Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing

Rudolph Ahlswede and Imre Csiszàr, *Fellow, IEEE*

Abstract—**As the first part of a study of problems involving common randomness at distant locations, information-theoretic models of secret sharing, i.e., of generating a common random key at two terminals, without letting an eavesdropper obtain information about this key, is considered. The concept of key-capacity is defined. Single-letter formulas of key-capacity are obtained for several models, and bounds to key-capacity are derived also for other models.**

Index Terms—**Common randomness, key-capacity, wiretapper, multiterminal source, multiway channels.**

I. Introduction

COMMON randomness available at distant locations plays an important role in various problems of information theory and cryptography. For example, if common randomness is available to sender and receiver, they can use random codes for transmitting information. In certain communication situations random codes can far outperform deterministic codes, e.g., in the case of arbitrarily varying channels; for the latter, concerning the relation of capacity for deterministic codes to capacity for random codes, cf. Ahlswede [1] and Csiszár and Narayan [6]. Common randomness shared by sender and receiver plays a key role also in the theory of identification capacity as opposed to transmission capacity, recently developed by Ahlswede and Dueck [2], [3]. The significance of common randomness is perhaps most obvious in cryptography, where a random key shared by two terminals can be used for secure communication between them, by encryption; here the common randomness (the key) should be such that a third party (the eavesdropper) has no information about it.

We propose a systematic study of the role of common randomness in information theory and cryptography. In this first part, attention will be restricted to generating common randomness without giving information about it to a third party, i.e., to secret sharing.

Secret sharing may be realized by generating a random message at either terminal and transmitting it over a secure channel to the other one, but also in more complex ways that may involve communication over a public channel and using side information that may be available. Of course, once secret sharing has taken place, it can always be used to achieve secret transmission via encryption. While this general problem area has been intensively researched, it has hardly been looked at from the information—theoretic point of view. The popular computational complexity approach (Diffie and Hellman [7], Rivest, Shamir, and Adleman [9]) certainly appears fruitful. Still, we argue that an information-theoretic approach to this field is also needed. Even though it may not lead to the emergence of new cryptosystems, it is likely to lead to new insights, complementing the more practical complexity approach in much the same way as Shannon theory, in general, complements communication theory and coding theory.

An information-theoretic model of communication subject to secrecy constraints is Wyner's "wiretap channel" [10], to be reviewed in Section III. Intuitively, a wiretap channel is a channel with one input and two output terminals; one output terminal is seen by the legitimate receiver and the other by an eavesdropper or "wiretapper." One question is at what rate, if any, can messages be sent to the legitimate receiver while keeping the wiretapper completely ignorant of the message sent.

Recently, Maurer [8] demonstrated that the availability of a public feedback channel could make secret transmission possible even in such cases when the secrecy capacity without feedback was zero. In fact, Maurer proposed a scheme that enabled the legitimate receiver to share a random key with the sender, using transmissions over the public feedback channel in such a way that no information about the key was given away to the wiretapper. In this scheme, both the legitimate receiver's and the wiretapper's channel were assumed to be binary symmetric, with independent but otherwise arbitrary noise. Since the key generated by the receiver and shared with the sender could be used to encrypt messages, secret transmission became possible even if the wiretapper's channel was the better one. Maurer also hinted at a source-type model. His presentation gave an important motivation for this work.

We will consider two kinds of models of secret sharing, one having the flavor of source coding and the other of channel coding. These two kinds of models are closely related. Some problems that immediately present themselves will be completely or partially solved. The large variety of related problems is left for future research.

To facilitate understanding, first the simplest models will be treated, in Section II. Our main results will be stated in

Manuscript received September 18, 1991; revised December 10, 1992. This work was presented at the IEEE International Symposium on Information Theory, Budapest, Hungary, June 24 to 28, 1991. A prior version of this paper was Preprint 90-081 (November 1990) in the series "Sonderforschungsbereich Diskrete Strukturen in der Mathematik" of the University of Bielefeld, Germany.

R. Ahlswede is with the Mathematics Department of the University of Bielefeld, D-4800 Bielefeld, Germany.

I. Csiszár is with the Mathematical Institute of the Hungarian Academy of Sciences, H-1364 Budapest, POB 127, Hungary.

IEEE Log Number 9208637.

Section III and proved in Section IV. Throughout the paper, the terminology of the book Csiszár and Körner [5] will be used.

In the proofs, essential use is made of techniques developed by Csiszár and Körner [4] for the wiretap channel and its generalization called broadcast channel with confidential messages. Still, in order to keep the paper self-contained, the paper [4] or more sophisticated material of the book [5] will not be directly relied upon.

After this paper had been submitted, the authors learned of more recent results of Maurer on generating a shared key, that partially overlap with results in this paper. Maurer's results will be published in full in [12], and some of them appear already in [11]. In particular, Maurer [11] gave lower bounds on what we call key-capacity for the channel-type model with wiretapper, in the binary case. He also showed that the key rate he had obtained in [8] was the best possible for that model. This proof relied on a general upper bound stated but not proved in [11], which was the same as ours in Theorem 2. Maurer [12] addresses general source-type and channel-type models with wiretapper (in our terminology) and gives lower and upper bounds on key-capacity, including a proof of the upper bound stated in [11]. He also obtains the results of the Corollaries of our Theorems 1 and 2. Maurer's results do not include a single-letter characterization of key-capacity with a one-way use of the public channel (our Theorems 1 and 2) and nor do they include our Theorem 3. On the other hand, his papers [11], [12] contain some other results which we do not have in this paper.

II. Generating a Shared Secret Key when Third Party has No Side Information

The main results of this paper will be stated in Section III. Here, we introduce simpler versions of the problems treated there, in order to facilitate their understanding.

In both models, we consider secret sharing between two terminals, to be called Terminal $\mathcal{X}$ and Terminal $\mathcal{Y}$. Both models involve an unspecified integer n (the blocklength), and we will be interested in the case when n is large.

Model S (Source-Type Model): We are given a DMMS (discrete memoryless multiple source) with two component sources and generic variables (X, Y). Terminal $\mathcal{X}$ "can see" the source outputs $X^n = (X_1, \cdots, X_n)$ and Terminal $\mathcal{Y}$ "can see" the source outputs $Y^n = (Y_1, \cdots, Y_n)$. Further, a noiseless public channel of unlimited capacity is available for communication between the two terminals.

Model C (Channel-Type Model): We are given a DMC (discrete memoryless channel) $\{W: \mathcal{X} \to \mathcal{Y}\}$. Terminal $\mathcal{X}$ can govern the input of this DMC while Terminal $\mathcal{Y}$ observes the output. In addition to transmissions of length n over this DMC, which is considered a secure channel, also a noiseless public channel of unlimited capacity may be used for communication between the two terminals.

Remark: In Model C, we chose to denote the input and output alphabets by the same symbols as the corresponding terminals, believing that this will be intuitive rather than ambiguous. Similarly, in Model S, the alphabets of the two component sources will also be denoted by $\mathcal{X}$ and $\mathcal{Y}$.

Next, we describe what we mean by permissible secret sharing strategies. Since we want to allow for all strategies that are intuitively conceivable (even very complex ones that may be quite inpractical), this description is somewhat cumbersome. The main result of this section will be that recourse to those complex secret sharing strategies is not necessary because optimum secret sharing can be achieved in a very simple way.

Communication over the public channel will be visualized as an exchange of messages or codewords Φ_i, generated by Terminal $\mathcal{X}$, and Ψ_i, generated by Terminal $\mathcal{Y}$, at consecutive instances $i = 1, \cdots, k$. Here, Φ_i and Ψ_i may depend on all information available at the corresponding terminal at instant i. For convenience, these Φ_i and Ψ_i will be referred to as *forward transmissions* and *backward transmissions*, respectively. Of course, our model includes the possibility of one-way communication, because Φ_i or Ψ_i (or both) may be set equal to the empty word. It will be convenient to assume that as the zeroth step of any secret sharing strategy, the two terminals generate independent random variables $M_{\mathcal{X}}$ and $M_{\mathcal{Y}}$, respectively, and all further steps are deterministic. This does not restrict generality, because any randomized operations at either terminal (at any step) may be equivalently regarded as deterministic operations that depend also on an initially chosen random variable $M_{\mathcal{X}}$ or $M_{\mathcal{Y}}$, respectively.

Now the formal definition of a permissible secret sharing strategy for Model S is as follows.

Step 0) The terminals generate random variables $M_{\mathcal{X}}$ and $M_{\mathcal{Y}}$ such that $M_{\mathcal{X}}$, $M_{\mathcal{Y}}$, and (X^n, Y^n) are mutually independent.

Step 1) The two terminals exchange messages Φ_1, Ψ_1 over the public channel, where $\Phi_1 = \Phi_1(M_{\mathcal{X}}, X^n)$, $\Psi_1 = \Psi_1(M_{\mathcal{Y}}, Y^n)$.

Step i) The two terminals exchange messages Φ_i, Ψ_i where $\Phi_i = \Phi_i(M_{\mathcal{X}}, X^n, \Psi^{i-1})$, $\Psi_i = \Psi_i(M_{\mathcal{Y}}, Y^n, \Phi^{i-1})$ (with the usual shorthand that upper index denotes a sequence up to that index).

Final step (after k "exchange steps" have taken place)) Both terminals compute what they deem to be the key established by the secret sharing process, as a function of the information available to them:

$$K = K(M_{\mathcal{X}}, X^n, \Psi^k), \qquad L = L(M_{\mathcal{Y}}, Y^n, \Phi^k), \quad (2.1)$$

where K and L take values in the same finite set $\mathcal{K}$.

Of course, K and L must satisfy certain conditions in order that we can speak of a successful secret sharing. Before stating these (viz. (2.4) and (2.5) in Definition 2.1), first we define the permissible strategies for Model C. Here, the situation is more complex because two channels are available for communication (the secure DMC, however, in one direction only) and these may be used in an interactive way.

In the following formal definition of a permissible secret sharing strategy for Model C, we assume that the n symbols transmitted over the DMC are sent at the instants $i_1 < i_2 < \cdots < i_n$, and the public channel is used at the remaining instants $i \in \{1, \cdots, k\} \backslash \{i_1, \cdots, i_n\}$; here $i_1 \geq 1$, $i_n \leq k$, and for technical convenience we set $i_{n+1} = k + 1$.

Step 0) The terminals generate independent random variables $M_{\mathcal{X}}$ and $M_{\mathcal{Y}}$.

Step i, $0 < i < i_1$) The terminals exchange messages Φ_i, Ψ_i over the public channel, where $\Phi_i = \Phi_i(M_{\mathcal{X}}, \Psi^{i-1})$, $\Psi_i = \Psi_i(M_{\mathcal{Y}}, \Phi^{i-1})$.

Step $i = i_j$, $1 \le j \le n$) Terminal $\mathcal{X}$ determines the jth input X_j to the DMC, $X_j = X_j(M_{\mathcal{X}}, \Psi^{i_j-1})$, and Terminal $\mathcal{Y}$ observes the corresponding output Y_j. Φ_i and Ψ_i are set void.

Step i, $i_j < i < i_{j+1}$, $1 \le j \le n$) The terminals exchange messages Φ_i, Ψ_i over the public channel, where

$$\Phi_i = \Phi_i(M_{\mathcal{X}}, \Psi^{i-1}), \qquad \Psi_i = \Psi_i(M_{\mathcal{Y}}, Y^{j-1}, \Phi^{i-1}). \tag{2.2}$$

Final step) Same as in Model S; now in (2.1) actually $K = K(M_{\mathcal{X}}, \Psi^k)$, because X^n is uniquely determined by $M_{\mathcal{X}}$ and Ψ^k.

Notice that a strategy as above always determines X_j as a function of $M_{\mathcal{X}}$, $M_{\mathcal{Y}}$ and Y^{j-1}. The formal meaning of saying that Y_j is the DMC output corresponding to input X_j is

$$\Pr\{Y_j = y \mid M_{\mathcal{X}} = m,\ M_{\mathcal{Y}} = m',\ Y^{j-1} = y^{j-1}\} = W(y \mid X_j(m, m', y^{j-1})), \tag{2.3}$$

where $X_j(m, m', y^{j-1})$ denotes the input X_j determined by $M_{\mathcal{X}} = m$, $M_{\mathcal{Y}} = m'$, $Y^{j-1} = y^{j-1}$. It is easy to see that the functional relationships in the description of the strategy and (2.3) uniquely determine the joint distribution of all random variables involved (once the distributions of $M_{\mathcal{X}}$ and $M_{\mathcal{Y}}$ are specified), as it is necessary for mathematical consistency.

Definition 2.1: For Model S or C, a number H will be called an *achievable key rate* if for every $\epsilon > 0$ and sufficiently large n there exists a permissible secret sharing strategy such that K and L of (2.1) satisfy

$$\Pr\{K \neq L\} < \epsilon \tag{2.4}$$

$$\frac{1}{n} I(\Phi^k, \Psi^k \wedge K) < \epsilon \tag{2.5}$$

$$\frac{1}{n} H(K) > H - \epsilon \tag{2.6}$$

and

$$\frac{1}{n} \log |\mathcal{K}| < \frac{1}{n} H(K) + \epsilon. \tag{2.7}$$

The largest achievable key rate is the *key-capacity*.

Here, (2.4) means that the two terminals have indeed generated a common key (with a small probability of error), and (2.5) means that this is a secret key: the exchange over the public channel has given away effectively no information about it. Condition (2.7) means that the distribution of the key is nearly uniform in an entropy sense; this certainly appears desirable if the key is to be used for encryption, the most likely purpose of secret sharing.

Now we show that if H is an achievable key rate in the sense of Definition 2.1 then, using the established key for encryption, secure transmission at rate H is possible over the public channel. For this, we set (without restricting generality) $\mathcal{K} = \{1, \cdots, N\}$, and consider the encryption of a random message $M \in \{1, \cdots, N\}$ (generated at Terminal $\mathcal{X}$, say) simply as $M \oplus K$ where $\oplus$ denotes addition mod N. If $M \oplus K$ is sent over the public channel, Terminal $\mathcal{Y}$ can decode M with small probability of error (by (2.4)). The next lemma shows hat a cryptanalist having access to the public transmissions only, gets effectively no information about M.

Lemma 2.1: For a random variable M with values in $\{1, \cdots, N\}$ and independent of (Φ^k, Ψ^k, K), (2.5) and (2.7) imply that

$$\frac{1}{n} I(\Phi^k, \Psi^k, M \oplus K \wedge M) < 2\epsilon.$$

Proof:

$$\begin{aligned} &I(\Phi^k, \Psi^k, M \oplus K \wedge M) \\ &\overset{\text{(i)}}{=} I(M \oplus K \wedge M \mid \Phi^k, \Psi^k) \\ &= H(M \oplus K \mid \Phi^k, \Psi^k) - H(M \oplus K \mid M, \Phi^k, \Psi^k) \\ &\le \log N - H(K \mid M, \Phi^k, \Psi^k) \\ &\overset{\text{(ii)}}{\le} H(K) + n\epsilon - H(K \mid M, \Phi^k, \Psi^k) \\ &= I(K \wedge M, \Phi^k, \Psi^k) + n\epsilon \overset{\text{(iii)}}{\le} 2n\epsilon. \end{aligned}$$

Here, (i) holds because M is independent of (Φ^k, Ψ^k), (ii) follows from (2.7) with $|\mathcal{K}| = N$, and (iii) follows from (2.5) because M is independent of (Φ^k, Ψ^k, K). □

Remark: The same proof shows that if $I(\Phi^k, \Psi^k \wedge K)$ were exactly 0 and the distribution of K were exactly uniform then we would have $I(\Phi^k, \Psi^k, M \oplus K \wedge M) = 0$, i.e., perfect secrecy. In the simple models of this section this is indeed attainable, but in the more complex models of Section III one probably has to be satisfied with the almost complete secrecy of Lemma 2.1.

For technical reasons, it will be convenient to introduce also the concepts of *weakly achievable key rates* and *weak key-capacity*. These are obtained by dropping the conditions (2.4), (2.7) in Definition 2.1 and replacing (2.6) by

$$\frac{1}{n} I(K \wedge L) > H - \epsilon, \tag{2.8}$$

while condition (2.5) is retained. The fact that every achievable key rate is also weakly achievable, as the terminology suggests, follows immediately from the definition, using Fano's inequality.

In the simple models treated in this section it will be easily shown that weak key-capacity actually equals key-capacity. We expect that the same holds also for the more complex models and all variants of the concept of key-capacity treated in Section III; indeed, this will be established in all cases when we can determine the key-capacity. Still, no attempt will be made to prove a general theorem about this equality because this technical problem does not appear to be of primary interest.

The main result in this section is the following.

Proposition 1:

a) For Model S, key-capacity and weak key-capacity both equal the mutual information $I(X \wedge Y)$ and this is attainable by using a single forward (or backward) transmission only.

b) For Model C, key-capacity and weak key-capacity both equal the ordinary capacity $C(W)$ of the DMC $\{W\}$, and this is attainable without using the public channel at all.

Proof: First we prove the direct assertion of a), i.e., that $I(X \wedge Y)$ is an achievable key rate by using a single forward transmission. The idea is to transmit a code of X^n of rate $\approx H(X \mid Y)$ that, with the knowledge of Y^n, makes the reproduction of X^n possible with small probability of error. A closer look at the proof of the Slepian–Wolf theorem ([5], pp. 238–239, Theorem 1.2) reveals that this can be done in such a way that the desired secret sharing results.

For a formal proof, consider the DMC $\{W\colon \mathcal{X} \to \mathcal{Y}\}$ where $W = P_{Y|X}$, fix $\epsilon > 0$, $\delta > 0$, $\eta > 0$, and pick consecutively disjoint codeword sets C_i of (n, ϵ)-codes for this DMC, each consisting of codewords of the same type, and each of size

$$M = \lceil \exp\{n(I(X \wedge Y) - \delta)\} \rceil. \tag{2.9}$$

If this process can not be continued after having picked C_N, say, then necessarily

$$P_X^n\left(\bigcup_{i=1}^{N} C_i\right) > 1 - \eta \tag{2.10}$$

(providing n is sufficiently large). Indeed, any subset A of $\mathcal{X}^n$ with $P_X^n(A) \geq \eta$ contains a codeword set C with the desired properties ([5, p. 107]; there the constant type property was not required, but it can obviously be attained by looking at the largest subcode with codewords of constant type).

Now let Terminal $\mathcal{X}$ transmit

$$\Phi(X^n) = \begin{cases} i, & \text{if } X^n \in C_i, \quad 1 \leq i \leq N \\ 0, & \text{if } X^n \notin \bigcup_{i=1}^{N} C_i. \end{cases}$$

Enumerate (in any way) the elements of each C_i, and set $K = j$ if X^n equals the jth element of some C_i. Terminal $\mathcal{Y}$, knowing Y^n and $\Phi(X^n) = i$, can use the decoder of the channel code with codeword set C_i; set $L = j$ if this decoding results in the jth element of C_i. Then, since $W = P_{Y|X}$, and an (n, ϵ)-code was used for the DMC $\{W\}$, we have

$$\Pr\{L \neq K \mid X^n \in C_i\} < \epsilon, \qquad i = 1, \cdots, N.$$

This and (2.10) imply that

$$\Pr\{K \neq L\} < \epsilon + \eta, \tag{2.11}$$

no matter how K and L are defined when $X^n \notin \bigcup_{i=1}^{N} C_i$. Further, since each set C_i consists of sequences of the same type, the conditional distribution of K on the condition $X^n \in C_i$ is uniform on $\{1, \cdots, M\}$, for every $i = 1, \cdots, N$. For convenience, for $X^n \notin \bigcup_{i=1}^{N} C_i$ we set K equal to a random variable uniformly distributed on $\{1, \cdots, M\}$ and independent of X^n, Y^n.

By this simple scheme a key has been obtained, shared by both terminals ((2.11)), that is both uniformly distributed and independent in the exact sense of Φ transmitted over the public channel, and such that $1/nH(K)$ is arbitrarily close to $I(X \wedge Y)$ ((2.9)).

Having proved the direct assertion of a), and the direct assertion of b) being obvious from the DMC coding theorem, it remains to prove the converses, i.e., that a weakly achievable key rate can not exceed $I(X \wedge Y)$ in Model S or $C(W)$ in Model C.

To this we send forward a simple lemma.

Lemma 2.2: Let U and V be arbitrary random variables, and let $\Phi_1, \cdots, \Phi_k$, $\Psi_1, \cdots, \Psi_k$ be such that for every $i \leq k$, Φ_i is a function of U and Ψ^{i-1}, and Ψ_i is a function of V and Φ^{i-1}. Then,

$$I(U \wedge V \mid \Phi^k, \Psi^k) \leq I(U \wedge V).$$

Proof:

$$\begin{aligned} I(U \wedge V \mid \Phi^k, \Psi^k) &= I(U \wedge V \mid \Phi^{k-1}, \Phi_k, \Phi^{k-1}, \Psi_k) \\ &\leq I(U, \Phi_k \wedge V \mid \Phi^{k-1}, \Psi^{k-1}, \Psi_k) \\ &\leq I(U, \Phi_k \wedge V, \Psi_k \mid \Phi^{k-1}, \Psi^{k-1}) \\ &= I(U \wedge V \mid \Phi^{k-1}, \Psi^{k-1}); \end{aligned}$$

here the last step follows from the assumption that Φ_k is a function of (U, Ψ^{k-1}) and Ψ_k is a function of (V, Φ^{k-1}). Repeating this argument k times, the lemma follows.

Returning to the proof of the converse assertions of Proposition 1, consider any strategy (permissible for either Model S or Model C) with the property (2.5). Then

$$\begin{aligned} I(K \wedge L) &\leq I(K \wedge L, \Phi^k, \Psi^k) \\ &\leq I(K \wedge L \mid \Phi^k, \Psi^k) + n\epsilon. \end{aligned} \tag{2.12}$$

Now, for Model S, we have

$$\begin{aligned} I(K \wedge L \mid \Phi^k, \Psi^k) &\overset{\text{(i)}}{\leq} I(M_{\mathcal{X}}, X^n \wedge M_{\mathcal{Y}}, Y^n \mid \Phi^k, \Psi^k) \\ &\overset{\text{(ii)}}{\leq} I(M_{\mathcal{X}}, X^n \wedge M_{\mathcal{Y}}, Y^n) \\ &\overset{\text{(iii)}}{=} I(X^n \wedge Y^n) = nI(X \wedge Y). \end{aligned} \tag{2.13}$$

Here, (i) follows by (2.1), (ii) from Lemma 2.2, and (iii) from the independence of $M_{\mathcal{X}}$, $M_{\mathcal{Y}}$, (X^n, Y^n). Substituting (2.13) into (2.12) completes the proof of the converse for Model S.

For Model C, we have

$$\begin{aligned} I(K \wedge L \mid \Phi^k, \Psi^k) &\overset{\text{(i)}}{\leq} I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}, Y^n \mid \Phi^k, \Psi^k) \\ &\overset{\text{(ii)}}{\leq} I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}, Y^n) \\ &\overset{\text{(iii)}}{=} \sum_{j=1}^{n} I(M_{\mathcal{X}} \wedge Y_j \mid M_{\mathcal{Y}}, Y^{j-1}). \end{aligned} \tag{2.14}$$

Here, (i) follows because for Model C in (2.1) we have $K = K(M_{\mathcal{X}}, \Psi^k)$, (ii) follows by Lemma 2.2, and (iii) is the chain rule, taking into account that $I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}) = 0$. But by (2.3), we have

$$\begin{aligned} &I(M_{\mathcal{X}} \wedge Y_j \mid M_{\mathcal{Y}}, Y^{j-1}) \\ &\quad = H(Y_j \mid M_{\mathcal{Y}}, Y^{j-1}) - H(Y_j \mid M_{\mathcal{X}}, M_{\mathcal{Y}}, Y^{j-1}) \\ &\quad = H(Y_j \mid M_{\mathcal{Y}}, Y^{j-1}) - H(Y_j \mid X_j) \leq I(X_j \wedge Y_j). \end{aligned}$$

Hence, the right side of (2.14) is upper bounded by $nC(W)$. Returning to (2.12), the proof for Model C is complete. □

III. Secret Sharing When Third Party has Side Information

In this section, we consider generalizations of the simple models treated in Section II to the case when the third party to be kept ignorant of the result of secret sharing (to be called the wiretapper) has access to more information than what is transmitted over the public channel.

Model SW (Source-Type Model with Wiretapper): We are given a DMMS with three component sources and generic variables (X, Y, Z). Terminal $\mathcal{X}$ "sees" the source outputs X^n, Terminal $\mathcal{Y}$ "sees" the source outputs Y^n, and the wiretapper "sees" the source outputs Z^n.

Model CW (Channel-Type Model with Wiretapper): We are given a DMC $\{W: \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}\}$. Terminal $\mathcal{X}$ governs the input, Terminal $\mathcal{Y}$ "sees" the Y-outputs, whereas the wiretapper "sees" the Z-outputs.

In both cases a noiseless public channel of unlimited capacity is also available for communication between Terminals $\mathcal{X}$ and $\mathcal{Y}$; communication over this channel is completely known to the wiretapper.

The permissible strategies for Models SW and CW are the same as for Models S and C in Section II, with two formal modifications: For Model SW, in Step 0 we have to postulate that $M_{\mathcal{X}}$, $M_{\mathcal{Y}}$, (X^n, Y^n, Z^n) are mutually independent, and in Model CW it has to be taken into account that every DMC input X_j generates a pair of outputs Y_j, Z_j; the formal way of doing this is to replace (2.3) by

$$\Pr\{Y_j = y,\ Z_j = z \mid M_{\mathcal{X}} = m,\ M_{\mathcal{Y}} = m',\ Y^{j-1} = y^{j-1},\ Z^{j-1} = z^{j-1}\} = W(y, z \mid X_j(m, m', y^{j-1})). \quad (3.1)$$

Definition 2.1 and its relaxation stated before Proposition 1 apply also to Models SW and CW, with the single change that (2.5) has to be replaced by

$$\frac{1}{n} I(\Phi^k, \Psi^k, Z^n \wedge K) < \epsilon. \quad (3.2)$$

In order to deal more systematically with the question of whether simple strategies suffice in Models SW and CW to achieve the key-capacity, we will consider some variants of the concept of key-capacity, obtained by restricting the class of permissible secret sharing strategies.

One possible restriction would be that no more than k exchanges are permitted over the public channel; the analogue of key-capacity under this restriction might be called k-key-capacity. In this paper, only the case $k = 1$ will be considered, moreover the restriction will be made that only a forward or only a backward transmission is permitted (formally, all Ψ_i and Φ_i in the description of a permissible strategy in Section II equal the empty word, except for one Ψ_i or Φ_i); recall that "forward" means the direction $\mathcal{X} \to \mathcal{Y}$ and "backward" the direction $\mathcal{Y} \to \mathcal{X}$. Thus, for both models SW and CW, we define the *forward key-capacity* and *backward key-capacity*, as well as their weak versions, analogously to the general definition of key-capacity (weak key-capacity) but permitting the use of the public channel for a single forward transmission or a single backward transmission only. For Model SW these two notions are completely symmetric but for Model CW they differ substantially.

By Proposition 1, for Models S and C both the forward and backward key-capacities equal the key-capacity. We will see that for Models SW and CW this is no longer true, in general. It remains, however, open whether for either model key-capacity can ever be larger than what by the previous paragraph would be termed the 1-key-capacity.

Before stating our main results, let us briefly review previous literature related to our subject. The model "wiretap channel" introduced by Wyner [10] and generalized by Csiszár and Körner [4] (cf. also [5, p. 407]) can be described as follows: Given $W: \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$, the sender is required to encode a random variable M, uniformly distributed over a possibly large set, into a channel input X^n so that M be decodable (with small probability of error) from the received sequence Y^n whereas the other output sequence Z^n should give negligibly small information about M. The supremum of the rates $1/nH(M)$ subject to these conditions is called the *secrecy capacity*. Since this coding problem depends on W only through its marginal channels $W_1: \mathcal{X} \to \mathcal{Y}$ and $W_2: \mathcal{X} \to \mathcal{Z}$, it is often stated—as in [4], [5]—in terms of these two channels rather than $W: \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$. Wyner [10] determined the secrecy capacity for the case when W_2 was a degraded version of W_1, and Csiszár and Körner [4] gave a single-letter characterization of secrecy capacity in the general case.

Clearly, any code in the definition of secrecy capacity represents a secret sharing strategy for our Model CW, that does not use the public channel at all, but has the properties required in Definition 2.1. Hence, both the forward and backward key-capacity for Model CW must be at least as large as the wiretap secrecy capacity. Not unexpectedly, we will see that the forward key-capacity for Model CW is actually equal to the corresponding wiretap channel secrecy capacity.

The general problem of secret sharing does not seem to have been considered before in Shannon theory context, but an important step in this direction was made by Maurer [8]. He considered a wiretap channel whose marginal channels W_1 and W_2 were both binary symmetric, and had "independent noise" which, in our terminology, means that

$$W(y, z \mid x) = W_1(y \mid x)W_2(z \mid x). \quad (3.3)$$

For this case, Maurer proposed a scheme in which the sender transmitted a $1/2 - 1/2$ i.i.d. sequence, and it was the receiver who sent back information, using a public channel, in such a way that the original sender could decode this information but the wiretapper remained in complete ignorance. This made a key exchange at a positive rate possible even in those cases when the wiretap channel secrecy capacity was equal to zero. Clearly, in our terminology, the key rate achieved in this way is a lower bound to backward key-capacity and hence also to key-capacity. Our results will imply that the key rate achieved by Maurer's scheme is actually equal to the key-capacity of his model, thus his scheme is optimal for that case.

At this point, a general observation about the relationship of Models SW and CW suggests itself. Namely, if a channel-type

model (with wiretapper) is determined by W: $\mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$, an associated class of source-type models is determined by the class of DMMS's with generic variables (X, Y, Z) such that $P_{YZ|X} = W$. Given the channel-type model, Terminal $\mathcal{X}$ can simulate either of the source-type models in the associated class, simply by letting the input sequence X^n consist of i.i.d. random variables. It follows that the key-capacity for the channel-type model is greater than or equal to the supremum of the key-capacities for the associated source-type models. Remarkably, in those cases when we could determine key-capacity, here the equality holds; it remains open whether the same is true in general.

Now we state the main results of this paper. Though not stated explicitly, all assertions are true also for the weak versions of the corresponding key-capacities. The theorems stated in this section will be proved in Section IV.

Theorem 1: For Model SW, the forward key-capacity equals the maximum of

$$I(T \wedge Y \mid U) - I(T \wedge Z \mid U), \tag{3.4}$$

for all pairs of random variables T, U (taking values in sufficiently large finite sets) that satisfy the Markov condition

$$U\text{–}\circ\text{–}T\text{–}\circ\text{–}X\text{–}\circ\text{–}YZ. \tag{3.5}$$

Further, the key-capacity is upper bounded by $I(X \wedge Y \mid Z)$, and this bound is tight if X, Y, Z form a Markov chain in any order.

Corollary: If $X\text{–}\circ\text{–}Y\text{–}\circ\text{–}Z$ then forward key-capacity and key-capacity both equal $I(X \wedge Y) - I(X \wedge Z)$.

Theorem 2: For Model CW, the forward key-capacity is equal to the secrecy capacity of the corresponding wiretap channel, namely to the maximum of $I(T \wedge Y) - I(T \wedge Z)$ for all triples of random variables T, Y, Z such that for some X with $P_{YZ|X} = W$ the Markov condition $T\text{–}\circ\text{–}X\text{–}\circ\text{–}YZ$ holds. Further, the key-capacity is upper bounded by the maximum of $I(X \wedge Y \mid Z)$ subject to $P_{YZ|X} = W$, and this bound is tight if W has the property that $P_{YZ|X} = W$ implies that X, Y, Z form a Markov chain in some order.

Corollary:

1) If W has the form

$$W(y, z \mid x) = W_1(y \mid x)V(z \mid y) \tag{3.6}$$

then forward key-capacity and key-capacity both equal the maximum of $I(X \wedge Y) - I(X \wedge Z)$ subject to $P_{YZ|X} = W$, and can be attained without any use of the public channel.

2) If W is of form (3.3) then backward key-capacity and key-capacity both equal the maximum of $I(X \wedge Y) - I(Y \wedge Z)$ subject to $P_{YZ|X} = W$, and this is in general larger than forward key-capacity.

Remarks:

1) The sets of expressions whose maximum is claimed to equal forward key-capacity for Models SW and CW, respectively, remain unchanged if the ranges of the auxiliary random variables T and U are supposed to be (sufficiently large but finite) fixed sets. This can be seen in a standard way using the Support Lemma ([5, p. 310]), as was explicitly done in Csiszár and Körner [4]. It follows, in particular, that the maximums in question are indeed attained.

2) The upper bounds in Theorems 1 and 2 on key-capacity may sometimes be poor, e.g., they may be larger than key-capacity in the absence of a wiretapper, determined in Section II. For Model SW, the bound may be improved by the simple observation that for any random variable V satisfying the Markov condition $XY\text{–}\circ\text{–}Z\text{–}\circ\text{–}V$, the key-capacity for the DMMS with generic variables (X, Y, V) is at least as large as for that with (X, Y, Z). Hence the result of Theorem 1 implies that the minimum of $I(X \wedge Y \mid V)$ subject to $XY\text{–}\circ\text{–}Z\text{–}\circ\text{–}V$ is also an upper bound to key-capacity in Model SW. The bound for Model CW given in Theorem 2 could be improved in a similar way. Still, we have no reason to believe that even these improved bounds are tight.

Although the upper bounds on key-capacity for Models SW and CW given in Theorems 1 and 2 are not tight, in general, they always give the exact answer for a natural modification of these models. This modification consists in the assumption that Terminal $\mathcal{X}$ (or Terminal $\mathcal{Y}$) has access to the wiretapper's side information, i.e., the source resp. channel output sequence Z^n is available to Terminal $\mathcal{X}$ (or Terminal $\mathcal{Y}$).

In this modification of Model SW or CW, for which we prefer not to introduce a new notation, the permissible strategies will differ from those for Model SW or CW only in the obvious way: the operations at that terminal where Z^n is available may depend also on Z^n or, in the channel-type model, on that part Z^j of Z^n that is already available.

It appears safe to save space by omitting formal definitions, so we just state the following theorem.

Theorem 3: If Model SW or CW is modified by letting either Terminal $\mathcal{X}$ or Terminal $\mathcal{Y}$ know the Z-outputs, the key-capacity for the source-type model will always equal $I(X \wedge Y \mid Z)$ and for the channel-type model the maximum of $I(X \wedge Y \mid Z)$ subject to $P_{YZ|X} = W$. Further, this also equals the backward or forward key-capacity, respectively, according as Terminal $\mathcal{X}$ or Terminal $\mathcal{Y}$ is informed.

At first sight, the result of Theorem 3 appears counterintuitive, because it means that in some cases we can do better with a known wiretapper than if there were no wiretapper at all. The answer is, of course, that access to the wiretapper's information does contribute to generating common randomness (what secret sharing is all about) and this benefit can more than balance out the negative effect that the wiretapper must be kept ignorant of this common randomness.

It may be instructive to consider the following examples.

Example 1: Let the DMMS with generic variables (X,Y,Z) be as follows: let X and Y be independent $1/2 - 1/2$ binary random variables, and $Z = X + Y \mod 2$. Then, $I(X \wedge Y) = 0$, $I(X \wedge Y \mid Z) = 1$. Clearly, if the terminals $\mathcal{X}$ and $\mathcal{Y}$ have access to X^n and Y^n only, no secret sharing between them is possible. However, if Terminal $\mathcal{X}$, say, knows also Z^n then he can compute Y^n. Thus, with $K = Y^n$, secret sharing with

key rate equal to 1 has taken place; the wiretapper remains completely ignorant because $I(Z^n \wedge Y^n) = 0$.

Example 2: Let the DMMS with generic variables (X,Y,Z) be as follows: $X = (X', X'')$, $Y = (Y', Y'')$, $Z = (Z', Z'')$, where X'–o–Y'–o–Z', Y''–o–X''–o–Z'', and the triples (X', Y', Z') and (X'', Y'', Z'') are independent. Applying the Corollary of Theorem 1 to the mutually independent DMMS's with generic variables (X', Y', Z') and (X'', Y'', Z''), it follows that for the first DMMS

$$I(X' \wedge Y' \mid Z') = I(X' \wedge Y') - I(X' \wedge Z') \tag{3.7}$$

is an achievable key rate, with a single forward transmission, and for the second DMMS

$$I(X'' \wedge Y'' \mid Z'') = I(X'' \wedge Y'') - I(Y'' \wedge Z'') \tag{3.8}$$

is an achievable key rate, with a single backward transmission. Hence, for the DMMS with generic variables (X, Y, Z),

$$I(X \wedge Y \mid Z) = I(X' \wedge Y' \mid Z') + I(X'' \wedge Y'' \mid Z'') \tag{3.9}$$

is an achievable key rate, with one forward transmission and one backward transmission. Thus, in this example, the key-capacity equals the upper bound in Theorem 1, and it can be attained by one exchange of messages over the public channel. In particular, the sufficient condition for the tightness of the bound to key-capacity in Theorem 1 is not necessary. This example also shows that the key-capacity can strictly exceed both the forward and backward key-capacities. To see this, let the joint distribution of X'', Y'', Z'' be such that

$$I(X'' \wedge Z'') > I(Y'' \wedge Z'') \tag{3.10}$$

(i.e., the data processing lemma for Y''–o–X''–o–Z'' holds with the strict inequality) and that X''–o–$\tilde{Y}''$–o–Z'' for some $\tilde{Y}''$ with $P_{X''\tilde{Y}''} = P_{X''Y''}$, where—without restricting generality—we assume that $(X'', \tilde{Y}'', Z'')$ is independent of (X', Y', Z'). By Theorem 1, forward key-capacity depends on the joint distribution P_{XYZ} through its marginals P_{XY} and P_{XZ} only. Hence, in the present case the forward key-capacity remains unchanged if $Y = (Y', Y'')$ is replaced by $\tilde{Y} = (Y', \tilde{Y}'')$, and therefore—using the Corollary of Theorem 1—it equals

$$\begin{aligned} I(X \wedge \tilde{Y}) - I(X \wedge Z) &= I(X \wedge Y) - I(X \wedge Z) \\ &= I(X' \wedge Y') + I(X'' \wedge Y'') \\ &\quad - I(X' \wedge Z') - I(X'' \wedge Z''). \end{aligned}$$

On account of (3.7), (3.8), (3.10), the last expression is smaller than $I(X \wedge Y \mid Z)$ in (3.9). It follows similarly that the backward key-capacity is also smaller than the key-capacity (3.9), providing the joint distribution of X', Y', Z' is suitable.

IV. Proofs

Proof of Theorem 1: We send forward a general observation: if T–o–X–o–YZ then any Model-SW secret sharing strategy for the DMMS with generic variables (T, Y, Z) gives rise to one with identical secrecy performance for the DMMS with generic variables (X, Y, Z). To see this, let $\{T_{x,i}\}_{x \in \mathcal{X},\ 1 \le i \le n}$ be a collection of random variables, independent of each other and of (X^n, Y^n, Z^n) (the outcomes of the DMMS with generic variables (X, Y, Z)), and set

$$T_i = T_{x,i} \text{ if } X_i = x, \qquad (i = 1, \cdots, n).$$

Then (T^n, Y^n, Z^n) will represent outcomes of the DMMS with generic variables (T, Y, Z), and any secret sharing strategy for the latter amounts to a secret sharing strategy for the DMMS with generic variables (X, Y, Z), regarding the collection $\{T_{x,i}\}$ as part of the random variable $M_{\mathcal{X}}$ generated at Terminal $\mathcal{X}$ in Step 0.

To prove the direct part of Theorem 1 it suffices to show that for any U with U–o–X–o–YZ, $I(X \wedge Y \mid U) - I(X \wedge Z \mid U)$ is a forward-achievable key rate (i.e., achievable with a single forward transmission). Indeed, applying this to the DMMS with generic variables (T, Y, Z), it will follow that (3.4) is a forward-achievable key rate for the DMMS whenever T and U satisfy the Markov condition (3.5). By the observation sent forward, this implies that (3.4) is a forward-achievable key rate also for the original DMMS, which means that the forward key-capacity is at least as large as the maximum of (3.4) subject to (3.5).

The proof that

$$H = I(X \wedge Y \mid U) - I(X \wedge Z \mid U)$$

is a forward-achievable key rate (if U–o–X–o–YZ) will be similar to the proof of the direct part of Proposition 1a), but now $\mathcal{X}^n$ will be partitioned into sets C_i of a more complex structure, namely wiretap-channel codes.

Formally, supposing $H > 0$, without any loss of generality, we apply Lemma A in the Appendix to consecutively select mutually disjoint sets $C_i \subset \mathcal{X}^n$ such as $\tilde{A}$ in that Lemma. Then, if this process can not be continued after having selected C_N, we necessarily have

$$P_X^n\left(\bigcup_{i=1}^{N} C_i\right) > 1 - \eta. \tag{4.1}$$

By definition, each C_i consists of sequences of the same type and is the codeword set of an (n, ϵ)-code for the DMC $\{V\}$, where V represents the conditional distribution $P_{Y|X}$. Further, C_i is the disjoint union of $M = \lceil \exp\{n(H - \epsilon)\} \rceil$ subsets $C_{i,m}$ of equal size, such that the following holds: If $\hat{X}^n$ is uniformly distributed on C_i and the conditional distribution of $\hat{Z}^n$ on the condition $\hat{X}^n$ is $P_{Z|X}^n$ then, setting $\hat{K} = m$ if $\hat{X}^n \in C_{i,m}$, we have

$$I(\hat{Z}^n \wedge \hat{K}) < \tau n. \tag{4.2}$$

Now, let Terminal $\mathcal{X}$ transmit

$$\Phi = \Phi(X^n) = \begin{cases} i, & \text{if } X^n \in C_i, \quad 1 \le i \le N \\ 0, & \text{if } X^n \notin \bigcup_{i=1}^{N} C_i. \end{cases}$$

Further, define K as that index m for which $X^n \in C_{i,m}$ if $X^n \in C_i$; if $X^n \notin \bigcup_{i=1}^{N} C_i$, let K be equal to a random variable uniformly distributed on $\{1, \cdots, M\}$ and independent of X^n, Y^n, Z^n. Finally, let $L = L(Y^n, \Phi)$ be defined by setting $L = m$ if $\Phi = i$, $1 \le i \le N$, and the decoding of the (n, ϵ)-code for the DMC $\{V\}$ with codeword set C_i results

in a codeword that belongs to $C_{i,m}$; if $\Phi = 0$ then L can be arbitrary.

We claim that the secret sharing strategy defined by Φ, K, and L as above satisfies the conditions in Definition 2.1 for the achievability of H, of course with (2.5) replaced by (3.2). Actually, since there is only a single forward transmission Φ, (3.2) reduces to

$$\frac{1}{n} I(\Phi, Z^n \wedge K) < \epsilon. \tag{4.3}$$

Clearly, the definition of K and L implies by (4.1) that (2.4) is satisfied, with $\epsilon + \eta$ in the role of ϵ. Further, since C_i consists of sequences of the same type and each $C_{i,m}$ has the same size, the conditional distribution of K on the condition $X^n \in C_i$ is the uniform distribution on $\{1, \cdots, M\}$; the same holds, by definition, also on the condition $X^n \notin \bigcup_{i=1}^N C_i$. Thus, K is uniformly distributed on $\mathcal{K} = \{1, \cdots, M\}$, and it is independent of Φ. In particular, condition (2.7) holds trivially, and on account of $M = \lceil \exp\{n(H - \epsilon)\} \rceil$ so does also (2.6).

It remains to check (4.3). Now,

$$\begin{aligned} I(\Phi, Z^n \wedge K) &\overset{\text{(i)}}{=} I(Z^n \wedge K \mid \Phi) \\ &\overset{\text{(ii)}}{=} \sum_{i=1}^N P_X^n(C_i) I(Z^n \wedge K \mid X^n \in C_i) \end{aligned} \tag{4.4}$$

Here (i) follows by the independence of K and Φ, and (ii) holds because

$$I\left(Z^n \wedge K \mid X^n \notin \bigcup_{i=1}^N C_i\right) = 0$$

by the definition of K. Since C_i consists of sequences of the same type, the conditional distribution of X^n on the condition $X^n \in C_i$ is uniform on C_i. It follows that the conditional joint distribution of Z^n and K on the condition $X^n \in C$ is the same as the joint distribution of $\hat{Z}^n$ and $\hat{K}$ in (4.2). Thus (4.2) and (4.4) imply that (4.3) is satisfied with τ in the role of ϵ.

Turning to the converse part of Theorem 1, consider any strategy with a single forward transmission Φ, i.e., let

$$\Phi = \Phi(M_{\mathcal{X}}, X^n), \quad K = K(M_{\mathcal{X}}, X^n),$$

$$L = L(M_{\mathcal{Y}}, Y^n, \Phi). \tag{4.5}$$

We will show that if (4.3) holds then there exist T and U satisfying the Markov condition (3.5) such that

$$\frac{1}{n} I(K \wedge L) \le I(T \wedge Y \mid U) - I(T \wedge Z \mid U) + \epsilon. \tag{4.6}$$

The proof is similar to the wiretap channel converse proof of Csiszár and Körner [4], and relies on the following

Lemma 4.1: For arbitrary random variables U, V and sequences of random variables Y^n, Z^n we have

$$\begin{aligned} &I(U \wedge Y^n \mid V) - I(U \wedge Z^n \mid V) \\ &= \sum_{i=1}^n [I(U \wedge Y_i \mid Y^{i-1} Z_{i+1} \cdots Z_n V) \\ &\quad - I(U \wedge Z_i \mid Y^{i-1} Z_{i+1} \cdots Z_n V)]. \end{aligned}$$

Proof: This identity appears in [4]; still, for completeness, we give a proof since it is quite simple.

The ith term of the sum equals

$$\begin{aligned} &H(U \mid Y^{i-1} Z_{i+1} \cdots Z_n V) - H(U \mid Y^i Z_{i+1} \cdots Z_n V) \\ &\quad - H(U \mid Y^{i-1} Z_{i+1} \cdots Z_n V) \\ &\quad + H(U \mid Y^{i-1} Z_i Z_{i+1} \cdots Z_n V) \\ &= H(U \mid Y^{i-1} Z_i \cdots Z_n V) - H(U \mid Y^i Z_{i+1} \cdots Z_n V). \end{aligned}$$

Summing these, after cancellations the result is

$$H(U \mid Z^n V) - H(U \mid Y^n V).$$

On the other hand,

$$\begin{aligned} &I(U \wedge Y^n \mid V) - I(U \wedge Z^n \mid V) \\ &= H(U \mid V) - H(U \mid Y^n V) \\ &\quad - H(U \mid V) + H(U \mid Z^n V) \\ &= H(U \mid Z^n V) - H(U \mid Y^n V). \end{aligned}$$

Continuing the proof of Theorem 1, we can write

$$\begin{aligned} I(K \wedge L) &\overset{\text{(i)}}{\le} I(K \wedge M_{\mathcal{Y}}, Y^n, \Phi) \\ &\overset{\text{(ii)}}{=} I(K \wedge Y^n, \Phi) \\ &\overset{\text{(iii)}}{\le} I(K \wedge Y^n, \Phi) - I(K \wedge Z^n, \Phi) + n\epsilon \\ &= I(K \wedge Y^n \mid \Phi) - I(K \wedge Z^n \mid \Phi) + n\epsilon \\ &\overset{\text{(iv)}}{=} \sum_{i=1}^n [I(K \wedge Y_i \mid Y^{i-1} Z_{i+1} \cdots Z_n \Phi) \\ &\quad - I(K \wedge Z_i \mid Y^{i-1} Z_{i+1} \cdots Z_n \Phi)] + n\epsilon. \end{aligned} \tag{4.7}$$

Here (i) is by (4.5), (ii) because of the independence of $M_{\mathcal{Y}}$ from (K, Y^n, Φ), implied by (4.5) and the mutual independence of $M_{\mathcal{X}}$, $M_{\mathcal{Y}}$, (X^n, Y^n); (iii) is from (4.3), and (iv) is by Lemma 4.1.

The last sum can be written, in the usual way, as

$$n[I(K \wedge Y_J \mid U) - I(K \wedge Z_J \mid U)],$$

where J is a random variable independent of all the previous ones and uniformly distributed on $\{1, \cdots, n\}$, and $U = Y^{J-1} Z_{J+1} \cdots Z_n \Phi J$. Thus, (4.7) gives

$$\begin{aligned} \frac{1}{n} I(K \wedge L) &\le I(K \wedge Y_J \mid U) - I(K \wedge Z_J \mid U) + \epsilon \\ &= I(T \wedge Y_J \mid U) - I(T \wedge Z_J \mid U) + \epsilon, \end{aligned} \tag{4.8}$$

where $T = (K, U)$.

It is clear from the definitions of J, U, and T—using also (4.5)—that the Markov property U–o–T–o–X_J–o–$Y_J Z_J$ holds and the joint distribution of X_J, Y_J, Z_J is the same as that of X, Y, Z. Hence, (4.8) establishes our claim (4.6), and this proves that (weak) forward key-capacity can not be larger than the maximum of all expressions of form (3.4), with the Markov condition (3.5).

The upper bound on (weak) key-capacity stated in Theorem 1 follows by the simple argument in the proof of Proposition 1. Namely for any secret sharing strategy satisfying (3.2) we have

$$I(K \wedge L) \le I(K \wedge L \mid \Phi^k, \Psi^k, Z^n) + \epsilon n, \tag{4.9}$$

and to the exact analogy of the derivation of (2.13) we obtain that

$$I(K \wedge L \mid \Phi^k, \Psi^k, Z^n) \le I(X^n \wedge Y^n \mid Z^n) = nI(X \wedge Y \mid Z)$$

(a minor difference is that Lemma 2.2 has to be used in a "conditional" version; but clearly that Lemma remains valid if a conditioning random variable is added on both sides). Substituting this into (4.9) shows that $I(X \wedge Y \mid Z)$ is an upper bound to weak key-capacity.

If X–o–Z–o–Y then $I(X \wedge Y \mid Z)$ is equal to 0 and hence gives a tight bound. Suppose next that X–o–Y–o–Z. Then $I(X \wedge Y \mid Z) = I(X \wedge Y) - I(X \wedge Z)$ is a forward-achievable key rate by the first assertion of Theorem 1 (set $T = X$, $U = \text{const}$ in (3.4)). As key-capacity could only be larger than forward key-capacity, this shows that the upper bound $I(X \wedge Y \mid Z)$ is tight in this case. Finally, the third possible Markovity Y–o–X–o–Z is not a new case, by symmetry.

The corollary has already been proved.

Proof of Theorem 2: Clearly, the forward key-capacity for Model CW is at least as large as the secrecy capacity of the corresponding wiretap channel. As shown by Csiszár and Körner [4], the latter equals the maximum of

$$I(T \wedge Y) - I(T \wedge Z), \tag{4.10}$$

for random variables T such that T–o–X–o–YZ for some X with $P_{YZ|X} = W$. Presently, we use only the direct part of this result, namely that the secrecy capacity is at least as large as (4.10), for any T as before; this is an easy consequence of Lemma A in the Appendix, applied to T, Y, Z in the role of X, Y, Z, with $U = \text{const}$. Now, the first assertion of Theorem 2 will be proved if we show that the weak forward key-capacity can not exceed the maximum of (4.10) for T as before. To this end, we use the method of Csiszár and Körner [4] as in the proof of Theorem 1.

Consider any secret sharing strategy for Model CW that enters the definition of weak forward key-capacity. Then, since there are no backward transmissions, X^n has to be a function of $M_{\mathcal{X}}$ alone, and so have also Φ (the forward transmission over the public channel) and K:

$$X^n = X^n(M_{\mathcal{X}}), \quad \Phi = \Phi(M_{\mathcal{X}}), \quad K = K(M_{\mathcal{X}}).$$

Unlike in the proof of Theorem 1, Y^n and Z^n are now the channel outputs corresponding to input X^n, but (4.7) still holds as there (for step (ii) of the derivation of (4.7) we need that $M_{\mathcal{Y}}$ is independent of (K, Y^n, Φ); this is intuitively obvious, and formally follows from (3.1) where now $X_j(m, m', y^{j-1}) = X_j(m)$). Also the rewriting (4.8) works as there, and the resulting random variables $X_J Y_J Z_J$ satisfy both $P_{Y_J Z_J | X_J} = W$ and the Markov condition U–o–T–o–X_J–o–$Y_J Z_J$. It follows that the weak forward key-capacity can not be larger than the maximum of

$$I(T \wedge Y \mid U) - I(T \wedge Z \mid U) \tag{4.11}$$

subject to the condition $P_{YZ|X} = W$ and the Markov condition U–o–T–o–X–o–YZ. Finally, notice that (4.11) can be written as the average of $I(T_u \wedge Y_u) - I(T_u \wedge Z_u)$ with respect to the distribution of U, where T_u, X_u, Y_u, Z_u denote random variables whose joint distribution equals the conditional joint distribution of T, X, Y, Z on the condition $U = u$; in particular, the Markov condition T_u–o–X_u–o–$Y_u Z_u$ holds and $P_{Y_u Z_u | X_u} = P_{YZ|X} = W$. Thus, (4.11) is upper bounded by the maximum of (4.10) for T as there, and this establishes our claim.

Now we turn to the proof of the upper bound on (weak) key-capacity for Model CW. This is more difficult than the proof of the similar bound for Model SW in Theorem 1 or for Model C in Proposition 1.

Consider any permissible strategy, as described in Section II for Model C; in particular, $K = K(M_{\mathcal{X}}, \Psi^k)$, $L = L(M_{\mathcal{Y}}, Y^n, \Phi^k)$. Since (4.9) holds also in the present case, and by the last functional relationships

$$I(K \wedge L \mid \Phi^k, \Psi^k, Z^n) \le I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}, Y^n \mid \Phi^k, \Psi^k, Z^n), \tag{4.12}$$

it suffices to bound the right-hand side of (4.12). We proceed as follows:

$$I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}, Y^n \mid \Phi^k, \Psi^k, Z^n) = I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}} Y^n Z^n \Phi^k \Psi^k) - I(M_{\mathcal{X}} \wedge Z^n \Phi^k \Psi^k). \tag{4.13}$$

Here, by the chain rule,

$$I(M_{\mathcal{Y}} \wedge M_{\mathcal{Y}} Y^n Z^n \Phi^k \Psi^k) = I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}} \Phi^{i_1 - 1} \Psi^{i_1 - 1}) + \sum_{j=1}^{n} (F_j + G_j), \tag{4.14}$$

where

$$F_j = I(M_{\mathcal{X}} \wedge Y_j Z_j \mid M_{\mathcal{Y}} Y^{j-1} Z^{j-1} \Phi^{i_j - 1} \Psi^{i_j - 1}), \tag{4.15}$$

$$G_j = I(M_{\mathcal{X}} \wedge \Phi_{i_j + 1} \cdots \Phi_{i_{j+1} - 1} \Psi_{i_j + 1} \cdots \Psi_{i_{j+1} - 1} \mid M_{\mathcal{Y}} Y^j Z^j \Phi^{i_j - 1} \Psi^{i_j - 1}) \tag{4.16}$$

(recall the convention $i_{n+1} = k + 1$).

Similarly,

$$I(M_{\mathcal{X}} \wedge Z^n \Phi^k \Psi^k) = I(M_{\mathcal{X}} \wedge \Phi^{i_1 - 1} \Psi^{i_1 - 1}) + \sum_{j=1}^{n} (F'_j + G'_j) \tag{4.17}$$

with

$$F'_j = I(M_{\mathcal{X}} \wedge Z_j \mid Z^{j-1} \Phi^{i_j - 1} \Psi^{i_j - 1}) \tag{4.18}$$

$$G'_j = I(M_{\mathcal{X}} \wedge \Phi_{i_j + 1} \cdots \Phi_{i_{j+1} - 1} \cdot \Psi_{i_j + 1} \cdots \Psi_{i_{j+1} - 1} \mid Z^j \Phi^{i_j - 1} \Psi^{i_j - 1}). \tag{4.19}$$

Substituting (4.14) and (4.17) into (4.13) gives

$$I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}, Y^n \mid \Phi^k, \Psi^k, Z^n) = I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}} \mid \Phi^{i_1 - 1} \Psi^{i_1 - 1}) + \sum_{j=1}^{n} (F_j + G_j - F'_j - G'_j). \tag{4.20}$$

From (4.15) and (4.18),

$$\begin{aligned} F_j - F_j' = {} & H(Y_jZ_j \mid M_{\mathcal{Y}}Y^{j-1}Z^{j-1}\Phi^{i_j-1}\Psi^{i_j-1}) \\ & - H(Y_jZ_j \mid M_{\mathcal{X}}M_{\mathcal{Y}}Y^{j-1}Z^{j-1}\Phi^{i_j-1}\Psi^{i_j-1}) \\ & - H(Z_j \mid Z^{j-1}\Phi^{i_j-1}\Psi^{i_j-1}) \\ & + H(Z_j \mid M_{\mathcal{X}}Z^{j-1}\Phi^{i_j-1}\Psi^{i_j-1}). \end{aligned} \tag{4.21}$$

It follows from (3.1) that the conditional joint distribution of Y_jZ_j on either of the conditions in the second and fourth terms of (4.21) is the same as on the condition $X_j = X_j(M_{\mathcal{X}}, \Psi^{i_j-1})$. Hence, the second and fourth terms of (4.21) equal $H(Y_jZ_j \mid X_j)$ and $H(Z_j \mid X_j)$, respectively. Substituting these, and upper bounding the first term by dropping $M_{\mathcal{Y}}Y^{j-1}$ from the condition, (4.21) gives

$$\begin{aligned} F_j - F_j' &\le H(Y_j \mid Z_jZ^{j-1}\Phi^{i_j-1}\Psi^{i_j-1}) - H(Y_j \mid X_jZ_j) \\ &\le H(Y_j \mid Z_j) - H(Y_j \mid X_jZ_j) = I(X_j \wedge Y_j \mid Z_j). \end{aligned} \tag{4.22}$$

Next, we compare the terms G_j and G_j'. (4.16) can be equivalently written as

$$\begin{aligned} G_j = {} & I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}Y^j\Phi_{i_j+1}\cdots\Phi_{i_{j+1}-1} \\ & \cdot \Psi_{i_j+1}\cdots\Psi_{i_{j+1}-1} \mid Z^j\Phi^{i_j-1}\Psi^{i_j-1}) \\ & - I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}Y^j \mid Z^j\Phi^{i_j-1}\Psi^{i_j-1}). \end{aligned}$$

This and (4.19) give

$$\begin{aligned} G_j - G_j' = {} & I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}Y^j \mid Z^j\Phi^{i_{j+1}-1}\Psi^{i_{j+1}-1}) \\ & - I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}Y^j \mid Z^j\Phi^{i_j-1}\Psi^{i_j-1}). \end{aligned}$$

On account of Lemma 2.2 (conditional version), this shows that

$$G_j - G_j' \le 0. \tag{4.23}$$

By Lemma 2.2, we also have

$$I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}} \mid \Phi^{i_1-1}\Psi^{i_1-1}) \le I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}) = 0. \tag{4.24}$$

By (4.22)–(4.24) it follows from (4.20) that

$$I(M_{\mathcal{X}} \wedge M_{\mathcal{Y}}Y^n \mid \Phi^k\Psi^kZ^n) \le \sum_{i=1}^{n} I(X_i \wedge Y_i \mid Z_i).$$

Returning to (4.12) and (4.9), this completes the proof of our upper bound on (weak) key-capacity for Model CW. □

If $P_{YZ|X} = W$ implies X–o–Z–o–Y then our upper bound is 0, and hence automatically tight. Suppose next that $P_{YZ|X} = W$ implies X–o–Y–o–Z (which means that W is of form (3.6)). Then, the first assertion of Theorem 2 implies that $I(X \wedge Y \mid Z) = I(X \wedge Y) - I(X \wedge Z)$ is a forward-achievable key rate for every X, Y, Z with $P_{YZ|X} = W$ (actually, achievable without using the public channel at all). Hence, in this case, our upper bound on key-capacity is tight, and key-capacity can be attained without any use of the public channel. Finally, if $P_{YZ|X} = W$ implies Y–o–X–o–Z (which means that W is of form (3.3)), we refer to the observation preceding Theorem 1. Since the key-capacity for Model SW with generic variables satisfying Y–o–X–o–Z is $I(X \wedge Y \mid Z)$, and it can be attained with a single backward transmission (by the Corollary of Theorem 1), it follows that the maximum of $I(X \wedge Y \mid Z)$ subject to $P_{YZ|X} = W$ is an achievable key rate, with a single backward transmission. Hence, our upper bound to key-capacity is tight also in this case, and, in addition, key-capacity equals backward key-capacity.

Proof of Theorem 3: The formal meaning of the assumption that the Z-outputs are known at Terminal $\mathcal{X}$ is that in the definition of a permissible secret sharing strategy, the condition $\Phi_i = \Phi_i(M_{\mathcal{X}}, X^n, \Psi^{i-1})$ is replaced by $\Phi_i = \Phi_i(M_{\mathcal{X}}, X^n, Z^n, \Psi^{i-1})$ for the source-type model, resp. $\Phi_i = \Phi_i(M_{\mathcal{X}}, Z^{i_j}\Psi^{i-1})$ for the channel-type model, and that in the final step, cf. (2.1), K may depend also on Z^n. If the Z-outputs are known at Terminal $\mathcal{Y}$, it is the functions Ψ_i (and L in (2.1)) which are modified in a similar way. The proofs by which $I(X \wedge Y \mid Z)$ and the maximum of $I(X \wedge Y \mid Z)$ subject to $P_{YZ|X} = W$ were shown to be upper bounds to the (weak) key-capacity for Models SW and CW, respectively, apply also when the Z-outputs are known at Terminal $\mathcal{X}$ or at Terminal $\mathcal{Y}$. Hence, Theorem 3 will be proved if we show that in the latter cases our upper bounds are actually achievable key rates.

If the Z-outputs are known at Terminal $\mathcal{Y}$, the Y-outputs Y_i can be replaced by the pairs Y_iZ_i without changing the permissible strategies. These new Y-outputs trivially satisfy the Markov condition Y–o–YZ–o–Z, hence Theorems 1 and 2 imply that $I(X \wedge YZ \mid Z) = I(X \wedge Y \mid Z)$ is an achievable key rate for the source-type model and the corresponding maximum is achievable for the channel-type model.

If the Z-outputs are known at Terminal $\mathcal{X}$, for the source-type model we are in the same situation as above. For the channel-type model, we refer to the observation preceding Theorem 1. Letting Terminal $\mathcal{X}$ transmit an i.i.d. sequence, a source-type model is simulated, for which the assertion has already been proved. It follows that $I(X \wedge Y \mid Z)$ is an achievable key rate whenever $P_{YZ|X} = W$.

The proof is complete. □

V. Conclusion

We have considered various models of generating common randomness at two distant terminals $\mathcal{X}$ and $\mathcal{Y}$, with the additional requirement that a third party, the wiretapper $\mathcal{Z}$, be kept ignorant of the generated common randomness. Then the latter could be used as an encryption key to make communication between $\mathcal{X}$ and $\mathcal{Y}$ secure from $\mathcal{Z}$. For some models of generating this common randomness or key, we were able to determine the largest achievable key rate, called the key-capacity. For other models we gave bounds on the key-capacity.

The problems can be studied for all multiway channels and multiterminal sources. One can conceive even of situations with several wiretappers.

The mathematical tools used in this paper were those of multiuser information theory, in particular the single-letterization technique developed by Csiszár and Körner [4] for the wiretap channel and its generalization called broadcast channel with confident messages. Still, it should be emphasized that there is a conceptual difference between the wiretap channel problem of transmitting messages from $\mathcal{X}$ to $\mathcal{Y}$ without giving informa-

tion about them to $\mathcal{Z}$, and the problem of generating common randomness shared by $\mathcal{X}$ and $\mathcal{Y}$, secret from $\mathcal{Z}$. Notice that this common randomness need not be generated at $\mathcal{X}$ and communicated to $\mathcal{Y}$, it may as well be generated at $\mathcal{Y}$ and communicated to $\mathcal{X}$, or cooperatively generated by $\mathcal{X}$ and $\mathcal{Y}$.

Following the suggestion of a reviewer, we now summarize our main results and mention some of the open problems.

Our models were of two main types. In Model SW (source-type model with wiretapper), a discrete memoryless multiple source with generic variables X, Y, Z was given, and $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ "could see" the length-n outputs X^n, Y^n, Z^n, respectively. In Model CW (channel-type model with wiretapper), a discrete memoryless channel with one input and two outputs was given, $\mathcal{X}$ governed the input, and the outputs were seen by $\mathcal{Y}$ and $\mathcal{Z}$, respectively. Both models involved the availability of a noiseless public channel of unlimited capacity for communication between $\mathcal{X}$ and $\mathcal{Y}$. As to the permitted use of the public channel, we focused mainly on the extreme cases.

1) A single transmission from $\mathcal{X}$ to $\mathcal{Y}$ or from $\mathcal{Y}$ to $\mathcal{X}$; the corresponding key-capacities were called the forward key-capacity and the backward key-capacity, respectively.
2) As many exchanges between $\mathcal{X}$ and $\mathcal{Y}$ as desired; the term "key-capacity," without qualification, has been used to refer to this case of unlimited conversation.

For Model SW, we gave a single-letter characterization of forward key-capacity; by symmetry, this provided a characterization of backward key-capacity, too. The key-capacity with unlimited conversation could not be determined in general, but it was always upper bounded by $I(X \wedge Y \mid Z)$. If X, Y, Z formed a Markov chain in some order, that bound was tight, and key-capacity with unlimited, conversation was equal to the forward or backward key-capacity. In general, two-way communication over the public channel could increase the key-capacity above both forward and backward key-capacity, even if only one exchange of messages was permitted. In our example demonstrating this, the key-capacity for one exchange of messages was the same as for unlimited conversation. We do not expect this to be always so, but our results do not rule out that contingency.

For Model CW, it may be possible for $\mathcal{X}$ and $\mathcal{Y}$ to share common randomness secret from $\mathcal{Z}$ without using the public channel; this is the wiretap channel situation when our key-capacity reduces to the wiretap channel secrecy capacity. Using the public channel from $\mathcal{X}$ to $\mathcal{Y}$ does not help: we have shown that the forward key-capacity for Model CW equals the wiretap channel secrecy capacity, determined in [4]. A single-letter characterization of backward key-capacity, as well as of key-capacity with unlimited conversation, remains elusive for Model CW. Still, the maximum of $I(X \wedge Y \mid Z)$—where (Y, Z) is the pair of outputs for input X—was shown to be an upper bound to key-capacity with unlimited conversation. This bound is tight in two important special cases, viz. for channels of form (3.6) or (3.3), and in those cases key-capacity with unlimited conversation equals the forward or backward key-capacity, respectively. In the cases, we could determine key-capacity with unlimited conversation for Model CW, it could be achieved with $\mathcal{X}$ producing i.i.d. channel inputs. It remains open whether this is true in general.

Finally, if the information available to $\mathcal{Z}$ was made available to $\mathcal{X}$ and/or $\mathcal{Y}$, the key-capacity with unlimited conversation for this modified model (of either type) was shown to always equal the upper bound obtained before, and also to equal the forward or backward key-capacity for the modified model. This appears to be the first coding theorem that provides a direct operational characterization of conditional mutual information.

APPENDIX

Lemma A: Given $U \multimap X \multimap YZ$ with

$$I(X \wedge Y \mid U) - I(X \wedge Z \mid U) = H > 0,$$

and arbitrarily small $\eta > 0$, $\epsilon > 0$, $\tau > 0$, for sufficiently large n every set $A \subset \mathcal{X}^n$ with $P_X^n(A) \geq \eta$ contains a subset $\tilde{A}$ with the following properties.

1) $\tilde{A}$ consists of sequences of the same type, and it is codeword set of an (n, ϵ)-code for the DMC $\{V\}$, where V represents the conditional distribution $P_{Y|X}$.
2) $\tilde{A}$ is the union of $M = \lceil \exp\{n(H - \epsilon)\} \rceil$ mutually disjoint sets $\tilde{A}^{(m)}$ of size $\mid \tilde{A}^{(m)} \mid = \lceil \exp\{n(I(X \wedge Z \mid U) - \epsilon)\} \rceil$, $m = 1, \cdots, M$.
3) If $\hat{X}^n$ denotes a random variable uniformly distributed on $\tilde{A}$ and $\hat{Z}^n$ denotes the corresponding output of the DMC $\{W\}$, where W represents the conditional distribution $P_{Z|X}$, then for $\hat{K}$ defined by

$$\hat{K} = m \text{ if } \hat{X}^n \in \tilde{A}^{(m)}, \qquad 1 \leq m \leq M,$$

we have

$$I(\hat{K} \wedge \hat{Z}^n) < \tau n.$$

Proof: We will use Lemma 3.3.17 of [5], which is a basic result for multiuser information theory, and has a simple and intuitive proof. This Lemma says that if $A \subset \mathcal{X}^n$ satisfies

$$P_{X|U}^n(A \mid \boldsymbol{u}) > \eta, \qquad \text{for some } U - \text{typical } \boldsymbol{u}, \qquad \text{(A.1)}$$

then A contains a subset $\tilde{A}$ with the properties 1), 2), and and the following.

3′) $\tilde{A}^{(m)}$ is the codeword set of an (n, ϵ)-code for the DMC $\{W\}$.

The standard properties of typical and generated sequences (cf. [5, section 1.2]) will be used freely, without reference.

Since

$$P_X^n(A) = \sum_{\boldsymbol{u}} P_U^n(\boldsymbol{u}) P_{X|U}^n(A \mid \boldsymbol{u}),$$

and the set of U-typical sequences $\boldsymbol{u}$ has P_U^n-probability arbitrarily close to 1 (if n is sufficiently large), it follows that any $A \subset \mathcal{X}^n$ with $P_X^n(A) \geq \eta$ satisfies (A.1), with $\eta/2$ in the role of η (say). Then the subset of A consisting of sequences $X \mid U$-generated by $\boldsymbol{u}$ will also satisfy (A.1), now with $\eta/4$, say. Thus it follows that any $A \subset \mathcal{X}^n$ with $P_X^n(A) \geq \eta$ contains a subset $\tilde{A}$ with the properties 1), 2), 3′) such that, in

addition, $\tilde{A}$ consists of sequences $X \mid U$-generated by some U-typical $\boldsymbol{u}$. It suffices to show that any such $\tilde{A}$ has property 3), at least if ϵ/τ is sufficiently small. This is implicit in Csiszár and Körner [4] but for completeness we give the proof.

Now, with the notation in 3),

$$I(\hat{K} \wedge \hat{Z}^n) = H(\hat{Z}^n) - H(\hat{Z}^n \mid \hat{K}) = H(\hat{Z}^n) - H(\hat{Z}^n \mid \hat{X}^n) - I(\hat{X}^n \wedge \hat{Z}^n \mid \hat{K}); \tag{A.2}$$

we bound these three terms separately.

Recalling that $\tilde{A}$ consists of sequences $X \mid U$-generated by a U-typical $\boldsymbol{u}$, let D denote the set of those $\boldsymbol{z} \in \mathcal{Z}^n$ which are $Z \mid U$-generated by $\boldsymbol{u}$. Then, D contains every $\boldsymbol{z} \in \mathcal{Z}^n$ which, for some $\boldsymbol{x} \in \tilde{A}$, is $Z \mid XU$-generated by $(\boldsymbol{x}, \boldsymbol{u})$ (providing the constants in the definition of generated sequences are suitably chosen). Thus, using also the Markov property U–o–X–o–Z,

$$W^n(D \mid \boldsymbol{x}) = P^n_{Z\mid X}(D \mid \boldsymbol{x}) = P^n_{Z\mid XU}(D \mid \boldsymbol{x}, \boldsymbol{u}) > 1 - \epsilon, \quad \text{if } \boldsymbol{x} \in \tilde{A} \tag{A.3}$$

(for n sufficiently large). Defining a random variable S by letting $S = 1$ if $\hat{Z}^n \in D$ and $S = 0$ otherwise, we obtain

$$H(\hat{Z}^n) = H(S, \hat{Z}^n) = H(S) + H(\hat{Z}^n \mid S) \le 1 + \Pr\{S = 1\} \log \mid D \mid + \Pr\{S = 0\} \log \mid \mathcal{Z}^n \mid \le 1 + n(H(Z \mid U) + \epsilon) + \epsilon n \log \mid \mathcal{Z} \mid; \tag{A.4}$$

here the last inequality follows (for sufficiently large n) by the standard bound on the number of sequences $Z \mid U$-generated by a given U-typical $\boldsymbol{u}$, and by (A.3).

Further, for every $\boldsymbol{x} \in \tilde{A}$,

$$H(\hat{Z}^n \mid \hat{X}^n = \boldsymbol{x}) = n \sum_{x \in \mathcal{X}} P(x) H(W(\cdot \mid x)), \tag{A.5}$$

where P denotes the common type of the sequences $\boldsymbol{x} \in \tilde{A}$. Since $\tilde{A}$ consists of sequences $X \mid U$-generated by a U-typical $\boldsymbol{u}$, this P is arbitrarily close to P_X if n is sufficiently large, thus (A.5) gives

$$H(\hat{Z}^n \mid \hat{X}^n) \ge n(H(Z \mid X) + \epsilon). \tag{A.6}$$

Finally, since the sets $\tilde{A}^{(m)}$ are codeword sets of (n, ϵ)-codes for the DMC $\{W\}$, there exist (decoding) functions $g^{(m)} : \mathcal{Z}^n \to \tilde{A}^{(m)}$ such that $\Pr\{g^{(m)}(\hat{Z}^n) \neq \hat{X}^n \mid \hat{K} = m\} < \epsilon$, $1 \le m \le M$. Hence,

$$I(\hat{X}^n \wedge \hat{Z}^n \mid \hat{K} = m) \ge I(\hat{X}^n \wedge g^{(m)}(\hat{Z}^n) \mid \hat{K} = m) \ge H(\hat{X}^n \mid \hat{K} = m) - \epsilon \log \mid \tilde{A}^{(m)} \mid -1 = (1 - \epsilon) \log \mid \tilde{A}^{(m)} \mid -1,$$

where the second step is by Fano's inequality. Substituting the value of $\mid \tilde{A}^m \mid$ from property 2), it follows that

$$I(\hat{X}^n \wedge \hat{Z}^n \mid \hat{K}) \ge (1 - \epsilon)n(I(X \wedge Z \mid U) - \epsilon) - 1. \tag{A.7}$$

Returning to (A.2), it follows from (A.4), (A.6), and (A.7) that property 3) holds, as claimed, providing ϵ/τ is sufficiently small.

References

[1] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrsch. Verw. Gebiete*, vol. 33, pp. 159–175, 1978.

[2] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Inform. Theory*, vol. 35, pp. 15–29, Jan. 1989.

[3] ——, "Identification in the presence of feedback—A discovery of new capacity formulas," *IEEE Trans. Inform. Theory*, vol. 35, pp. 30–39, Jan. 1989.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339–348, May 1978.

[5] ——, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1982.

[6] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inform. Theory*, vol. 34, pp. 181–193, Mar. 1988.

[7] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[8] V. M. Maurer, "Provably secure key distribution based on independent channels," presented at the *IEEE Workshop Inform. Theory*, Eindhoven, The Netherlands, June 1990.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, 1978.

[10] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, 1355–1387, 1975.

[11] U. M. Maurer, "Perfect cryptographic security from partially independent channels," *Proc. 23rd ACM Symp. Theory Computing*, New Orleans, LA, 1991, pp. 561–572.

[12] ——, "Secret key agreement by public discussion based on common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.