Secret Message Capacity of Erasure Broadcast Channels with Feedback

László Czap Vinod M. Prabhakaran Christina Fragouli
École Polytechnique Fédérale de Lausanne, Switzerland
Email: {laszlo.czap vinod.prabhakaran christina.fragouli}@epfl.ch

Suhas Diggavi
University of California, Los Angeles (UCLA)
Email:suhas@ee.ucla.edu

***Abstract*—We characterize the secret message capacity of a wiretapped erasure channel where causal channel state information of the honest nodes is publicly available. In doing so, we establish an intimate connection between message secrecy and secret key generation for the same channel setup. We propose a linear coding scheme that has polynomial encoding/decoding complexity, and prove a converse that shows the optimality of our scheme. Our work also demonstrates the value of causal public feedback, which has previously been shown for the secret key generation problem.**

I. Introduction

We investigate the problem where a node, Alice, wants to secretly convey a message to another node, Bob, in the presence of a passive eavesdropper, Eve. Alice can communicate with Bob using a broadcast erasure channel, but both Bob and Eve will receive (independently) erased versions of her transmissions. Additionally, we assume a low capacity public feedback channel from Bob to Alice that enables Alice to learn which of her past transmissions were correctly received by Bob. That is, Alice (and Eve) have causal channel state information for the channel between Alice and Bob.

The term *secrecy capacity* is commonly used for either secret key generation or secret message transmission; however, there is an important difference between these two. In secret key generation we require that honest users agree on *any* common secret randomness; on the other hand, for secret message transmission, we require that Bob secretly recovers a *specific message* sent by Alice. For clarity, we will use *secret key capacity* C_K and *secret message capacity* C_{SM} whenever we want to emphasize the difference. We are interested in calculating C_{SM}.

Clearly, the secret key capacity of a channel is an upper bound for the secret message capacity, i.e., $C_{SM} \leq C_K$. This is because for the secret key problem, we are not constrained by what common randomness Alice and Bob securely agree upon. In contrast, the message secrecy problem requires secure delivery of a particular message, which can also serve as secure common randomness. One natural strategy is to generate a secret key, use it as a one-time pad to encrypt the message, and send the encrypted message reliably using a forward error correcting (FEC) code. An improvement over this is possible when Eve has a higher erasure probability than Bob by leveraging secrecy from both the secret key generated and the channel advantage of Bob over Eve using the scheme of Yamamoto [1]. However, our capacity-achieving scheme demonstrates that one can do even better by exploiting feedback (see Figures 1-2). In particular we design a hybrid scheme that uses a key to partially encrypt the message and generates the additional secrecy required from the channel using feedback. The benefits of our scheme come from using ARQ (as opposed to FEC or a wiretap code) to deliver encrypted message packets to Bob. ARQ focuses on reliable transmission to Bob and hence could repeat (identical) transmissions, with the result that Eve receives fewer *distinct* encrypted message packets. Even when Eve has a lower erasure probability than Bob, the ARQ scheme ensures that Bob has a relative advantage over Eve. Therefore feedback has been used for the purpose of reducing the required key size by tilting the channel advantage towards Bob.

The rest of this paper is organized as follows. Section II overviews related work; Section III describes the channel model; Section IV provides our main result; Section V gives a constructive proof of achievability; Section VI proves the the converse.

II. Related Work

Wyner's seminal paper [2] calculated the secrecy capacity of the wiretap channel without feedback. Applied to erasure channels, this result states that the secrecy capacity is non-zero only if the honest party has a better channel than the eavesdropper, *i.e.,* the erasure probability towards Eve is higher than towards Bob. In this case, there is no difference between the secret key and the secret message capacity. In contrast, we show that if we use feedback, this equivalence does not always hold.

Use of feedback and public discussion can improve the secrecy capacity, as was first shown by Maurer [3], followed by more general results for multiple terminals in [4], [5]. All these results focus on secret key generation, however, a cost-free public channel with infinite capacity is also available by assumption. As a result, the secret message capacity is trivially the same, because the message can be encrypted with the generated secret key using a one-time-pad and sent securely on the public channel. In contrast, our setup assumes only state feedback is available publicly, and there is no other high-capacity public channel. A similar setup, but with *non-causal* state-information available *only* to the transmitter was studied in [6], [7] for the Gaussian problem, where some achievability

978-1-4577-0437-6/11/$26.00 ©2011 IEEE

schemes based on dirty-paper coding were examined. As far as we know, this paper presents the first characterization of the secret message capacity with limited feedback for a non-trivial setup.

For the broadcast erasure channel with public discussion a capacity achieving scheme was proposed in [8], [9] for the group secret key generation problem, where the public channel is also considered free and unlimited. However in the two-party special case the secrecy capacity characterized in [3] specializes easily to requiring only the channel state to be communicated over the public channel. This observation gives the secret key capacity for our setup as well; in the sequel we will focus on the secret message capacity problem.

III. System model and notation

We investigate two-party communication in the presence of an eavesdropping adversary, Eve. The sender Alice wants to securely send a message W to Bob through a memoryless erasure broadcast channel defined as follows. The ith input to the channel by Alice is denoted by X_i, and is a length L vector over $\mathbb{F}_q$. Let us denote Y_i and Z_i the ith output of the channel, *i.e.,* the vectors received by Bob and Eve respectively. We use $\perp$ as the symbol of an erasure. The broadcast channel is conditionally independent, *i.e.,* $\Pr\{Y_i, Z_i|X_i\} = \Pr\{Y_i|X_i\}\Pr\{Z_i|X_i\}$, and

$$\Pr\{Y_i|X_i\} = \begin{cases} 1-\delta, & Y_i = X_i \\ \delta, & Y_i = \perp, \end{cases}$$

$$\Pr\{Z_i|X_i\} = \begin{cases} 1-\delta_E, & Z_i = X_i \\ \delta_E, & Z_i = \perp . \end{cases}$$

The probabilities δ, δ_E are assumed to be known by all parties.

The notation X^i will be used to denote $(X_1, X_2, \ldots, X_i)$ and X_i^j to denote $(X_i, X_{i+1}, \ldots, X_j)$. Let S_i denote the random variable that describes the state of Bob's channel at the ith transmission. S_i is a random variable on values in $\{B, \emptyset\}$, where $\Pr\{S_i = B\} = 1-\delta$ meaning Bob correctly received the ith packet. We model the feedback channel as Alice and Eve having access causally to the channel states, i.e. before the ith transmission they both know the vector S^{i-1}. We also allow private randomness at all nodes. We denote by U the private randomness of Alice.

Definition 1. *We say that R_{SM} is an achievable secret message rate if for any $\epsilon > 0$ and sufficiently large n the following conditions hold for some functions $f_i(\cdot), W_B(\cdot)$:*

$$X_i = f_i(W, U, S^{i-1}), \quad i = 1, 2, \ldots, n, \tag{1}$$

where the message W is uniformly distributed over $\{1, 2, \ldots, 2^{n(R_{SM}-\epsilon)}\}$. Bob is able to recover W with high probability:

$$\hat{W} = W_B(Y^n), \tag{2}$$

$$\Pr\{\hat{W} \neq W\} < \epsilon. \tag{3}$$

Eve gains negligible useful information:

$$I(W; Z^n S^n) < \epsilon. \tag{4}$$

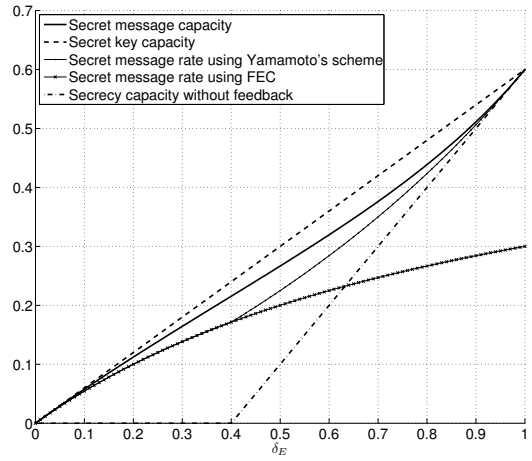

Figure 1. Secret message and secret key capacities with and without state-feedback for $\delta = 0.4$. The rates achieved using FEC and Yamamoto's scheme are also plotted.

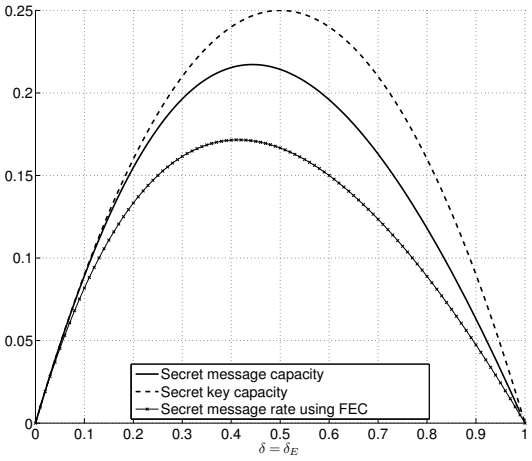

Figure 2. Secret message and secret key capacities for $\delta = \delta_E$ together with the rate achieved using FEC (or Yamamoto's scheme).

Definition 2. *The supremum of all achievable secret message rates is the secret message capacity of the channel denoted by C_{SM}.*

IV. Main result

The following theorem is the main result of this paper.

Theorem 1. *The secret message capacity of the wiretapped erasure channel with state-feedback is*

$$C_{SM} = (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2} L \log q.$$

For comparison we plot the secret message and the secret key capacity together with the secrecy capacity when no

feedback is available for some special parameter values. We plot secret message rates achieved using FEC and Yamamoto's scheme as well. For simplicity we set $L = 1, q = 2$. Figures 1-2 show the gap between the secret message and the secret key capacities as well as the benefit that state-feedback provides. We derive the secret message capacity of the described channel in two steps: we first propose a coding scheme for secret message sending, and then give the converse proof.

V. Achievability scheme

For simplicity, we assume that the message W can be divided into N packets $W_1, W_2, \ldots, W_N$ each of size $L \log q$. Our scheme has two phases as follows:

1) Key setup: A common secret key is set up between Alice and Bob. The size of this key is (in units of $L \log q$)

$$K = M + M^{3/4}, \tag{5}$$

$$\text{where} \quad M = N\frac{1-\delta_E}{1-\delta\delta_E}. \tag{6}$$

2) Message transmission: Our scheme uses a mix of a one-time pad with the key generated in the first phase and secrecy obtained by the noisy erasure broadcast. In particular, we linearly mix the pure message packets with encrypted message packets using a one-time-pad with the key. This mixture is then sent to Bob using an ARQ scheme, *i.e.* each packet is repeated until Bob receives it. Eve will receive fewer *distinct* packets under this ARQ scheme compared to a FEC erasure coding scheme which ignores the state feedback.

In the following, we describe the two phases in detail.

1) Key setup: The capacity achieving scheme for the secret key generation problem is given in [3], [8], [9]. We utilize this as the first phase of our scheme. For convenience, we summarize the main steps here:

- Alice sends n' packets selected independently from $\mathbb{F}_q^L$ uniformly at random. In expectation, Bob correctly receives $n'(1-\delta)$ packets, out of which $n'(1-\delta)\delta_E$ are not received by Eve.
- By assumption, Alice knows exactly the packets that Bob correctly received. Both Alice and Bob create the same $n'((1-\delta)\delta_E - \epsilon')$ linear combinations of Bob's packets. For this, the parity check matrix of an MDS code is utilized to ensure that resulting packets are independent and their encoding vector has sufficiently large weight. The resulting packets are concatenated and can be used as a secret key.

The amount of secret key generated by this scheme is $n'((1-\delta)\delta_E - \epsilon')L \log q$.

The secrecy is in the sense of (4) with security parameter ϵ'. For proofs and details we refer the reader to [8], [9].

2) Message transmission: From the properties of the first phase we may assume that Alice and Bob have common keys $\mathcal{K} = (\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_K)$ each of size $L \log q$ that are secret from Eve[1].

Alice does the following:

[1]The loss from treating K as an integer is negligible.

1) She encrypts a part of the message using one-time-pad:
$$W' = W^K \oplus \mathcal{K}. \tag{7}$$
2) The resulting partially encrypted message $[W',\ W_{K+1}^N]$ is then encoded using a generator matrix $G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}$. The encoded block is then
$$\mathcal{W} = W'G_1 + W_{K+1}^N G_2.$$
G is a publicly known full-rank $N \times N$ matrix such that G_1 is the generator matrix of an (N, K) MDS code.
3) The columns $(\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_N)$ of $\mathcal{W}$ are transmitted to Bob using ARQ. Formally, given that n' is the length of the first (key-generation) phase,
$$X_{n'+1} = \mathcal{W}_1;\ X_{n'+i+1} = \begin{cases} X_i = \mathcal{W}_j, & \text{if } S_{n'+i} = \emptyset \\ \mathcal{W}_{j+1}, & \text{if } S_{n'+i} = B. \end{cases}$$
If all the columns have not been received by Bob before the end of the blocklength n defined below, the protocol terminates and an error is declared. Let
$$n = n' + n'' + n''^{3/4}, \tag{8}$$
$$\text{where} \quad n'' = \frac{N}{1-\delta}. \tag{9}$$

Theorem 2. *The scheme described above achieves a secret message rate of*

$$R_{SM} = (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2} L \log q.$$

Proof: Let us first investigate conditions (1)-(4). Out of these, (1) is trivially satisfied by the scheme. Next, we prove that the secrecy condition (4) also holds.

First, note that by construction (and by the properties of the scheme for key setup), anything that Eve learns during the first phase is independent of the message and practically independent of all packets sent during the second phase. From this it follows that it is sufficient to investigate the second phase only. Thus

$$I(W; Z^n S^n) = I(W; Z^{n'} S^{n'} \mathcal{W}_I I) = I(W; \mathcal{W}_I | Z^{n'} S^{n'} I),$$

where $\mathcal{W}_I$ are the columns of $\mathcal{W}$ Eve overhears, and I is the set of indices of these overheard columns. Notice that

$$H(\mathcal{W}_I | Z^{n'} S^{n'}, I = i) \le |i| L \log q.$$

Moreover, from the MDS property of the G_1 matrix, we have

$$\begin{aligned} H(\mathcal{W}_I | W Z^{n'} S^{n'}, I = i) &= H(\mathcal{K} G_1^{(i)} | Z^{n'} S^{n'}) \\ &= H(\mathcal{K} G_1^{(i)}) - I(\mathcal{K} G_1^{(i)}; Z^{n'} S^{n'}) \\ &\ge \min(|i|, K) L \log q - \epsilon', \end{aligned}$$

where $G_1^{(i)}$ is the G_1 matrix restricted to the columns indexed by i. Here, ϵ' is the security parameter from the key-generation scheme. Hence,

$$\begin{aligned} I(W; Z^n S^n) &\le \sum_{m=0}^{N} \Pr\{|I| = m\} \max(0, m-K) L \log q + \epsilon' \\ &\le \Pr\{|I| \ge K\} N L \log q + \epsilon'. \end{aligned}$$

Now, we need a concentration result for $|I|$ by using the erasure channel probabilities and our ARQ strategy. By inspecting the ARQ scheme, the probability that a given column is received correctly by Eve is

$$p = (1-\delta_E) + \delta\delta_E(1-\delta_E) + \cdots = \frac{1-\delta_E}{1-\delta\delta_E}.$$

Then, $|I|$ can be seen as the sum of N independent random variables on $\{0,1\}$ drawn from a Bernoulli distribution $Ber(p)$. So, we have that

$$E[|I|] = N\frac{1-\delta_E}{1-\delta\delta_E} = M. \tag{10}$$

Moreover, from the Chernoff-Hoeffding bound

$$\Pr\{|I| \geq K\} = \Pr\left\{|I| \geq M + M^{3/4}\right\} \leq \exp\left(-\frac{\sqrt{M}}{4}\right).$$

From this concentration result we get

$$I(W; Z^n S^n) \leq \exp\left(-\frac{\sqrt{M}}{4}\right) NL\log q + \epsilon'. \tag{11}$$

By choosing N (and at the same time M) sufficiently large and using (6), we may satisfy (4).

To show (2)-(3), notice that if Bob receives all the columns of $\mathcal{W}$ in the second phase, then since G is full rank, he can decode $[W',\ W_{K+1}^N]$. From the first phase, Bob knows $\mathcal{K}$, so by (7) he can decode W. The probability that the protocol terminates before Bob receives all the columns can be made arbitrarily small: To see this, notice that since the expected number of transmissions for each column of $\mathcal{W}$ so that Bob receives it is $1/(1-\delta)$, the average number of transmissions in an unterminated protocol which continues till Bob receives all the columns is $n'' = N/(1-\delta)$. Now we can employ Chernoff-Hoeffding bound to argue that the probability that our protocol terminates before Bob receives all the columns can be made arbitrarily small by a large enough choice of N [10, Problem 2.4]. It only remains to calculate the rate.

The rate of communication achieved is

$$\begin{aligned}\frac{N}{n} &= \frac{N}{n' + n'' + n''^{3/4}} \\ &= \frac{N}{\frac{K}{\delta_E(1-\delta)-\epsilon'} + \frac{N}{1-\delta} + \frac{N^{3/4}}{(1-\delta)^{3/4}}}.\end{aligned}$$

Substituting for K from (5)-(6), it is easy to see that for a sufficiently large choice of N this can be made arbitrarily close to R_{SM} in the theorem statement. ∎

VI. Converse

We give a matching upper bound on the achievable secret message rate. To prove the converse part, we will assume that the channel state of Eve is also known publicly. Hence, in this part $S_i \in \{B, E, EB, \emptyset\}$. The four possible outcomes refer to correct receptions by: "Bob only", "Eve only","Eve & Bob" and "Neither" respectively. Clearly, this extension could only increase the achievable secret message rate, thus an upper bound in this model is valid in the original channel also.

We are going to use the following two lemmas.

Lemma 1. *If $I(W; Z^n S^n) < \epsilon$, then*

$$\sum_{i=1}^n I(W; X_i | Z^{i-1} S^{i-1}) < \frac{\epsilon}{1-\delta_E}$$

Proof:

$$\begin{aligned}\epsilon > I(W; Z^n S^n) &= \sum_{i=1}^n I(W; Z_i S_i | Z^{i-1} S^{i-1}) \\ &= \sum_{i=1}^n I(W; Z_i | Z^{i-1} S^{i-1} S_i) && (12) \\ &= \sum_{i=1}^n I(W; Z_i | Z^{i-1} S^{i-1} S_i \in \{E, EB\}) \cdot \\ &\quad \cdot \Pr\{S_i \in \{E, EB\}\} && (13) \\ &= \sum_{i=1}^n I(W; X_i | Z^{i-1} S^{i-1} S_i \in \{E, EB\})(1-\delta_E) && (14) \\ &= \sum_{i=1}^n I(W; X_i | Z^{i-1} S^{i-1})(1-\delta_E) && (15)\end{aligned}$$

Here, (12) comes from the fact that S_i is independent of W, Z^i and S^{i-1}. To get (13) we exploit that the mutual information is 0 if $Z_i = \perp$. Given $S_i \in \{E, EB\}$, $Z_i = X_i$, this results (14). Then, we use again the independence of S_i to get (15). This concludes the proof. ∎

Lemma 2. *In the described model, if conditions (1)-(4) are satisfied, then*

$$\sum_{i=1}^n I(W; X_i | Y^{i-1} Z^{i-1} S^{i-1}) \geq \frac{nR_{SM}}{1-\delta\delta_E}$$

The proof is similar to the proof of Lemma 1 and is omitted. Next, we state the converse theorem.

Theorem 3. *For the achievable secret message rate as defined in Def. 1 it holds that*

$$R_{SM} \leq (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2} L\log q.$$

Proof:

$$\begin{aligned}nR_{SM} \leq I(W; Y^n S^n) &= \sum_{i=1}^n I(W; Y_i S_i | Y^{i-1} S^{i-1}) \\ &= \sum_{i=1}^n I(W; Y_i | Y^{i-1} S^{i-1} S_i) \\ &= \sum_{i=1}^n I(W; Y_i | Y^{i-1} S^{i-1} S_i \in \{B, EB\}) \cdot \\ &\qquad \cdot \Pr\{S_i \in \{B, EB\}\} \\ &= (1-\delta)\sum_{i=1}^n I(W; X_i | Y^{i-1} S^{i-1}) \\ &= (1-\delta)\sum_{i=1}^n H(X_i | Y^{i-1} S^{i-1}) - H(X_i | Y^{i-1} S^{i-1} W)\end{aligned}$$

$$\leq (1-\delta)\left(nL\log q - \sum_{i=1}^{n} H(X_i|Y^{i-1}S^{i-1}W)\right)$$
$$\leq (1-\delta)\left(nL\log q - \sum_{i=1}^{n} H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W)\right) \quad (16)$$

So far, besides basic information equalities and inequalities we used the same properties as in the proof of Lemma 1.

As the next step in our proof, we are going to bound the term $\sum_{i=1}^{n} H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W)$ separately. Observe the following:

$$\begin{aligned}
0 &\leq H(Y^nS^n|Z^nS^nW) = \\
&= H(Y^{n-1}S^{n-1}|Z^nS^nW) + H(Y_nS_n|Y^{n-1}Z^nS^nW) \\
&= H(Y^{n-1}S^{n-1}|Z^{n-1}S^{n-1}W) \\
&\quad - I(Y^{n-1}S^{n-1}; Z_nS_n|Z^{n-1}S^{n-1}W) \\
&\quad + H(Y_n|Y^{n-1}Z^nS^nW) \\
&= H(Y^{n-1}S^{n-1}|Z^{n-1}S^{n-1}W) \\
&\quad - I(Y^{n-1}S^{n-1}; Z_n|Z^{n-1}S^{n-1}S_nW) \\
&\quad + H(Y_n|Y^{n-1}Z^nS^nW) \\
&= H(Y^{n-1}S^{n-1}|Z^{n-1}S^{n-1}W) \\
&\quad - I(Y^{n-1}S^{n-1}; Z_n|Z^{n-1}S^{n-1}W, S_n \in \{E, EB\})\cdot \\
&\quad \cdot \Pr\{S_n \in \{E, EB\}\} \\
&\quad + H(Y_n|Y^{n-1}Z^nS^{n-1}W, S_n = B)\Pr\{S_n = B\} \\
&\quad + H(Y_n|Y^{n-1}Z^nS^{n-1}W, S_n = EB)\Pr\{S_n = EB\} \\
&= H(Y^{n-1}S^{n-1}|Z^{n-1}S^{n-1}W) \\
&\quad - I(Y^{n-1}S^{n-1}; X_n|Z^{n-1}S^{n-1}W)(1-\delta_E) \\
&\quad + H(X_n|Y^{n-1}Z^{n-1}S^{n-1}W)(1-\delta)\delta_E \\
&\quad + H(X_n|Y^{n-1}Z^{n-1}X_nS^{n-1}W)(1-\delta)(1-\delta_E) \\
&= H(Y^{n-1}S^{n-1}|Z^{n-1}S^{n-1}W) \\
&\quad - I(Y^{n-1}S^{n-1}; X_n|Z^{n-1}S^{n-1}W)(1-\delta_E) \\
&\quad + H(X_n|Y^{n-1}Z^{n-1}S^{n-1}W)(1-\delta)\delta_E
\end{aligned}$$

Again, all we needed was the independence property of S_n. We can perform the same steps recursively to obtain:

$$(1-\delta)\delta_E \sum_{i=1}^{n} H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W) \geq$$
$$(1-\delta_E)\sum_{i=1}^{n} I(Y^{n-1}S^{n-1}; X_n|Z^{n-1}S^{n-1}W) \quad (17)$$

We further bound $\sum_{i=1}^{n} I(Y^{n-1}S^{n-1}; X_n|Z^{n-1}S^{n-1}W)$:

$$\begin{aligned}
&\sum_{i=1}^{n} I(Y^{n-1}S^{n-1}; X_n|Z^{n-1}S^{n-1}W) \\
&= \sum_{i=1}^{n} H(X_i|Z^{i-1}S^{i-1}W) - H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W) \\
&= \sum_{i=1}^{n} H(X_i|Z^{i-1}S^{i-1}) - H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W) \\
&\quad - I(W; X_i|Z^{i-1}S^{i-1}) \\
&\geq \sum_{i=1}^{n} H(X_i|Y^{i-1}Z^{i-1}S^{i-1}) - H(X_i|Y^{i-1}Z^{i-1}S^{i-1}W) \\
&\quad - I(X_i; W|Z^{i-1}S^{i-1}) \\
&= \sum_{i=1}^{n} I(W; X_i|Y^{i-1}Z^{i-1}S^{i-1}) - I(W; X_i|Z^{i-1}S^{i-1}) \\
&> \frac{nR_{SM}}{1-\delta\delta_E} - \frac{\epsilon}{1-\delta_E} \quad (18)
\end{aligned}$$

To get (18) we made use of our two lemmas. Now, we can put together (16)-(18) and get:

$$nR_{SM} < (1-\delta)\left(nL\log q - \frac{(1-\delta_E)nR_{SM}}{(1-\delta\delta_E)(1-\delta)\delta_E} + \right.$$
$$\left. + \frac{\epsilon}{(1-\delta)\delta_E}\right)$$

Rearranging terms gives:

$$R_{SM} < (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2} L\log q + \frac{\epsilon(1-\delta\delta_E)}{n(1-\delta\delta_E^2)} \quad (19)$$

Number ϵ can be chosen arbitrary small, so we are done. ■

Note that (19) shows that the converse is true for a weaker security condition $\frac{1}{n}I(W; Z^nS^n) < \epsilon$ as well.

Theorems 2-3 together provide the proof for Theorem 1.

REFERENCES

[1] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, 1997.

[2] A. D. Wyner, "The wire-tap channel," *The Bell system Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

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

[5] ——, "Secrecy capacities for multiterminal channels," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 2437–2452, 2008.

[6] C. Mitrpant, A. Vinck, and Y. Luo, "An achievable region for the gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181 –2190, May 2006.

[7] Y. Chen and A. H. Vinck, "Wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 395 –402, Jan. 2008.

[8] M. Jafari Siavoshani, U. K. Pulleti, C. Fragouli, A. Argyraki, and S. Diggavi, "Erased Secrets: Practical Information-Theoretic Group Secrecy," EPFL, Tech. Rep., 2010.

[9] M. Jafari Siavoshani, C. Fragouli, S. Diggavi, U. K. Pulleti, and K. Argyraki, "Group secret key generation over broadcast erasure channels," in *Asilomar Conference on Signals, Systems, and Computers*, 2010, pp. 719–723.

[10] D. P. Dubhashi and A. Panconesi, *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, 2009.