Appeared in *IEEE Transactions on Information Theory*, Vol. 39, pp. 733-742, 1993.

Secret Key Agreement by Public Discussion From Common Information [1]

Ueli M. Maurer [2], *Member, IEEE*

Abstract. The problem of generating a shared secret key S by two parties knowing dependent random variables X and Y, respectively, but not sharing a secret key initially, is considered. An enemy who knows the random variable Z, jointly distributed with X and Y according to some probability distribution P_{XYZ}, can also receive all messages exchanged by the two parties over a public channel. The goal of a protocol is that the enemy obtains at most a negligible amount of information about S. Upper bounds on $H(S)$ as a function of P_{XYZ} are presented. Lower bounds on the rate $H(S)/N$ (as $N \to \infty$) are derived for the case where $X = [X_1, \ldots, X_N]$, $Y = [Y_1, \ldots, Y_N]$ and $Z = [Z_1, \ldots, Z_N]$ result from N independent executions of a random experiment generating X_i, Y_i and Z_i, for $i = 1, \ldots, N$. In particular it is shown that such secret key agreement is possible for a scenario where all three parties receive the output of a binary symmetric source over independent binary symmetric channels, even when the enemy's channel is superior to the other two channels. The results of this paper suggest to build cryptographic systems that are provably secure against enemies with unlimited computing power under realistic assumptions about the partial independence of the noise on the involved communication channels.

Index Terms. Secret key agreement, public discussion protocols, provable security, broadcast channel, secrecy capacity, wire-tap channel, privacy amplification.

I. Introduction

One of the fundamental problems in cryptography is the transmission of a message M from a sender (referred to as Alice) to a receiver (Bob) over an insecure communication channel such that an enemy (Eve) with access to this channel is unable to obtain useful information about M.

In the classical model of a cryptosystem (or cipher) introduced by Shannon [13], Eve has perfect access to the insecure channel; thus she is assumed to receive an identical copy of the ciphertext C received by the legitimate receiver Bob, where C is obtained by Alice as a function of the plaintext message M and a secret key K shared by Alice and Bob. Shannon defined a cipher system to be perfect if

$$I(M;C) = 0, \tag{1}$$

[1]The results of this paper were presented in part at the 1990 IEEE International Workshop on Information Theory, Eindhoven, The Netherlands, June 10-15, 1990. Some results were also presented at the 23rd ACM Symposium on Theory of Computing, New Orleans, May 6-8, 1991.

[2]The author is with the Department of Computer Science, Swiss Federal Institute of Technology, ETH-Zentrum, CH-8092 Zurich, Switzerland

i.e., if the ciphertext gives no information about the plaintext or, equivalently, if M and C are statistically independent. When a perfect cipher is used to encipher a message M, an enemy can do no better than guess M without even looking at the ciphertext C.

Shannon gave as a simple example of a perfect cipher the so-called one-time pad previously proposed by Vernam [14] without proof of security; the binary plaintext is concealed by adding modulo 2 (EXOR) a random binary secret key of the same length. Of course, this system is completely impractical for most applications where only a short secret key is available. Shannon proved the pessimistic result that perfect secrecy can be achieved only when the secret key is at least as long as the plaintext message or, more precisely, when

$$H(K) \;\geq\; H(M). \tag{2}$$

Almost all presently-used ciphers, including public-key cryptosystems, are based on the assumption of Shannon's model that an enemy receives precisely the same information (the ciphertext) as the legitimate receiver. Since the secret key is short for these ciphers, they can theoretically be broken, for instance by an exhaustive key search. The goal of designing such a practical cipher is hence to guarantee that there exists no efficient algorithm for breaking it, for a reasonable definition of breaking. However, for no existing cipher can the computational security be proved (without invoking an unproven intractability hypothesis). For instance the security of the well-known RSA public-key cryptosystem [11] is based on the (unproven) difficulty of factoring large integers, and many other cryptographic systems and protocols are based on the similarly unproven difficulty of computing discrete logarithms in certain groups (e.g., see [6]).

Information-theoretic or unconditional security is more desirable in cryptography than computational security for two reasons. First, for the former no assumption about the enemy's computing power is needed, and second, perfect secrecy is unarguably the strongest definition of security and hence the justification of a weaker definition of security (for instance that an enemy cannot guess any plaintext bit with probability of success greater than a specified bound) is avoided.

Perfect secrecy is often prejudged as being impractical because of Shannon's pessimistic inequality (2). It is one of the goals of this paper to relativize this pessimism by pointing out that Shannon's apparently innocent assumption that, except for the secret key, the enemy has access to precisely the same information as the legitimate receiver, is much more restrictive than has generally been realized.

The key to perfect secrecy without a secret key K satisfying (2) is to modify Shannon's model such that the enemy cannot receive precisely the same information as the legitimate receiver. Several previous approaches based on this idea are briefly discussed in the following. All these approaches are either impractical or based on unrealistic assumptions about an enemy's accessible information.

Quantum cryptography introduced by Wiesner and put forward by Bennett, Brassard *et al.* [1, 4], which is for several reasons not truly practical (even though a prototype exists) is based on the (unproven but plausible) uncertainty principle of quantum physics: By measuring one component of the polarization of a photon Eve irreversibly loses the ability to perform a measurement for the orthogonal component of the polarization.

The randomized cipher introduced by Maurer [8] makes use of a public random string that is too long to be read entirely in feasible time. This cipher is impractical because a source of the required large amount of randomness remains to be discovered.

Both these systems allow two parties initially sharing a short secret key to generate a much longer and unconditionally secure shared secret key. In quantum cryptography, the secret key is required for authentication (like in a realistic implementation of our protocols) and in the randomized cipher it is used to select a feasible number of the public random bits for generating the keystream.

Wyner [16] and subsequently Csiszár and Körner [5] considered a scenario in which the enemy Eve is assumed to receive messages transmitted by the sender Alice over a channel that is noisier than the legitimate receiver Bob's channel. The assumption that Eve's channel is worse than the main channel is unrealistic in general. It will be shown in the following section that this unrealistic assumption is unnecessary if Alice and Bob can also communicate over a completely insecure public channel. This broadcast channel scenario is generalized in Section 3 to a scenario where Alice, Bob and Eve know random variables X, Y and Z, respectively, jointly distributed according to some probability distribution P_{XYZ}, and where Alice and Bob can also communicate over a public channel.

Note that the need for a public channel entails no significant loss of practicality in a cryptographic context because the channel need not provide secrecy. It is assumed, however, that all messages sent over the public channel can be received by Eve without error, but that she cannot modify messages or introduce fraudulent messages without being detected. If this last assumption cannot realistically be made, authenticity and data integrity can be ensured by using an unconditionally secure authentication scheme, for instance that of [15] based on universal hashing, which requires that Alice and Bob share a short secret key initially. As for the protocols discussed in Bennett's and Brassard's work on quantum cryptography [1], the purpose of our protocols is in this case to stretch (rather than to generate) a secret key unconditionally securely. Part of the generated key can be used for authentication in a subsequent instance of the protocol.

The use of a public channel by two parties for extracting a secret key from an initially shared partially secret string was previously considered by Leung-Yan-Cheong [7] and independently by Bennett, Brassard and Robert [2].

This paper is concerned with key distribution as well as encryption: a shared secret key generated by one of our protocols can be used as the key sequence in the above mentioned one-time pad, thus achieving (virtually) perfect secrecy of the transmitted messages.

The outline of the paper is as follows. Known results on the secrecy capacity of broadcast channels are reviewed in Section 2, and the secrecy capacity with public discussion is introduced informally. In Section 3, the general problem of key agreement from common information by public discussion is introduced, and upper bounds on the achievable amount of shared secret key are stated. The case of X, Y and Z being generated by a sequence of independent executions of a random experiment is considered as a special case in Section 4, and lower and upper bounds on the achievable rate at which Alice and Bob can agree on a secret key are derived. Furthermore, the secrecy capacity with public discussion of broadcast channels is discussed. In Section 5 it is demonstrated that the secret key rate is positive even for cases where intuition suggests that it vanishes, demonstrating the possibility for practical perfect secrecy under realistic assumptions. One such case is a satellite broadcasting random bits such that Alice, Bob and Eve can receive these bits over independent binary symmetric channels with error probabilities ϵ_A, ϵ_B and ϵ_E, respectively, where both $\epsilon_E < \epsilon_A$ and $\epsilon_E < \epsilon_B$. The condition that the channels be independent is shown to be unnecessary.

II. Secret Communication Using Broadcast Channels

Shannon's assumption that an enemy receives precisely the same message as the legitimate receiver is motivated by considering error-free communication channels. However, most real communication channels are noisy, and it is only for applications that such noisy channels are converted into virtually error-free channels (with reduced information rate) by the use of error-correcting codes. This apparently trivial observation suggests that Shannon's assumption is unnecessarily restrictive if the underlying noisy channels are accessible for a cryptographic application.

Motivated by such considerations, Wyner [16] considered a communications scenario in which Alice can send information to Bob over a discrete memoryless channel such that a wire-tapper Eve can receive Bob's channel output only through an additional cascaded independent channel reducing the capacity of Eve's channel. Wyner proved that in such a (generally unrealistic) setting Alice can send information to Bob in virtually perfect secrecy without sharing a secret key with Bob initially.

Wyner's model and results were generalized by Csiszár and Körner [5] who considered a discrete memoryless broadcast channel for which the wire-tapper Eve's received message is not necessarily a degraded version of the legitimate receiver's message. The common input to the main channel and Eve's channel is the random variable X chosen by Alice according to some probability distribution P_X, and the random variables received by the legitimate receiver Bob and by the enemy Eve are Y and Z, respectively. X, Y and Z take on values in some finite or countably infinite alphabets $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$, respectively. The channel behavior is completely specified by the conditional probability distribution $P_{YZ|X}$. Note that in Wyner's original setting [16], X, Y and Z form a Markov chain, i.e., $P_{Z|XY} = P_{Z|Y}$, which implies $I(X;Z|Y) = 0$.

The secrecy capacity $C_s(P_{YZ|X})$ of the described broadcast channel with transition probability distribution $P_{YZ|X}$ was defined in [5] as the maximum rate at which Alice can reliably send information to Bob such that the rate at which Eve obtains this information is arbitrarily small. In other words, the secrecy capacity is the maximal number of bits per use of the channel that Alice can send to Bob in secrecy. A formal definition is given below.

Definition 1. The *secrecy capacity* of a broadcast channel specified by $P_{YZ|X}$ is the maximal rate R for which for every $\gamma > 0$, for all sufficiently large N, there exists a (possibly probabilistic) encoding function $e : \{0,1\}^K \rightarrow \mathcal{X}^N$, where $K = \lfloor RN \rfloor$, together with a corresponding decoding function $d: \mathcal{Y}^N \rightarrow \{0,1\}^K$ such that for V is uniformly distributed over $\{0,1\}^K$ the following two conditions are satisfied:

(1) $P[d(Y) \neq V] < \gamma$, where $X = e(V)$ and $P_{Y|X}$ is the marginal distribution of $P_{YZ|X}$.

(2) $H(V|Z^N)/K > 1 - \gamma$.

It would be equivalent to require the two conditions to hold for all probability distributions

P_V. Note that a deterministic encoding function corresponds to a binary code of length N with 2^K codewords.

Csiszár and Körner [5] proved that

$$\begin{aligned} C_s(P_{YZ|X}) &= \max_{P_{UX}}[I(U;Y) - I(U;Z)] \\ &\geq \max_{P_X}[I(X;Y) - I(X;Z)] \\ &= \max_{P_X}[H(X|Z) - H(X|Y)] \end{aligned} \tag{3}$$

where the first maximization is over probability distributions P_{UX} with U taking on values in an arbitrary set $\mathcal{U}$ and where $P_{UXYZ} = P_{UX} \cdot P_{YZ|X}$. The inequality follows from the fact that $U = X$ is a legitimate choice. One condition for equality in (3) is that $I(X;Y) \geq I(X;Z)$ for all choices of P_X, but equality actually holds for most probability distributions $P_{YZ|X}$ that are of interest. In this case, the secrecy capacity is zero unless $I(X;Y) > I(X;Z)$ for some P_X.

In order to demonstrate that feedback from Bob to Alice over an insecure public channel can increase the secrecy capacity of a broadcast channel, we consider a broadcast channel for which the main channel and Eve's channel are independent binary symmetric channels with bit error probabilities ϵ and δ, respectively, i.e., X, Y and Z are binary random variables and $P_{YZ|X} = P_{Y|X} \cdot P_{Z|X}$ where $P_{Y|X}(y|x) = 1 - \epsilon$ if $x = y$, $P_{Y|X}(y|x) = \epsilon$ if $x \neq y$, $P_{Z|X}(z|x) = 1 - \delta$ if $x = z$, and $P_{Z|X}(z|x) = \delta$ if $x \neq z$. Without loss of generality we may assume that $\epsilon \leq 1/2$ and $\delta \leq 1/2$. For ease of notation, we will refer to the described probability distribution $P_{YZ|X}$ as $D(\epsilon, \delta)$. Let h denote the binary entropy function defined by $h(p) = -p \log_2 p - (1-p)\log_2(1-p)$.

Lemma 1. *The secrecy capacity of the described binary broadcast channel is given by*

$$C_s(D(\epsilon,\delta)) = \begin{cases} h(\delta) - h(\epsilon) & \textit{if } \delta > \epsilon, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let $P_X(0) = p$. We have $H(X|Y) = H(X) - H(Y) + H(Y|X)$, $H(X) = h(p)$, $H(Y|X) = h(\epsilon)$ because $H(Y|X = x) = h(\epsilon)$ independent of x, and $H(Y) = h(p + \epsilon - 2p\epsilon)$ since $P(Y = 0) = p(1-\epsilon) + (1-p)\epsilon = p + \epsilon - 2p\epsilon$. Thus $H(X|Y) = h(p) + h(\epsilon) - h(p + \epsilon - 2p\epsilon)$ and similarly one obtains that $H(X|Z) = h(p) + h(\delta) - h(p + \delta - 2p\delta)$. It is easy to verify that the stated condition for equality in (3) is satisfied. For every $p < 1/2$, $p + \xi - 2p\xi$ and hence $h(p + \xi - 2p\xi)$ are monotonically increasing functions for $0 \leq \xi < 1/2$. Thus $H(X|Z) - H(X|Y) = h(\delta) - h(\epsilon) + h(p + \epsilon - 2p\epsilon) - h(p + \delta - 2p\delta)$ is maximized for $p = 1/2$, in which case the last two terms vanish. This completes the proof of the lemma. □

It should be pointed out that the proofs for (3) given in [5] and [16] are non-constructive existence proofs based on a random-coding argument. The problem of finding actual efficiently encodable and decodable codes that perform well in a particular situation will be the subject of a forthcoming paper.

According to Lemma 1, the secrecy capacity vanishes when $\delta \leq \epsilon$. We now show that by allowing *feedback* from Bob to Alice over an insecure public channel (which is assumed without loss of generality to be error-free), messages can be exchanged in perfect secrecy between Alice and Bob, even when $\delta < \epsilon$, provided they know an upper bound on δ.

In analogy to the secrecy capacity of a broadcast channel specified by $P_{YZ|X}$ one can define the secrecy capacity with public discussion, denoted as $\hat{C}_s(P_{YZ|X})$, as the maximal rate (in bits per use of the $X \to YZ$ channel) at which Alice and Bob can agree on a secret key by exchanging arbitrary messages over an insecure public channel, such that the rate at which Eve obtains information about the secret key by observing the public messages and the Z-outputs of the channel is arbitrarily small. We refer to Section 4 for a formal definition.

Proposition 2. *The secrecy capacity with public discussion of the described binary broadcast channel is given by*

$$\hat{C}_s(D(\epsilon,\delta)) \;=\; h(\epsilon+\delta-2\epsilon\delta) - h(\epsilon).$$

Moreover, $\hat{C}_s(D(\epsilon,\delta))$ *is strictly positive unless* $\epsilon = 0.5$*,* $\delta = 0$ *or* $\delta = 1$*, i.e., unless* X *and* Y *are statistically independent or* Z *uniquely determines* X*.*

Proof. In order to prove that the stated secrecy capacity can be achieved we demonstrate that Bob can create a conceptual broadcast channel from Bob to Alice and Eve such that the conceptual main channel (to Alice) is equivalent to the real main channel from Alice to Bob but Eve's conceptual channel is equivalent to a cascade of the real main channel and Eve's real channel.

Alice sends a random bit X over the (real) broadcast channel, i.e., $P_X(0) = P_X(1) = 0.5$. Let E and D denote the (independent) error bits of the main and of Eve's channel, respectively, i.e., let $Y = X + E$ and $Z = X + D$ where $P(E=1) = \epsilon$ and $P(D=1) = \delta$. In order to send a bit V over the described conceptual broadcast channel, Bob sends $W = Y + V$ over the public channel. Alice computes $W + X = V + E$ and thus "receives" V with error probability ϵ. Eve on the other hand knows $Z = X + D$ and $W = X + E + V$ and can compute $Z + W = V + E + D$, which is equivalent to receiving V over a cascade of the actual main channel and Eve's actual channel.

In order to prove that without loss of optimality Eve can compute $Z + W$ and discard Z and W we show that this step entails no loss of information about V for Eve.

$$\begin{aligned}
H(V|ZW) &= H(V|Z+W, W)\\
&= H(VW|Z+W) - H(W|Z+W)\\
&= H(V|Z+W) + H(W|V, Z+W) - H(W|Z+W).
\end{aligned}$$

The first step follows from the fact that the pair (Z, W) uniquely determines the pair $(Z + W, W)$ and vice versa. The result now follows upon noting that $H(W|V, Z+W) = H(X + V + D|V, V + E + D) = 1$ and thus also $H(W|Z+W) = 1$ since X is completely random and statistically independent of V, E and D.

The bit error probabilities of the conceptual main channel and Eve's conceptual channel are ϵ and $\epsilon+\delta-2\epsilon\delta$, respectively. Because one way for Alice and Bob to generate a shared secret key is to let Bob use the described conceptual channel to transmit a secret key to Alice, $C_s(D(\epsilon, \epsilon+\delta-2\epsilon\delta)) = h(\epsilon+\delta-2\epsilon\delta) - h(\epsilon)$ is a lower bound on $\hat{C}_s(D(\epsilon,\delta))$. In order to prove that the lower bound cannot be exceeded we make use of Theorem 7 stated in Section 4. We have $I(X;Y|Z) = H(Y|Z) - H(Y|XZ) = H(Y|Z) - H(Y|X)$, where $H(Y|XZ) = H(Y|X)$ follows from the independence of the channels. It is straightforward to verify that $H(Y|Z) - H(Y|X)$ is maximized for the choice $P_X(0) = P_X(1) = 1/2$ for which it takes on the value $h(\epsilon+\delta-2\epsilon\delta) - h(\epsilon)$.

To prove the last claim, note that $h(x)$ is a monotonically increasing function for $0 \leq x < 1/2$, and that $h(\epsilon+\delta-2\epsilon\delta) \geq h(\epsilon)$ with equality if and only if either $\delta=0$, $\delta=1$ or $\epsilon=1/2$. $\square$

III. Secret Key Agreement by Public Discussion: Upper Bounds

Consider the following general key agreement problem. Assume that Alice, Bob and Eve know random variables X, Y and Z, respectively, with joint probability distribution P_{XYZ}, and that Eve has no information about X and Y other than through her knowledge of Z. More precisely, $I(XY;T|Z)=0$ where T summarizes Eve's complete information about the universe. In this paper, X, Y and Z take on values in some finite alphabets $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$, respectively. Alice and Bob share no secret key initially (other than possibly a short key required for guaranteeing authenticity and integrity of messages sent over the public channel), but are assumed to know P_{XYZ} or at least an upper bound on the quality of Eve's channel. In particular, the protocol and the codes used by Alice and Bob are known to Eve. Every message communicated between Alice and Bob can be intercepted by Eve, but it is assumed that Eve cannot insert fraudulent messages nor modify messages on this public channel without being detected.

As mentioned before, attacks by Eve other than passive wire-tapping can be detected when an unconditionally secure authentication scheme with a short initially shared secret key is used. If only a computationally secure authentication scheme were used, the unconditional security would only be retained against passive, but not against active wire-tapping.

A broadcast channel as described in the previous section is one of several possible realizations for the distribution of random variables X, Y and Z. An alternative for Alice and Bob to acquire random variables X and Y is to receive the signal of a satellite broadcasting random bits at a very low signal power (so that even if Eve uses a much better receiving antenna she cannot avoid at least a small bit error probability), or of a deep space radio source.

Alice and Bob use a protocol in which at each step either Alice sends a message to Bob depending on X and all the messages previously received from Bob, or vice versa (with X replaced by Y). Without loss of generality, we consider only protocols in which Alice sends messages at odd steps $(C_1, C_3, \ldots)$ and Bob sends messages at even steps $(C_2, C_4, \ldots)$. Moreover, we can restrict the analysis to deterministic protocols since a possible randomizer which Alice's and/or Bob's strategy and messages might depend on can be considered as part of X and Y, respectively. In other words, Alice and Bob can without loss of generality extend their known random variables X and Y, respectively, by random bits that are statistically independent of X, Y and Z. At the end of the t-step protocol, Alice computes a key S as a function of X and $C^t \stackrel{\triangle}{=} [C_1, \ldots, C_t]$ and Bob computes a key S' as a function of Y and C^t. Their goal is to maximize $H(S)$ under the conditions that S and S' agree with very high probability and that Eve has very little information about either S or S'. More formally,

$$H(C_i|C^{i-1}X)=0 \tag{4}$$

for odd i,

$$H(C_i|C^{i-1}Y)=0 \tag{5}$$

for even i,

$$H(S|C^tX) = 0 \tag{6}$$

and

$$H(S'|C^tY) = 0, \tag{7}$$

and it is required that

$$P[S \neq S'] \leq \epsilon \tag{8}$$

and

$$I(S;C^tZ) \leq \delta \tag{9}$$

for some specified (small) δ and ϵ. (These two parameters should not be confused with the bit error probabilities of the previous section.)

By Fano's Lemma (cf. [3], p. 156) condition (8) implies that

$$H(S|S') \leq h(\epsilon) + \epsilon \log_2(|\mathcal{S}| - 1) \tag{10}$$

where $|\mathcal{S}|$ denotes the number of distinct values that S takes on with non-zero probability. Note that $H(S|S') \to 0$ as $\epsilon \to 0$.

If one requires that $P[S \neq S'] = 0$ and $I(S;C^t) = 0$ (i.e., that $\epsilon = 0$ in (8) and $\delta = 0$ in (9)) it appears intuitive but not obvious that $I(X;Y)$ is an upper bound on $H(S)$. It appears to be similarly intuitive that $H(S) \leq I(X;Y|Z) = I(XZ;YZ) - H(Z)$ because even under the assumption that Alice and Bob could learn Z, the remaining information shared by Alice and Bob is an upper bound on the information they can share in secrecy. The following theorem, whose proof is not completely obvious, summarizes these results.

Theorem 3. *For every key agreement protocol satisfying (4)-(7),*

$$H(S) \;\leq\; I(X;Y|Z) + H(S|S') + I(S;C^tZ).$$

In particular,

$$H(S) \;\leq\; I(X;Y) + H(S|S') + I(S;C^t).$$

Proof. Note first of all that the second part is a special case of the first where Z is a constant random variable. It remains to prove the first part. We have

$$H(S) = I(S;C^tZ) + H(S|C^tZ) \tag{11}$$

where $H(S|C^tZ)$ can be upper bounded as follows:

$$\begin{aligned} H(S|C^tZ) &= H(SX|C^tZ) - H(X|C^tSZ) \\ &= H(X|C^tZ) + H(S|C^tXZ) - H(X|C^tSZ) \\ &\leq H(X|C^tZ) - H(X|C^tSYZ) \\ &= H(X|C^tZ) - H(XS|C^tYZ) + H(S|C^tYZ) \\ &= H(X|C^tZ) - H(X|C^tYZ) + H(S|C^tYZ) \\ &\leq I(X;Y|C^tZ) + H(S|S'). \end{aligned} \tag{12}$$

In the first inequality and in the second last step we have made use of (6) and the fact that conditioning on further random variables cannot increase entropy, and the second inequality follows from equation (7) which implies

$$H(S|C^tYZ) = H(S|C^tS'YZ) \leq H(S|S').$$

We continue the proof by showing that public discussion cannot increase the mutual information shared by Alice and Bob when given Eve's total information consisting of C^t and Z. Without loss of generality assume that t is odd, i.e., that the last public message C_t is sent by Alice and thus $H(C_t|C^{t-1}X) = 0$. The proof for even t is analogous.

$$\begin{aligned} I(X;Y|C^tZ) &= H(Y|C^tZ) - H(Y|C^tXZ) \\ &= H(Y|C^tZ) - H(Y|C^{t-1}XZ) \\ &\leq H(Y|C^{t-1}Z) - H(Y|C^{t-1}XZ) \\ &= I(X;Y|C^{t-1}Z). \end{aligned} \tag{13}$$

The second step follows from (4). By repeating this argument t times, but for even t with X and Y interchanged, we arrive at

$$I(X;Y|C^tZ) \ \leq \ I(X;Y|Z)$$

which together with (12) and (11) completes the proof of the theorem. □

Corollary 4. *For every key agreement protocol satisfying (4)-(9),*

$$H(S) \ \leq \ \min[I(X;Y), I(X;Y|Z)] + \delta + h(\epsilon) + \epsilon \log_2(|\mathcal{S}| - 1).$$

Proof. Immediate consequence of Theorem 3, inequality (10) and of $I(S;C^t) \leq I(S;C^tZ)$. □

It should be pointed out that $I(X;Y) < I(X;Y|Z)$ is possible. Consider as an example the case where X and Y are independent, binary and symmetrically distributed (i.e., $P[X = 0] = P[Y = 0] = 1/2$) and where Z is the modulo 2 sum of X and Y. Then $I(X;Y) = 0$ whereas $I(X;Y|Z) = H(X) = 1$. Furthermore, $I(X;Y) > I(X;Y|Z)$ is also possible, for instance when $I(X;Y) > 0$ and when $Z = X$.

IV. The Secret Key Rate: Upper and Lower Bounds

In order to be able to prove lower bounds on the achievable size of a key shared by Alice and Bob in secrecy we need to make more specific assumptions about the distribution P_{XYZ}. One natural assumption is that the random experiment generating XYZ is repeated many times independently: Alice, Bob and Eve receive $X^N = [X_1, \ldots, X_N]$, $Y^N = [Y_1, \ldots, Y_N]$ and $Z^N = [Z_1, \ldots, Z_N]$, respectively, where

$$P_{X^NY^NZ^N} \ = \ \prod_{i=1}^{N} P_{X_iY_iZ_i}$$

and where $P_{X_iY_iZ_i} = P_{XYZ}$ for $1 \leq i \leq N$.

For such a scenario of independent repetitions of a random experiment, which is well motivated by models such as discrete memoryless sources and channels previously considered in information theory, the quantity that appears to be of most interest is defined as follows.

Definition 2. The *secret key rate of X and Y with respect to Z*, denoted $S(X;Y||Z)$, is the maximum rate at which Alice and Bob can agree on a secret key S while keeping the rate at which Eve obtains information arbitrarily small, i.e., it is the maximal R such that for every $\epsilon > 0$ there exists a protocol for sufficiently large N satisfying (4)-(8) with X and Y replaced by X^N and Y^N, respectively, satisfying

$$\frac{1}{N} I(S; C^t Z^N) \ \leq \ \epsilon,$$

and achieving

$$\frac{1}{N} H(S) \ \geq \ R - \epsilon.$$

In all the protocols discussed below, S will be uniformly distributed. However, if for some other protocol the secret key generated by Alice and Bob were not uniformly distributed, an almost uniformly distributed key could be generated by applying the protocol a sufficient number of times and using an ideal data compression scheme. Hence the condition

$$\frac{1}{N} \log_2 |\mathcal{S}| \ < \ \frac{1}{N} H(S) + \epsilon$$

could be included in the above definition without loss of generality.

Before turning to the derivation of lower bounds on $S(X;Y||Z)$ we state the following theorem, which is an immediate consequence of Corollary 4.

Theorem 5. *The secret key rate of X and Y with respect to Z is upper bounded by*

$$S(X;Y||Z) \ \leq \ \min[I(X;Y),\ I(X;Y|Z)].$$

The following theorem states a nontrivial lower bound on the secret key rate. If it is either the case that Eve has less information about Y than Alice or, by symmetry, less information about X than Bob, then such a difference of information can be exploited.

Theorem 6. *The secret key rate of X and Y with respect to Z is lower bounded by*

$$S(X;Y||Z) \ \geq \ \max[I(Y;X) - I(Z;X),\ I(X;Y) - I(Z;Y)].$$

Proof. We only prove that $I(Y;X) - I(Z;X)$ is an achievable secret key rate; the proof for $I(X;Y) - I(Z;Y)$ follows by symmetry. Without loss of generality we assume that $\mathcal{X} = \{0, \ldots, L-1\}$ for some L and define addition on $\mathcal{X}$ to be modulo L. Alice can create a conceptual noisy broadcast channel for sending a random variable $V \in \mathcal{X}$ to Bob and Eve by sending $V + X$ over the public channel. Bob and Eve hence "receive" the pairs $[Y, V + X]$

and $[Z, V + X]$, respectively. Note that the first and second components of these pairs are the random variables received from the random experiment and from the public channel, respectively.

According to (3) the secrecy capacity of this conceptual broadcast channel is lower bounded by

$$C_s(P_{[Y,V+X],[Z,V+X]|V}) \;\geq\; \max_{P_V}[H(V|Z, V+X) - H(V|Y, V+X)]. \qquad (14)$$

Since Bob can use this conceptual channel for transmitting a message to Alice in secrecy at a rate arbitrarily close to the secrecy capacity, we have

$$S(X;Y||Z) \;\geq\; C_s(P_{[Y,V+X],[Z,V+X]|V}).$$

When P_V is the uniform distribution,

$$\begin{aligned} H(V|Y, V+X) &= H(V, V+X|Y) - H(V+X|Y) \\ &= H(V|Y) + H(V+X|VY) - H(V+X|Y) \\ &= H(V+X|VY) \\ &= H(X|Y). \end{aligned}$$

The third step follows from the fact that V is statistically independent of X and Y and hence $H(V|Y) = H(V + X|Y) = H(V) = \log_2 L$. Similarly, one obtains $H(V|Z, V+X) = H(X|Z)$. Thus the term to be maximized in (14) is equal to $H(X|Z) - H(X|Y) = I(Y;X) - I(Z;X)$. □

It will be shown by an example in Section 5 that the lower bound of Theorem 6 is not tight in general, i.e., there exist scenarios for which interaction between Alice and Bob (i.e., two-way communication) is necessary for achieving non-zero secrecy capacity. Theorem 6 demonstrates that the upper bound in Theorem 5 is tight if either $P_{YZ|X} = P_{Y|X} \cdot P_{Z|X}$ or $P_{XZ|Y} = P_{X|Y} \cdot P_{Z|Y}$.

The broadcast channel discussed in Section 2 can be considered as a generalization of the key agreement scenario described in this section. Alice can choose the channel input probability distribution P_X and hence choose the joint distribution P_{XYZ} subject to the constraint that $P_{YZ|X}$ equals the given conditional channel distribution. Note that the two above stated conditions for the upper bound to be tight in Theorem 5 correspond to the case of independent broadcast channels (cf. Section 2) and to Wyner's degraded wire-tap channel [16], respectively.

The *secrecy capacity with public discussion*, denoted $\hat{C}_s(P_{YZ|X})$, can be defined similarly to the secrecy rate of X and Y with respect to Z with the obvious modification that Alice is allowed to send the digits $X_1, \ldots, X_N$ at arbitrary steps of the protocol and to choose their probability distributions $P_{X_1}, \ldots, P_{X_N}$ adaptively, depending on the information available to her at the corresponding steps of the protocol. In slight deviation from the notation of Section 3 we will denote by $C_i = [C_{i1}, \ldots, C_{it_i}]$ the total sequence of t_i messages exchanged by Alice and Bob over the public channel after X_i has been sent by Alice over the broadcast channel. C^N (as opposed to C^t in Section 3) hence denotes the total conversation over the public channel.

One particular strategy is for Alice to choose $P_{X_1} = \cdots = P_{X_N} = P_X$ where P_X maximizes $S(X;Y||Z)$. Therefore

$$\begin{aligned} \hat{C}_s(P_{YZ|X}) &\geq \max_{P_X} S(X;Y||Z) \qquad (15) \\ &\geq \max[\max_{P_X}[I(Y;X) - I(Z;X)], \max_{P_X}[I(X;Y) - I(Z;Y)]]. \end{aligned}$$

It is an open problem whether equality holds in (15) in general. However, an upper bound similar to that of Theorem 5 for $S(X;Y||Z)$ can be proved for $\hat{C}_s(P_{YZ|X})$ and is summarized together with (15) in the following theorem stating that by adaptively choosing $P_{X_1}, \ldots, P_{X_N}$ Alice cannot increase the secrecy capacity. The proof of Theorem 7 is given in the Appendix. This result is in analogy to the well-known fact that feedback cannot increase the capacity of a discrete memoryless channel. Note, however, that as for the ordinary capacity, feedback may allow to increase the rate achievable in a practical implementation.

Theorem 7. *The secrecy capacity with public discussion of a broadcast channel specified by $P_{YZ|X}$ is bounded from below and from above by*

$$\max_{P_X} S(X;Y||Z) \;\leq\; \hat{C}_s(P_{YZ|X}) \;\leq\; \min[\max_{P_X} I(X;Y),\; \max_{P_X} I(X;Y|Z)].$$

V. Interaction is more Powerful than One-way Transmissions

It is demonstrated in this section that for certain probability distributions P_{XYZ} it is crucial for Alice and Bob to be able to use the public channel in both directions, possibly during several rounds.

Before presenting protocols for binary symmetric channels we first demonstrate by a simple example that it is theoretically possible for Alice and Bob to use public discussion for generating a secret key even if Eve's channel is less noisy. For simplicity, assume that the three channels are additive white Gaussian noise channels with statistically independent noise. Assume further that binary antipodal signaling is used by the satellite to transmit a sequence of independent and completely random bits. In order to turn the enemy's advantage into a disadvantage, Alice and Bob publicly agree to pick only those bits out of the data stream that they receive very reliably, but disregard bits that are not received reliably by both of them. Note that since the receiver output is analog rather than two-level quantized, the reliability of a decision about the bit sent by A can be determined as a function of the absolute value of the receiver's output. Although Alice's and Bob's bit error probabilities are on the average much worse than the Eve's bit error probability, they are much better when the average is taken only over the selected bits. Note that, by the independence of the two channels, knowledge of the positions of the bits received reliably by Alice and Bob gives no information to Eve about the values of these bits. By adding modulo 2 several of the selected bits, Eve's information about the sum of these bits can be reduced to an arbitrarily small amount while keeping the probability that Alice's and Bob's generated bits disagree within specified bounds. Alternatively, the protocol described in [2] could be used to reduce the enemy's information. Clearly, the protocol just described is completely impractical when

Eve's channel is substantially better since the probability that Alice and Bob both can accept a bit is very small.

Only symmetrically distributed binary random variables are considered in the following. One way of generating such a set X, Y, Z is by generating a random bit R according to

$$P_R(0) = P_R(1) = 1/2 \tag{16}$$

and "sending" R over three *independent* binary symmetric channels C_A, C_B and C_E with error probabilities ϵ_A, ϵ_B and ϵ_E, respectively, i.e., P_{XYZ} is defined by

$$P_{XYZ|R} = P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R} \tag{17}$$

where $P_{X|R}(x,r) = 1 - \epsilon_A$ if $x = r$ and ϵ_A else, $P_{Y|R}(y,r) = 1 - \epsilon_B$ if $y = r$ and ϵ_B else and $P_{Z|R}(z,r) = 1 - \epsilon_E$ if $z = r$ and ϵ_E else.

Consider now an arbitrary probability distribution P_{XYZ} over $\{0,1\}^3$ satisfying the symmetry condition

$$P_{XYZ}(x,y,z) \;=\; P_{XYZ}(\overline{x},\overline{y},\overline{z}) \tag{18}$$

for $x, y, z \in \{0,1\}$, where $\overline{c}$ denotes the complement of a binary variable c. Note that condition (18) implies that X, Y and Z are symmetrically distributed. One can prove by straightforward verification that every such set X, Y and Z specified by the parameters $\beta_{bc} = P_{XYZ}(0,b,c)$ for $b, c \in \{0,1\}$, and for which not exactly for one of the pairs $[X,Y]$, $[X,Z]$ and $[Y,Z]$ the two random variables are statistically independent, can be generated according to (16) and (17) by independent binary symmetric channels C_E, C_A and C_B with bit error probabilities

$$\epsilon_E = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 8\frac{\beta_{01} - 2(\beta_{01}+\beta_{10})(\beta_{01}+\beta_{11})}{1 - 4\beta_{10} - 4\beta_{11}}},$$

$$\epsilon_A = \frac{2\beta_{01} + 2\beta_{11} - \epsilon_E}{1 - 2\epsilon_E}$$

and

$$\epsilon_B = \frac{2\beta_{01} + 2\beta_{10} - \epsilon_E}{1 - 2\epsilon_E},$$

respectively. If $1 - 4\beta_{10} - 4\beta_{11} = 0$ and/or $\epsilon_E = 1/2$ and therefore one of the above denominators is 0, then ϵ_A, ϵ_B and ϵ_E can still be computed using formulas that are obtained from those above by exploiting the symmetry.

As one realistic scenario where X, Y and Z with probability distribution P_{XYZ} satisfying (18) are available for two parties and an enemy, consider a satellite broadcasting random bits at a very low signal-to-noise ratio such that even an enemy Eve with a receiving antenna that is much larger and more sophisticated than Alice's and Bob's antennae cannot receive the bits without error. As demonstrated above, such a scenario is equivalent to X, Y and Z being generated by three independent channels according to (16) and (17) for some choice of ϵ_A, ϵ_B and ϵ_E.

Theorem 8. *Let X, Y and Z be binary random variables generated according to (16) and (17). Then*

$$S(X;Y||Z) \;\geq\; \max[h(\epsilon_A+\epsilon_E-2\epsilon_A\epsilon_E),\; h(\epsilon_B+\epsilon_E-2\epsilon_B\epsilon_E)] - h(\epsilon_A + \epsilon_B - 2\epsilon_A\epsilon_B).$$

Proof. We have $X = Y$ if and only if either $X = R$ and $Y = R$ or $X \neq R$ and $Y \neq R$. Hence $P[X = Y] = \epsilon_A\epsilon_B + (1 - \epsilon_A)(1 - \epsilon_B) = 1 - \epsilon_A - \epsilon_B + 2\epsilon_A\epsilon_B$. Similarly, one obtains $P[X = Z] = 1 - \epsilon_A - \epsilon_E + 2\epsilon_A\epsilon_E$ and $P[Y = Z] = 1 - \epsilon_B - \epsilon_E + 2\epsilon_B\epsilon_E$. The theorem thus follows immediately from Theorem 6 where the term $I(X;Y)$ has been moved outside the maximization. □

The lower bound of Theorem 8 vanishes unless either $\epsilon_A < \epsilon_E$ or $\epsilon_B < \epsilon_E$, i.e., unless either Alice's or Bob's channel is superior to Eve's channel. It is somewhat surprising that even when Eve's channel is much more reliable that both Alice's and Bob's channel, secret key agreement is possible as will be demonstrated below.

Alice randomly selects a codeword V^N from the set of codewords of an appropriate error-correcting code $\mathcal{C}$ with codewords of length N and sends it to Bob (and also to Eve) over a conceptual broadcast channel by sending $X^N + V^N$ over the public channel. Bob and Eve receive the bits of V^N with bit error probabilities $\epsilon_A + \epsilon_B - 2\epsilon_A\epsilon_B$ and $\epsilon_A + \epsilon_E - 2\epsilon_A\epsilon_E$, respectively, where the latter is smaller than the former unless $\epsilon_E \geq \epsilon_B$. The key to achieving a positive secret key rate even if both $\epsilon_A > \epsilon_E$ and $\epsilon_B > \epsilon_E$ is for Bob to accept a received word only if he can make a very reliable decision about the codeword sent by Alice, i.e., if it is very close to some codeword of the code $\mathcal{C}$ or, more formally, if the Hamming distance to a codeword is much smaller than the number of errors correctable by an optimal decoder for the code, hence generally smaller than half the code's minimum distance. For each received block Bob announces over the public channel whether he accept or rejects it.

The key observation in the above protocol is that although Eve receives codewords V^N more reliably than Bob on the average, her conceptual channel may nevertheless be worse (for appropriate choices of a code $\mathcal{C}$ and for an appropriate reliability decision) than Bob's channel, if one averages only over those instances accepted by Bob. Because consecutive uses of the channel are independent, the words discarded by Bob are also useless for Eve.

Consider now the special case of a length N repeat code having only the two codewords $[0, 0, \ldots, 0]$ and $[1, 1, \ldots, 1]$. For $j = 1, 2, \ldots$ Alice randomly generates an information bit R_j and sends $V_j^N = [R_j, R_j, \ldots, R_j]$ over the conceptual channel to Bob. Bob accepts a received word if and only if it is exactly equal to one of the codewords, i.e., if and only if it is equal to $[0, 0, \ldots, 0]$ or $[1, 1, \ldots, 1]$. Let $\delta_A = 1 - \epsilon_A$, $\delta_B = 1 - \epsilon_B$ and $\delta_E = 1 - \epsilon_E$. The probability that a codeword is received by Bob without error is given by

$$p_{\text{correct}} = (\delta_A\delta_B + \epsilon_A\epsilon_B)^N$$

and similarly the probability that a codeword is received as its complement equals

$$p_{\text{error}} = (1 - \delta_A\delta_B - \epsilon_A\epsilon_B)^N.$$

The probability that Bob accepts a codeword is

$$p_{\text{accept}} = p_{\text{correct}} + p_{\text{error}}$$

and the channel from Alice to Bob thus corresponds to a binary symmetric channel with bit error probability

$$\beta \;=\; p_{\text{error}}/p_{\text{accept}}.$$

Let α_{rs} for $r, s \in \{0, 1\}$ be the probability that a single bit 0 sent by Alice is received by Bob as r and by Eve as s, i.e., let $\alpha_{00} = \delta_A\delta_B\delta_E + \epsilon_A\epsilon_B\epsilon_E$, $\alpha_{01} = \delta_A\delta_B\epsilon_E + \epsilon_A\epsilon_B\delta_E$,

$\alpha_{10} = \delta_A\epsilon_B\delta_E + \epsilon_A\delta_B\epsilon_E$, and $\alpha_{11} = \delta_A\epsilon_B\epsilon_E + \epsilon_A\delta_B\delta_E$. Let further p_w for $0 \leq w \leq N$ be the probability that the codeword $[0, 0, \ldots, 0]$ sent by Alice is accepted by Bob (whether correctly or not) and is received by Eve as a particular given word of Hamming weight w. We have

$$p_w \;=\; \alpha_{00}^{N-w}\alpha_{01}^{w} + \alpha_{10}^{N-w}\alpha_{11}^{w}.$$

Eve's average error probability when she guesses the bit sent by Alice is hence

$$\gamma \;=\; \frac{1}{p_{\text{accept}}} \sum_{w=\lceil N/2 \rceil}^{N} \binom{N}{w} p_w.$$

The block length N can always be chosen such that $\gamma > \beta$, i.e., such that Bob's decision about the bit sent by Alice (provided that Bob accepts the corresponding received word) is more reliable than Eve's decision. However, the more relevant quantities here are the mutual informations I_B and I_E obtained by Bob and Eve, respectively, about the bit sent by Alice. Clearly

$$I_B \;=\; 1 - h(\beta)$$

and I_E can be computed as the average over the weights $w = 0, \ldots, N$ of the information about the bit R_j (sent by Alice) obtained by Eve when she receives a words of weight w. We have

$$P_{R_j|Z^N}(0|z^N) = p_w/(p_w + p_{N-w})$$

and

$$P_{R_j|Z^N}(1|z^N) = p_{N-w}/(p_w + p_{N-w})$$

for all received words z^N of weight w. Hence

$$I_E \;=\; \sum_{w=0}^{N} \binom{N}{w} \frac{p_w}{p_{\text{accept}}} \left(1 - h(\frac{p_w}{p_w + p_{N-w}})\right).$$

Example. Let $\epsilon_A = \epsilon_B = 0.2$, $\epsilon_E = 0.15$ and $N = 5$. Then $p_{\text{correct}} = 0.14539$, $p_{\text{error}} = 0.003355$, $p_{\text{accept}} = 0.14875$, $\alpha_{00} = 0.55$, $\alpha_{01} = 0.13$, $\alpha_{10} = \alpha_{11} = 0.16$, $p_0 = 0.05043$, $p_1 = 0.01200$, $p_2 = 0.002917$, $p_3 = 0.0007695$, $p_4 = 0.0002619$ and $p_5 = 0.00014198$. Hence $\beta = 2.25\%$ compared to $\gamma = 6.15\%$ and thus Bob receives the selected bits much more reliably than Eve. One further obtains $I_B = 0.845$ and $I_E = 0.745$, i.e., Eve's information about the bit sent by Alice (and accepted by Bob) is 12% smaller than Bob's information.

For sufficiently large N we have $I_E < I_B$ and β arbitrarily small. By adding an appropriate number of such bits modulo 2, Eve's information about the resulting bit can be made arbitrarily small while at the same time keeping the probability that Alice's and Bob's bits disagree arbitrarily small. The following theorem is hence proved.

Theorem 9. *Let X, Y and Z be binary random variables generated according to (16) and (17) for some $\epsilon_E > 0$. Then $S(X;Y||Z)$ is strictly positive.*

The above example can be generalized in several ways. In particular, it is not necessary that after one round of this protocol, Bob knows the bits sent by Alice more reliably than Eve. The same protocol can be used in several rounds to continuously reduce the enemy's information and increase Alice's and Bob's reliability for the shared string. Some protocols that allow Alice and Bob to share a substantial amount of secret key even when Eve's channel is a few orders of magnitude more reliable than Alice's and Bob's channels are discussed in [10].

VI. Conclusions

In Shannon's classical view of cryptography [13], a necessary condition for two parties Alice and Bob to be able to communicate in secrecy is that they have a common advantage over potential enemies, be it a physically protected communication channel connecting them or a shared secret key. This view was dramatically revised by the publication of the seminal paper of Diffie and Hellman [6]. Public-key cryptography demonstrates that (computationally) secure communications can be achieved even if only the receiver of a message, but not necessarily the sender, has an advantage over all potential enemy receivers. The results of this paper can be interpreted as a further step in the same direction, namely as demonstrating that only a *difference* in the received signals, but not necessarily with an advantage for either of the legitimate communicants, suffices for achieving perfect cryptographic security, regardless of the enemy's computing power.

The paper suggests the following conclusion for the implementation of cryptographic systems on given noisy communication channels. Such channels should not be converted into error-free channels by means of error-correcting codes, followed by a cryptographic protocol based on error-free channels because this design strategy would imply that Shannon's pessimistic inequality (2) applies and therefore perfect secrecy cannot be achieved unless an impractically large amount of shared secret key is available. Instead, cryptographic coding and error-control coding should be combined, resulting in a system achieving virtually perfect secrecy, with a (short) secret key being required only for authentication.

The author hopes that this paper and a subsequent paper on practical implementations will help to move perfect secrecy closer to being practical.

Appendix

Proof of Theorem 7. The lower bound is trivial. In proving the upper bound, our goal is to show in analogy to Theorem 3 that

$$\frac{1}{N}H(S) \;\leq\; \max_{P_X} I(X;Y|Z) + \frac{1}{N}H(S|S') + \frac{1}{N}I(S;C^N Z^N). \tag{19}$$

According to (9), (10) and the definition of secrecy capacity the last two terms must vanish as $N \to \infty$. That $H(S)/N \leq \max_{P_X} I(X;Y)$ follows from $H(S)/N \leq \max_{P_X} I(X;Y|Z)$ by choosing Z as a constant random variable.

In order to prove (19), note that

$$H(S) \;\leq\; I(X^N;Y^N|C^N Z^N) + H(S|S') + I(S;C^N Z^N)$$

can be derived in exact analogy to the derivation of (11) and (12). It remains to prove that

$$I(X^N;Y^N|C^N Z^N) \;\leq\; N \cdot \max_{P_X} I(X;Y|Z). \tag{20}$$

In the following derivations, the index i is understood to range from 1 to N. Alice's choice of P_{X_i} depends only on C^{i-1} and X^{i-1}, but not further on Y^{i-1} and Z^{i-1}, i.e.,

$$H(X_i|C^{i-1}X^{i-1}Y^{i-1}Z^{i-1}) = H(X_i|C^{i-1}X^{i-1}). \tag{21}$$

Similarly, the ith broadcast channel output $[Y_i, Z_i]$ depends on $C^{i-1}, X^{i-1}, Y^{i-1}$ and Z^{i-1} only through its dependence on X_i, which can be written as

$$H(Y_iZ_i|C^{i-1}X^iY^{i-1}Z^{i-1}) = H(Y_iZ_i|X_i). \tag{22}$$

One similarly has

$$H(Z_i|C^{i-1}X^iY^{i-1}Z^{i-1}) = H(Z_i|X_i) \tag{23}$$

when only the Z-output of the channel is considered. Note that these conditions can be interpreted as corresponding to the first equality on p. 331 of [3] in the proof of Theorem 9.1.1 stating that feedback cannot increase the capacity of a discrete memoryless channel.

We now derive two equalities that will be used later. First, using (22) and (23) one obtains

$$\begin{aligned} H(Y_i|C^{i-1}X^iY^{i-1}Z^i) &= H(Y_iZ_i|C^{i-1}X^iY^{i-1}Z^{i-1}) - H(Z_i|C^{i-1}X^iY^{i-1}Z^{i-1}) \\ &= H(Y_iZ_i|Z_i) - H(Z_i|X_i) \\ &= H(Y_i|X_iZ_i). \end{aligned} \tag{24}$$

Second, expanding the following conditional entropy in two different ways,

$$\begin{aligned} H(X_iY^{i-1}Z_i|C^{i-1}X^{i-1}Z^{i-1}) &= H(X_iZ_i|C^{i-1}X^{i-1}Z^{i-1}) + H(Y^{i-1}|C^{i-1}X^iZ^i) \\ &= H(X_iZ_i|C^{i-1}X^{i-1}Y^{i-1}Z^{i-1}) + H(Y^{i-1}|C^{i-1}X^{i-1}Z^{i-1}), \end{aligned}$$

and using

$$\begin{aligned} H(X_iZ_i|C^{i-1}X^{i-1}Y^{i-1}Z^{i-1}) &= H(X_i|C^{i-1}X^{i-1}Y^{i-1}Z^{i-1}) + H(Z_i|C^{i-1}X^iY^{i-1}Z^{i-1}) \\ &= H(X_i|C^{i-1}X^{i-1}Z^{i-1}) + H(Z_i|C^{i-1}X^iZ^{i-1}) \\ &= H(X_iZ_i|C^{i-1}X^{i-1}Z^{i-1}), \end{aligned}$$

where the second step follows from applications of (21) and (23), leads to

$$H(Y^{i-1}|C^{i-1}X^iZ^i) \;=\; H(Y^{i-1}|C^{i-1}X^{i-1}Z^{i-1}). \tag{25}$$

Repeating the argument leading to (13) for every public message of step i, i.e., for $C_{i1}, \ldots, C_{it_i}$, where in the derivation of (13), X, Y and Z are replaced by X^i, Y^i and Z^i, respectively, C^t is replaced by $[C^{i-1}, C_{i1}, \ldots, C_{ij}]$ in the $(t_i - j)$-th application, and the term $I(X^i;Y^i|C^{i-1}C_{i1}\cdots C_{ij}Z^i)$ is expressed as a difference of conditional entropies of Y^i and X^i according to whether Alice or Bob is the sender of message C_{ij}, respectively, one arrives at

$$I(X^i;Y^i|C^iZ^i) \;\leq\; I(X^i;Y^i|C^{i-1}Z^i). \tag{26}$$

Now using the trivial inequalities

$$H(Y^{i-1}|C^{i-1}Z^i) \;\leq\; H(Y^{i-1}|C^{i-1}Z^{i-1})$$

and

$$H(Y_i|C^{i-1}Y^{i-1}Z^i) \leq \; H(Y_i|Z_i)$$

and equations (24) and (25) one obtains

$$\begin{aligned}
I(X^i;Y^i|C^{i-1}Z^i) &= H(Y^i|C^{i-1}Z^i) - H(Y^i|C^{i-1}X^iZ^i) \\
&= H(Y^{i-1}|C^{i-1}Z^i) + H(Y_i|C^{i-1}Y^{i-1}Z^i) \\
&\qquad -H(Y^{i-1}|C^{i-1}X^iZ^i) - H(Y_i|C^{i-1}X^iY^{i-1}Z^i) \\
&\leq H(Y^{i-1}|C^{i-1}Z^{i-1}) + H(Y_i|Z_i) - H(Y^{i-1}|C^{i-1}X^{i-1}Z^{i-1}) - H(Y_i|X_iZ_i) \\
&= I(X^{i-1};Y^{i-1}|C^{i-1}Z^{i-1}) + I(X_i;Y_i|Z_i). \qquad (27)
\end{aligned}$$

Inequality (20) and hence the theorem follow by consecutive applications of (26) and (27) for $i = N, N-1, \ldots, 1$ and the fact that for all i,

$$I(X_i;Y_i|Z_i) \; \leq \; \max_{P_X} I(X;Y|Z). \quad \Box$$

Acknowledgment

It is a pleasure to thank Charles H. Bennett, Gilles Brassard and Jim Massey for interesting and helpful discussions. Some of the results of this paper were found independently by R. Ahlswede and I. Csiszár who were motivated by a talk given by the author at the 1990 IEEE Workshop on Information Theory in Veldhoven, The Netherlands.

References

[1] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, Vol. 5, No. 1, pp. 3-28, 1992.

[2] C.H. Bennett, G. Brassard and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, Vol. 17, No. 2, pp. 210-229, 1988.

[3] R.E. Blahut, *Principles and Practice of Information Theory*, Reading, MA: Addison-Wesley, 1987.

[4] G. Brassard, *Modern Cryptology: A Tutorial*, Lecture Notes in Computer Science, Vol. 325, Berlin: Springer-Verlag, 1988.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339-348, 1978.

[6] W. Diffie and M.E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-654, 1976.

[7] S.K. Leung-Yan-Cheong, "Multi-user and wiretap channels including feedback," Tech. Rep. No. 6603-2, Stanford University, Information Systems Lab., July 1976.

[8] U.M. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher," *Journal of Cryptology*, Vol. 5, No. 1, pp. 53-66, 1992.

[9] U.M. Maurer, "Perfect cryptographic security from partially independent channels," *Proc. 23rd ACM Symposium on Theory of Computing*, New Orleans, May 6-8, pp. 561-572, 1991.

[10] U.M. Maurer, "Protocols for secret key agreement based on common information," presented at CRYPTO'92, Santa Barbara, CA, Aug. 16-20, 1992.

[11] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[12] C.E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, Vol. 27, pp. 379-423 and 623-656, 1948.

[13] C.E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, Vol. 28, pp. 656-715, Oct. 1949.

[14] G.S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Elec. Eng.*, Vol. 55, pp. 109-115, 1926.

[15] M.N. Wegman and J.L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, Vol. 22, pp. 265-279, 1981.

[16] A.D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, 1975.