$$
$$|p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i$$

Therefore $p(U_i = u|\widetilde{Z} = (0,0))$ is within the $3\delta_i$ distance of a point in the set

$\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\}$.

Similarly, $p(U_i = u|\widetilde{Z} = (0,1))$ is within the $3\delta_i$ distance of a point in the set

$\{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\}$.

Now, as the variational distance between the distribution of $\Im(U_i|\widetilde{Z} = (0,0))$ and $\Im(U_i|\widetilde{Z} = (0,1))$ should converge to zero, and as the intersection between the sets $\{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\}$ and $\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\}$ is just $\{0,1\}$, one can conclude that there is some $i_0 \in \aleph$ so that for $\forall\ i > i_0,\ \forall u \in \Omega_i$, the probabilities

$p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))$,

$p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0))$,

$p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0))$

are either all less than $\frac{1}{2}$ or all greater than $\frac{1}{2}$.

Let $h(x) = x\log(\frac{1}{x})$. We would like to bound from above the entropy of the distribution of $\Im(U_i|\widetilde{Z} = (0,0))$ in terms of $h\big(p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))\big)$, $h\big(p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} =$

$(0,0))\big)$, $h\big(p(U_i=u|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))\big)$. Since entropy is a concave function, we can not use Jensen inequality to bound from above $H\big(\Im(U_i|\widetilde{Z}=(0,0))\big)$ which is a convex combination of these probabilities. However, noting that the three mentioned probabilities are all on the same side of $\frac{1}{2}$, and that $h(x)$ is monotonic for all $x<\frac{1}{2}$ and for all $x>\frac{1}{2}$, we can derive the following bound:

$$
\begin{aligned}
&H\big(\Im(U_i|\widetilde{Z}=(0,0)))\big)< \\
&\max\Big(h\big(p(U_i=u|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))\big), \\
&\qquad h\big(p(U_i=u|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))\big), \\
&\qquad h\big(p(U_i=u|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0)))\big)\Big)< \\
&\qquad h\big(p(U_i=u|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))\big)+ \\
&\qquad h\big(p(U_i=u|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))\big)+ \\
&\qquad h\big(p(U_i=u|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))\big)
\end{aligned}
$$

Therefore

$$
\begin{aligned}
&\textstyle\sum_u h\big(p(U_i|\widetilde{Z}=(0,0))\big)< \\
&\textstyle\sum_u h\big(p(U_i=u|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))\big)+ \\
&\textstyle\sum_u h\big(p(U_i=u|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))\big)+\sum_u h\big(p(U_i=u|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))\big)= \\
&H(U_i|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))+ \\
&H(U_i|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))+H(U_i|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))\to 0 \text{ as } i\to\infty.
\end{aligned}
$$

Therefore $H(U_i|\widetilde{Z}=(0,0))\to 0$ as $i\to\infty$. Similarly, $H(U_i|\widetilde{Z}=(0,1))\to 0$, etc. Thus,

$H(U_i|\widetilde{Z})\to 0$ as $i\to\infty$.

But the property number 3 of Lemma A1.1 states that $I(U_i;\widetilde{Z})\to 0$ as $i\to\infty$. Thus, we conclude that $H(U_i)\to 0$ as $i\to\infty$.

Hence, the limit of $H(U_i)+I(X;Y\downarrow ZU_i)$ is the same as that of $I(X;Y\downarrow ZU_i)$. The property number 1 of Lemma A1.1 states that the series converges to the double intrinsic information upper bound which is assumed to be equal to $\min_J[I(\widetilde{X};\widetilde{Y}|J)+I(\widetilde{X}\widetilde{Y};J|\widetilde{Z})]$.

Evaluating the expression at $J=\widetilde{Z}U$, gives us $0+I(XY;UZV|ZV)=I(XY;U|ZV)\le 1$

Therefore we should have: $\lim_{i\to\infty} I(X;Y\downarrow ZU_i)\le 1$. On the other hand, Renner and Wolf have shown that $I(X;Y\downarrow Z)=\frac{3}{2}$. But this is in contradiction with Lemma A1.2 noting that $H(U_i)\to 0$ as $i\to\infty$. ●

Now, we prove the Lemmas mentioned at the beginning of this appendix:

Proof of Lemma A1.1: Take a sequence U_1, U_2, ... such that

$H(U_i)+I(X;Y\downarrow ZU_i)\to \inf_U[H(U)+I(X;Y\downarrow ZU)]$.

For every U_i, there exists J_i such that $I(X;Y \downarrow ZU_i) = I(X;Y|J_i)$, and also $XY - ZU_i - J_i$ forming a Markov chain.

We have:

$I(XY;J_i|Z) = I(XY;U_i|Z) - I(XY;U_i|ZJ_i) \leq$

$I(XY;U_i|Z) = H(U_i|Z) - H(U_i|XYZ) = H(U_i) - I(U_i;Z) - H(U_i|XYZ)$.

Hence

$H(U_i) + I(X;Y \downarrow ZU_i) \geq [I(U_i;Z) + H(U_i|XYZ)] + [I(X;Y|J_i) + I(XY;J_i|Z)] \geq$

$[I(U_i;Z) + H(U_i|XYZ)] + \min_J [I(X;Y|J) + I(XY;J|Z)] =$

$[I(U_i;Z) + H(U_i|XYZ)] + \inf_U [H(U) + I(X;Y \downarrow ZU)]$.

Taking the limit as $i \to \infty$, we conclude that $[I(U_i;Z) + H(U_i|XYZ)] \to 0$ as $i \to \infty$. Therefore property number 2 and 3 are proved.

Since $H(U_i|XYZ) \to 0$, so should do $H(U_i|X=x,Y=y,Z=z)$ for all $(x,y,z):\ p(x,y,z) > 0$. Therefore for all $u \in \Omega_i$ $p(U_i = u|X=x,Y=y,Z=z) \log \frac{1}{p(U_i=u|X=x,Y=y,Z=z)}$ should go to zero. Therefore property number 4 is proved.

In order to prove property number 5, we note that

$I(U_i;Z) = \sum_{z:p(z)>0} p(z).D(\Im(U_i|Z=z) \| \Im(U_i)) \to 0$.

Therefore if $p(z_1)$ and $p(z_2)$ are positive, both $D(\Im(U_i|Z=z_1)\|\Im(U_i))$ and $D(\Im(U_i|Z=z_2)\|\Im(U_i))$ converge to zero. The Pinsker inequality, $D(p\|q) \geq \frac{1}{2\ln(2)} d^2(p,q)$ implies that both $d(\Im(U_i|Z=z_1), \Im(U_i))$ and $d(\Im(U_i|Z=z_2), \Im(U_i))$ converge to zero, and therefore the variational distance between $d(\Im(U_i|Z=z_1), \Im(U_i|Z=z_2))$ should also go to zero. ●

Proof of Lemma A1.2: Assume that $I(X;Y \downarrow ZT) = I(X;Y|J)$ for some $XY - ZT - J$.

$H(T) > H(T|Z) > p(Z=z)H(T|Z=z)$. Therefore

$H(T|Z=z) < \frac{\delta}{\min(p(z):p(z)>0)} \doteq Q$.

The denominator, $\min(p(z) : p(z) > 0)$, is a fixed constant depending on "z". Intuitively, since $H(T|Z=z)$ is small, with high probability it will be a constant. More precisely, assume that

$p(T = T_z|Z=z) \geq p(T=t|Z=z)$ for all t.

Since $H(T|Z=z) \geq h(p(T=T_z|Z=z))$, we have $h(p(T=T_z|Z=z)) \leq Q$. Let $c_1 \leq \frac{1}{2}$ and $c_2 = 1 - c_1$ be the two solutions of the equation $h(x) = Q$ in the interval $[0,1]$. c_2 goes to one as δ goes to zero. $h(p(T=T_z|Z=z)) \leq Q$ implies $p(T=T_z|Z=z) \leq c_1$ or $p(T=T_z|Z=z) \geq c_2$.

If $p(T=T_z|Z=z) \leq c_1$, we will have $p(T=t|Z=z) \leq c_1$ for all t. Therefore

$H(T|Z=z) \geq \log \frac{1}{c_1}$.

We also have $H(T|Z=z) < \frac{\delta}{\min(p(z):p(z)>0)}$. If δ goes to zero, $\frac{1}{c_1}$ goes to infinity, but $\frac{\delta}{\min(p(z):p(z)>0)}$

converges zero. Hence, for small enough δ, we must have $p(T = T_z|Z = z) \geq c_2$.

Define a random variable J' taking values on the same set as J is taking value on, such that

- $XY - Z - J'$ forms a Markov chain
- $p(J' = j|Z = z) = p(J = j|Z = z, T = T_z)$

We can furthermore couple J and J' so that $P(J \neq J') \leq 1 - c_2$ by first drawing J' and then changing it with probability $1 - c_2$. Let V be the indicator function of the event $J = J'$.

$$|I(X;Y|JJ') - I(X;Y|J)| = |I(X;Y|JJ'V) - I(X;Y|J)| \leq$$
$$|I(X;Y|JJ'V) - I(X;Y|JV)| + H(V) =$$
$$p(V = 0)|I(X;Y|JJ'V = 0) - I(X;Y|JV = 0)| + H(V) \leq$$
$$2p(V = 0)H(XY) + H(V)$$

Similarly, we can show that

$$|I(X;Y|JJ') - I(X;Y|J')| \leq 2p(V = 0)H(XY) + H(V)$$

These two inequalities show that $|I(X;Y|J') - I(X;Y|J)| \leq 4p(V = 0)H(XY) + 2H(V)$. $p(V = 0)$ and $H(V)$ converge to zero as δ goes to zero, we have: $\forall \xi > 0, \exists \delta > 0$ such that for all random variables T having entropy less than δ, we have $I(X;Y \downarrow Z) - I(X;Y \downarrow ZT) < \xi$.

It would be enough to prove that $I(X;Y \downarrow ZT) \leq I(X;Y \downarrow Z)$ to complete the proof. Assume J satisfies the Markov chain property $XY - Z - J$. Define a random variable J' taking values on the same set as J is taking value on, such that

- $p(J' = j|X = x, Y = y, Z = z, T = t) = p(J = j|X = x, Y = y, Z = z)$

We have $I(J';T|XYZ) = 0$, and $I(J';XY|Z) = I(J;XY|Z) = 0$. Therefore

$$I(J';XYT|Z) = I(J';XY|Z) + I(J';T|XYZ) = 0.$$

Since $I(J';XYT|Z) = I(J';T|Z) + I(J';XY|ZT)$, we have $I(J';XY|ZT) = 0$ and therefore the following Markov chain holds:

$$XY - ZT - J'.$$

Furthermore, we have $I(X;Y|J') = I(X;Y|Z)$. This proves that

$$I(X;Y \downarrow ZT) \leq I(X;Y \downarrow Z).$$ •

B. Appendix II

In this appendix, we verify that

$$\inf_J f^{-1}\big(f(S(X_1;X_2;...;X_u;(X_{u+1})^{(s)}...;(X_m)^{(s)}\|J)) + S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\big)$$

satisfies the five conditions of Theorem 1.

Property number 1.

It is enough to show that for any J, there exists some J' such that

$$n.f^{-1}\{f(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J)) + S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\} \geq$$
$$f^{-1}\{f(S(X_1^n;X_2^n;...;X_u^n;(X_{u+1}^n)^{(s)};...;(X_m^n)^{(s)}\|J')) + S_{f-one-way}(X_1^nX_2^n...X_m^n;J'^{(s)}\|Z^n)\}$$

We prove that $J' = J^n$ is an appropriate choice.

We will first prove that we will be done if we can prove that

$$n.S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z) \geq S_{f-one-way}(X_1^nX_2^n...X_m^n;(J^n)^{(s)}\|Z^n).$$

Let

$$s = S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J),$$
$$b = S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z), \text{ and}$$
$$c = S_{f-one-way}(X_1^nX_2^n...X_m^n;(J^n)^{(s)}\|Z^n) \leq nb.$$

We have:

$$f^{-1}\{f(ns)+c\} \leq f^{-1}\{f(ns)+nb\}$$

It suffices to prove that:

$$nf^{-1}\{f(s)+b\} \geq f^{-1}\{f(ns)+nb\} \text{ or equivalently}$$
$$f(nf^{-1}\{f(s)+b\}) \geq f(ns)+nb.$$

Let $t = f^{-1}\{f(s)+b\}-s$. We can then write this inequality as: $f(ns+nt) \geq f(ns)+nb$. According to the definition of t, we have $b = f(s+t)-f(s)$. Thus, we can rewrite the inequality as

$$f(ns+nt)-f(ns) \geq n.(f(s+t)-f(s)).$$

This inequality holds because f is increasing and convex.

It remains to show that

$$n.S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z) \geq S_{f-one-way}(X_1^nX_2^n...X_m^n;(J^n)^{(s)}\|Z^n).$$

Take some arbitrary U, and V satisfying $V-U-X_1^nX_2^n...X_m^n-J^nZ^n$. We will prove that there exist $\widetilde{U}$, and $\widetilde{V}$ satisfying

$$\widetilde{V}-\widetilde{U}-\widetilde{X_1}\widetilde{X_2}...\widetilde{X_m}-\widetilde{J}\widetilde{Z}$$

such that $(\widetilde{X_1},\widetilde{X_2},...,\widetilde{X_m},\widetilde{J},\widetilde{Z})$ has the same joint distribution as $(X_1,X_2,...,X_m,J,Z)$ and

$$f(H(U|Z^nV))-f(H(U|J^nV)) = n.\left[f(H(\widetilde{U}|\widetilde{Z}\widetilde{V}))-f(H(\widetilde{U}|\widetilde{J}\widetilde{V}))\right].$$

We start with the left hand side:

$$f(H(U|Z^nV))-f(H(U|J^nV)) =$$
$$\textstyle\sum_{i=1}^n f(H(U|Z^{i+1:n}J^{1:i-1}VZ(i)))-f(H(U|Z^{i+1:n}J^{1:i-1}VJ(i)))$$

By letting $V_i = Z^{i+1:n}J^{1:i-1}V$ and $U_i = (U,V_i)$ for $i = 1...n$, we can write the above equality as:

$f(H(U|Z^nV)) - f(H(U|J^nV)) = \sum_{i=1}^{n} f(H(U_i|V_iZ(i))) - f(H(U_i|V_iJ(i)))$

For every i, we have $V_i - U_i - X_1(i)X_2(i)...X_m(i) - J(i)Z(i)$. We would like to define an appropriate $(\widetilde{U}, \widetilde{V}, \widetilde{X_1}, \widetilde{X_2}, ..., \widetilde{X_m}, \widetilde{J}, \widetilde{Z})$ whose $f(H(\widetilde{U}|\widetilde{Z}\widetilde{V})) - f(H(\widetilde{U}|\widetilde{J}\widetilde{V}))$ is

$\frac{1}{n}(\sum_{i=1}^{n} f(H(U_i|V_iZ(i)) - f(H(U_i|V_iJ(i))))$.

This would be possible if the following region is convex:

$\{r \in \mathbb{R} | \exists U, V$ satisfying $(V - U - X_1X_2...X_m - JZ)$ such that $r = f(H(U|ZV)) - f(H(U|JV))\}$.

Since we can continuously move from $V_1 - U_1 - X_1X_2...X_m - JZ$ to $V_2 - U_2 - X_1X_2...X_m - JZ$ while having the expressions $H(U|ZV) = H(UVZ) - H(ZV)$ and $H(U|JV) = H(UJV) - H(JV)$ change continuously, the above region has to be convex (the entropy function is continuous in the whole probability simplex). The proof for this part is now completed.

Property number 2.

Let $H(F|X_i) = 0$, where $1 \leq i \leq m$. It is enough to show that for any J, the following inequality holds:

$f^{-1}\{f(S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J)) + S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z)\} \geq$

$f^{-1}\{f(S(X_1F; ...; X_uF; (X_{u+1}F)^{(s)}; ...; (X_mF)^{(s)} \| JF)) + S_{f-one-way}(X_1X_2...X_mF; (JF)^{(s)} \| ZF)\}$

It is clear that

$S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J) \geq$

$S(X_1F; ...; X_uF; (X_{u+1}F)^{(s)}; ...; (X_mF)^{(s)} \| JF)$

because the secret key rate itself satisfies the second property of Theorem 1. It remains to show that

$S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq S_{f-one-way}(X_1X_2...X_mF; (JF)^{(s)} \| ZF)$.

Since $H(F|X_i) = 0$, we can rewrite the last inequality as:

$S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq S_{f-one-way}(X_1X_2...X_m; (JF)^{(s)} \| ZF)$

Take some arbitrary U and V satisfying $V - U - X_1X_2...X_m - JZF$. It can be verified that for $\widetilde{U} = UF$ and $\widetilde{V} = VF$, the Markov property $\widetilde{V} - \widetilde{U} - X_1X_2...X_m - JZ$ holds. For this choice of $\widetilde{V}$ and $\widetilde{U}$:

$f(H(\widetilde{U}|\widetilde{V}Z)) - f(H(\widetilde{U}|\widetilde{V}J)) =$

$f(H((UF)|(VF)Z)) - f(H((UF)|(VF)J)) = f(H(U|V(ZF))) - f(H(U|V(JF)))$.

The proof for this part is now complete.

Property number 3.

By taking an approach similar to the one we took in the proof of the second condition, it would suffice to show that

$S_{f-one-way}(X_1X_2...X_m; J \| Z) \geq S_{f-one-way}(X_1'X_2'...X_m'; J \| Z)$.

Take U and V satisfying $V - U - X_1'X_2'...X_m' - JZ$. Define U_1 and V_1 in the following way:

$p(U_1, V_1, X_1, X_2, ..., X_m, Z, J) =$

$p(V_1|U_1).p(U_1|X_1', X_2', ..., X_m').p(X_1, X_2, ..., X_m ZJ)$, $p(V_1|U_1) = p(V|U)$

and

$p(U_1|X_1', X_2', ..., X_m') = p(U|X_1', X_2', ..., X_m')$.

It can be proved that $V_1 - U_1 - X_1X_2...X_m - JZ$ and that (V_1, U_1, J, Z) has the same joint distribution as (V, U, J, Z) implying $f(H(U_1|V_1Z)) - f(H(U_1|V_1J)) = f(H(U|VZ)) - f(H(U|VJ))$. The proof for this part is now complete.

Property number 4.

We need to prove that

$f^{-1}\{f(S(X_1; X_2; ...; X_m\|J)) + S_{f-one-way}(X_1X_2...X_m; J\|Z)\} \geq$

$H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)$.

If $H(X_1|Z) \leq \sum_{i=2}^m H(X_1|X_i)$, the inequality clearly holds. So we assume

$H(X_1|Z) > \sum_{i=2}^m H(X_1|X_i)$.

Using the fact that $S(X_1, X_2, ..., X_m\|J)$ itself satisfies property 4 of Theorem 1, and the definition of $S_{f-one-way}$, one can lower bound

$f^{-1}\{f(S(X_1; X_2; ...; X_m\|J)) + S_{f-one-way}(X_1X_2...X_m; J\|Z)\}$

by

$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^m H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$.

Having assumed that $H(X_1|Z) > \sum_{i=2}^m H(X_1|X_i)$, one of the following three cases must occur. In each case, we will prove that

$f^{-1}\{f(S(X_1, ..., X_m\|J)) + S_{f-one-way}(X_1...X_m; J\|Z)\} \geq H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)$.

1) $H(X_1|Z) \leq H(X_1|J)$: In this case,

$f(H(X_1|J) - \sum_{i=2}^m H(X_1|X_i)) \geq f(H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)) > 0$.

Therefore the lower bound

$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^m H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$

equals

$f^{-1}\{f(H(X_1|J) - \sum_{i=2}^m H(X_1|X_i))\}$

and is itself bounded below by

$f^{-1}\{f(H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i))\} = H(X_1|Z) - \sum_{i=2}^m H(X_1|X_i)$.

2) $H(X_1|Z) > \sum_{i=2}^m H(X_1|X_i) \geq H(X_1|J)$: In this case, the lower bound

$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^m H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$

equals

$$f^{-1}\{f(H(X_1|Z)) - f(H(X_1|J))\}.$$

But since

$$f(H(X_1|Z)) - f(H(X_1|Z) - H(X_1|J)) \geq$$
$$f(H(X_1|J)) - f(0),\ f^{-1}\{f(H(X_1|Z)) - f(H(X_1|J))\}$$

can be bounded below by $H(X_1|Z) - H(X_1|J)$ which in turn can be bounded below by

$$H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

3) $H(X_1|Z) > H(X_1|J) > \sum_{i=2}^{m} H(X_1|X_i)$: In this case the lower bound

$$f^{-1}\{f(\max[0, H(X_1|J) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$$

equals

$$f^{-1}\{f(H(X_1|J) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)) + f(H(X_1|Z)) - f(H(X_1|J))\}.$$

Since

$$H(X_1|Z) > H(X_1|J),\ f(H(X_1|Z)) - f(H(X_1|Z) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)) \geq$$
$$f(H(X_1|J)) - f(H(X_1|J) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)).$$

Therefore

$$f(H(X_1|J) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)) + f(H(X_1|Z)) - f(H(X_1|J)) \geq$$
$$f(H(X_1|Z) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)).$$

Therefore:

$$f^{-1}\{f(H(X_1|J) - \textstyle\sum_{i=2}^{m} H(X_1|X_i)) + f(H(X_1|Z)) - f(H(X_1|J))\} \geq$$
$$f^{-1}\{f(H(X_1|Z) - \textstyle\sum_{i=2}^{m} H(X_1|X_i))\} = H(X_1|Z) - \textstyle\sum_{i=2}^{m} H(X_1|X_i).$$

In all the three cases we have proved that

$$f^{-1}\{f(S(X_1, ..., X_m \| J)) + S_{f-one-way}(X_1 ... X_m; J \| Z)\} \geq H(X_1|Z) - \textstyle\sum_{i=2}^{m} H(X_1|X_i).$$

The proof for this part is now complete.

Property number 5.

It is enough to show that for any J, there exists J' such that the following inequality holds:

$$f^{-1}\{f(S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J)) +$$
$$S_{f-one-way}(X_1 X_2 ... X_m; J^{(s)} \| Z)\} \geq$$
$$f^{-1}\{f(S(X_1 M_1; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J')) +$$
$$S_{f-one-way}(X_1 M_1 ... X_u M_u X_{u+1} ... X_m; J'^{(s)} \| Z)\}$$

Take an arbitrary J jointly distributed with $(X_1, X_2, ..., X_m, Z)$, and define J' so that a)

$$p(J' X_1, X_2, ..., X_m, Z, M_1, ..., M_u) = p(J' X_1, X_2, ..., X_m, Z).p(M_1, ..., M_u)$$

and b)

TABLE III

JOINT PROBABILITY DISTRIBUTION OF X_1, X_2, X_3

X_3 \ X_1X_2	00	01	10	11
0	$\frac{1}{4}$	0	$\frac{1}{4}0.3$	$\frac{1}{4}0.7$
1	$\frac{1}{4}0.7$	$\frac{1}{4}0.3$	0	$\frac{1}{4}$

$p(J'|X_1, X_2, ..., X_m, Z) = p(J|X_1, X_2, ..., X_m, Z)$.

It is clear that

$S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; (X_m)^{(s)} \| J) \geq$

$S(X_1M_1; ...; X_uM_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J')$

because $p(J'|X_1, X_2, ..., X_m, Z) = p(J|X_1, X_2, ..., X_m, Z)$

and the secret key rate itself satisfies property number 5 of Theorem 1. It remains to show that

$S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq S_{f-one-way}(X_1M_1X_2M_2....X_uM_uX_{u+1}...X_m; J'^{(s)} \| Z)$.

Take some U and V satisfying $V - U - X_1X_2...X_mM_1...M_u - J'Z$. Since M_1, M_2, ..., M_u are independent of $(X_1, X_2, ..., X_m, Z, J')$, $M_1, M_2, ..., M_u$ can be thought of as playing the role of an external randomness employed by $X_1X_2...X_m$ to create U and V. Thus, if we let

$p(\widetilde{V}, \widetilde{U}|X_1X_2...X_mJZ) = p(V, U|X_1X_2...X_mJ'Z)$

$\widetilde{V}, \widetilde{U}$ will satisfy $\widetilde{V} - \widetilde{U} - X_1X_2...X_m - JZ$. For this choice of $\widetilde{V}$ and $\widetilde{U}$:

$f(H(\widetilde{U}|\widetilde{V}Z)) - f(H(\widetilde{U}|\widetilde{V}J)) = f(H(U|VZ)) - f(H(U|VJ))$.

The proof for this part is now complete. ●

C. Appendix III

In this appendix, we prove that $T(.)$ is not a concave function. Tables (III) and (IV) define probably distribution of binary random variables $X_1, X_2, X_3, X_1', X_2', X_3'$.

Let $(Y_1, Y_2, Y_3) = 0.5(X_1, X_2, X_3) + 0.5(X_1', X_2', X_3')$.

A simple calculation shows that $T(X_1, X_2, X_3\|\emptyset) = T(X_1', X_2', X_3'\|\emptyset) \cong 2.27$.

$T(Y_1, Y_2, Y_3\|\emptyset) \cong 2.25 < 2.27 = 0.5T(X_1, X_2, X_3\|\emptyset) + 0.5T(X_1', X_2', X_3'\|\emptyset)$. Therefore $T(.)$ is not a concave function.

TABLE IV

JOINT PROBABILITY DISTRIBUTION OF X_1', X_2', X_3'

X_3' \ $X_1'X_2'$	00	01	10	11
0	$\frac{1}{4}$	0	$\frac{1}{4}0.7$	$\frac{1}{4}0.3$
1	$\frac{1}{4}0.3$	$\frac{1}{4}0.7$	0	$\frac{1}{4}$

D. Appendix IV

Lemma A4.1 For any random variables $X_1, X_2, ..., X_m$ and Z taking value from sets χ_1, χ_2, χ_3, ..., χ_{m+1} and for any $\epsilon > 0$, there exist a natural number M such that for any $n \geq M$, there exists random variable C such that

- $H(C|X_1^n) = 0$;
- X_1^n could be reconstructed from C and X_j^n for all j with probability $1 - \epsilon$;
- $\frac{1}{n} I(C; Z^n) < \epsilon + \max(0, I(X_1; Z) - \min_j I(X_1; X_j))$;
- $\frac{1}{n} H(X_1^n | CZ^n) \geq \max[0, \min_j I(X_1; X_j) - I(X_1; Z) - \epsilon]$.

Proof:

We will find a mapping $f : \chi_1^n \mapsto \{1, 2, 3, ..., 2^{n(\max_j H(X_1|X_j) + c\epsilon)}\}$ such that $C = f(X_1^n)$ satisfies the required properties. $c < 1$ is a small constant that will be specified during the proof.

We consider two cases: In the first case we assume $I(X_1; Z) - \min_j I(X_1; X_j) \geq 0$. In other words $\max_j H(X_1|X_j) \geq H(X_1|Z)$. Consider the scenario in which the first terminal wants to enable the terminals X_2, X_3, ..., X_m and Z to recover his message with probability at least $1 - c\epsilon$. Slepian-Wolf tells us that there is a natural number M such that for any $n \geq M$, there exists random variable $C = f(X_1^n)$ of entropy $n[\max_j H(X_1|X_j) + c\epsilon]$ that would work. Among the four properties that C has to satisfy, all but the third one are trivial. Regarding the third inequality one can write:

$$I(X_1^n; Z^n) = I(C; Z^n) + I(X_1^n; Z^n|C) = I(C; Z^n) + H(X_1^n|C) - H(X_1^n|CZ^n).$$

According to the Fano inequality, $H(X_1^n|CZ^n)$ is of order $n(h(c\epsilon) + c\epsilon \log |\Delta_1|)$ since X_1^n can be recovered from CZ^n with probability $1 - c\epsilon$ and the logarithm of the support set of these random variables is of order n where Δ_1 is the alphabet set of X_1. The constant c can be chosen so that $h(c\epsilon) + c\epsilon \log |\Delta_1| \leq \epsilon$.

We get the desired bound on $I(C;Z^n)$ by noting that $H(X_1^n|C) = H(X_1^n) - H(C) = n[H(X_1) - \max_j H(X_1|X_j)] = n.\min_j I(X_1;X_j)$.

For the second case, we assume that $I(X_1;Z) - \min_j I(X_1;X_j) < 0$, or in other words

$\max_j H(X_1|X_j) < H(X_1|Z)$.

Slepian-Wolf shows the existence of a natural number M such that for any $n \geq M$, there are random variables $C = f(X_1^n)$ of entropy $n[\max_j H(X_1|X_j) + c\epsilon]$, and $C' = g(X_1^n)$ of entropy $n[H(X_1|Z) - \max_j H(X_1|X_j) + c\epsilon]$ such that X_1^n is recoverable from (C, C',Z^n) with probability $1 - c\epsilon$, and from (C, X_j^n) for any j with probability $1 - c\epsilon$. Now,

$I(X_1^n; CC'Z^n) = I(X_1^n; Z^n) + H(CC'|Z^n)$.

On the other hand,

$I(X_1^n; CC'Z^n) = H(X_1^n) - H(X_1^n|CC'Z^n) = H(X_1^n) - n(h(c\epsilon) + c\epsilon.\log|\Delta_1|)$.

The constant c can be chosen so that $h(c\epsilon) + c\epsilon.\log|\Delta_1| = \epsilon$. Therefore $H(CC'|Z^n) = H(X_1^n) - I(X_1^n;Z^n) - n\epsilon \geq H(C) + H(C') - n\epsilon$. In the last inequality we have used the fact that the values of $H(C)$ and $H(C')$ are known.

But since $H(CC'|Z^n) = H(C|Z^n) + H(C'|CZ^n)$, we can conclude $\frac{1}{n}I(C;Z^n) + \frac{1}{n}I(C';CZ^n) = \epsilon$. This proves the third property that C has to satisfy, i.e. $\frac{1}{n}I(C;Z^n) \leq \epsilon$. The fourth property can be proved by noting that

$\frac{1}{n}H(X_1^n|CZ^n) \geq \frac{1}{n}H(C'|CZ^n) \geq \frac{1}{n}[H(C') - I(C';CZ^n)] \geq$
$\min_j I(X_1;X_j) - I(X_1;Z) - \epsilon$. ●

ACKNOWLEDGMENT

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-0500023, 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. Korner, "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] 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.

[7] A. A. Gohari and V. Anantharam, “Communication for Omniscience by a Neutral Observer and Information-Theoretic Key Agreement of Multiple Terminals”, *Proceedings of International Symposium on Information Theory(ISIT)*, 2007, pp. 2056-2060.

[8] 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.

[9] U. M. Maurer and S. Wolf, “The Intrinsic Conditional Mutual Information and Perfect Secrecy”, *Proceedings of International Symposium on Information Theory (ISIT)*, 1997, p.88.

[10] 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.

[11] U. M. Maurer and S. Wolf, “From Weak to Strong Information-Theoretic Key Agreement”, *Proceedings of International Symposium on Information Theory (ISIT)*, 2000, p.18.

[12] 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.

[13] A. D. Wyner, “The Wiretap Channel”, *Bell System Technical Journal*, Vol. 54, No. 8, Oct. 1975, pp. 1355-1387.

[14] C.E. Shannon, “Communication Theory of Secrecy”, *Bell System Technical Journal*, Vol. 28, Oct. 1949, pp. 656-715.