

# Lossless Compression with Security Constraints

Deniz Gündüz<sup>\*†</sup>, Elza Erkip<sup>‡\*</sup>, H. Vincent Poor<sup>\*</sup>

<sup>\*</sup>Dept. of Electrical Engineering, Princeton University, Princeton, NJ, 08544

<sup>†</sup>Dept. of Electrical Engineering, Stanford University, Stanford, CA, 94305

<sup>‡</sup>Dept. of Electrical and Computer Engineering, Polytechnic University, Brooklyn, NY, 11201

Email: {dgunduz, poor}@princeton.edu, elza@poly.edu

**Abstract**—Secure distributed data compression in the presence of an eavesdropper is explored. Two correlated sources that need to be reliably transmitted to a legitimate receiver are available at separate encoders. Noise-free, limited rate links from the encoders to the legitimate receiver, one of which can also be perfectly observed by the eavesdropper, are considered. The eavesdropper also has its own correlated observation. Inner and outer bounds on the achievable compression-equivocation rate region are given. Several different scenarios involving the side information at the transmitters as well as multiple receivers/eavesdroppers are also considered.

## I. INTRODUCTION

With the emergence of wireless sensor networks and distributed video applications, distributed source compression has become an important research area. A significant amount of effort has been devoted to understanding the information theoretic limits of distributed lossless and lossy compression and developing codes to achieve these limits. However, in many real-life applications involving distributed compression, such as distributed video surveillance or monitoring of some private information, secure compression and communication while meeting the end-to-end quality of service requirements becomes important. In this paper we consider the information theoretic limits of secure lossless source compression in the presence of an adversary who has access to some of the links in the network as well as its own correlated observation of the data to be compressed. We consider information theoretic secrecy, that is, we want to limit the information leakage to a computationally unbounded eavesdropper who has the full knowledge of the compression algorithms used.

We first consider a simplified model of the general secure distributed compression problem, composed of two transmitters Alice and Charlie with correlated observations, a receiver Bob, and an eavesdropper Eve who is interested in the data of Alice. Eve eavesdrops Alice's channel to Bob, i.e., it knows Alice's message to Bob exactly. Eve also has her own correlated side information. We consider the scenario in which both Alice's and Charlie's data need to be reconstructed at Bob reliably while Eve is interested in only Alice's information source. Later, we consider various cases involving the availability of the side information at different terminals.

This research was supported in part by the US National Science Foundation under Grants ANI-03-38807, CCF-04-30885, CCF-06-35177, CCF-07-28208, and CNS-06-25637.

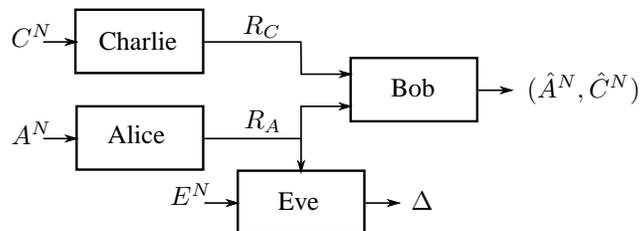


Fig. 1. Two terminal secure distributed compression. The eavesdropper (Eve) can only access one of the links.

Finally, we analyze cases with multiple receivers or multiple eavesdroppers.

In Wyner's classical wiretap channel model [1], nonzero secrecy rate can be achieved without using a secure key, if the intended receiver has a better quality communication channel than the eavesdropper. It was observed in [3] and [4] that, secrecy can also be generated through correlated observations at the legitimate users. In our model, since the channels are not noisy, the techniques of [1] do not apply; however, based on the ideas of [3], [4], it is still possible to achieve secrecy by exploiting the correlated information transmitted over secure links. Unlike [3], [4] which focus on generating secret key using correlated information sources, we impose the requirement of lossless decoding of the source sequence at the legitimate receiver while keeping Alice's information secret from Eve.

In [8], Yamamoto considers lossy compression with security constraints over a noisy broadcast channel, while the users share a secure key as well. He showed that first applying lossy source compression, then encrypting the compressed bits using the secure key and finally transmitting over the channel using a good wiretap channel code is optimal. In [5], Merhav extends this result to the case in which the legitimate receiver and the eavesdropper have correlated side information under the assumption that both the channel output and the side information at the eavesdropper are physically degraded. He shows that replacing lossy compression with Wyner-Ziv compression in the coding scheme of [8] is optimal. In [6], the minimum leakage rate in secure lossless compression with arbitrary side information is explored. It is shown in [6] that, in the case of arbitrarily correlated receiver side information, the usual Slepian-Wolf compression is not always sufficient.

Secure lossless compression of two correlated sources is considered in [7], where the eavesdropper has access to only one of the compressed bit streams and has no side information. Slepian-Wolf compression suffices in this setup due to the lack of side information at the eavesdropper.

We introduce the system model in Section II. In Section III we give inner and outer bounds to the achievable compression-equivocation rate region that generalize the well-known Slepian-Wolf region to include secrecy constraints. In Section IV we consider various different scenarios based on the availability of the side information and also considering multiple legitimate receivers or multiple eavesdroppers.

## II. SYSTEM MODEL

For the model in Fig. 1, we assume that Alice and Charlie have access to length- $N$  correlated source sequences  $A^N$  and  $C^N$ , respectively. They want to transmit these sources to Bob reliably over separate noise-free, finite capacity channels. Alice's transmission will also be perfectly received by an eavesdropper called Eve who has her own correlated side information  $E^N$ . We model  $A^N$ ,  $C^N$ , and  $E^N$  as being generated independent and identically distributed (i.i.d.) according to the joint probability distribution  $p_{ACE}(a, c, e)$  over the finite alphabet  $\mathcal{A} \times \mathcal{C} \times \mathcal{E}$ . While Alice and Charlie want to transmit their sources reliably to Bob, they also want to maximize the equivocation at Eve, which represents the uncertainty of Eve about  $A^N$  after receiving Alice's transmission and combining with her (Eve's) own side information  $E^N$ . We will also consider scenarios involving multiple legitimate receivers/eavesdroppers for which similar definitions apply. Throughout the paper we assume that all the transmissions are authenticated, i.e., the eavesdropper is passive.

An  $(M_A, M_C, N)$  code for secure source compression in this setup is composed of an encoding function<sup>1</sup> at Alice,  $f_A : \mathcal{A}^N \rightarrow I_{M_A}$ , an encoding function at Charlie,  $f_C : \mathcal{C}^N \rightarrow I_{M_C}$ , and a decoding function at Bob,  $g : I_{M_A} \times I_{M_C} \rightarrow \mathcal{A}^N \times \mathcal{C}^N$ , where  $I_k$  denotes the set  $\{1, \dots, k\}$  for  $k \in \mathbb{Z}^+$ . The equivocation rate of this code is defined as  $\frac{1}{N}H(A^N | f_A(A^N), E^N)$ , and the error probability as  $P_e^N = Pr\{g(f_A(A^N), f_C(C^N)) \neq (A^N, C^N)\}$ .

*Definition 2.1:* We say that  $(R_A, R_C, \Delta)$  is *achievable* if, for any  $\epsilon > 0$ , there exist an  $(M_A, M_C, N)$  code such that  $\log(M_A) \leq N(R_A + \epsilon)$ ,  $\log(M_C) \leq N(R_C + \epsilon)$ ,  $H(A^N | f_A(A^N), E^N) \geq N(\Delta - \epsilon)$  and  $P_e^N < \epsilon$ . Let  $\mathcal{R}$  denote the set of all achievable  $(R_A, R_C, \Delta)$  triplets.

## III. SECURE DISTRIBUTED COMPRESSION

For the model in Section II, when we remove the secrecy requirements, the problem reduces to the well-known Slepian-Wolf coding of correlated sources. However, the solution in the case of distributed compression with secrecy constraints is not a direct extension of the Slepian-Wolf theorem.

<sup>1</sup>We assume deterministic coding in the analysis for simplicity, but the proofs follow similarly for randomized coding which is modeled by assuming independent random variables at the terminals and deterministic coding functions that depend on these random variables.

*Definition 3.1:* Let  $U$  and  $V$  be two random variables jointly distributed with  $A, C$  and  $E$  and taking values over the finite alphabets  $\mathcal{U}$  and  $\mathcal{V}$ . We define  $\mathcal{P}_{in}$  as the set of  $(U, V)$  that satisfy  $H(C|A, V) = 0$  with a joint distribution of the form  $p_{ACEPU|APV|C}$ . We define  $\mathcal{P}_{out}$  as the set of  $(U, V)$  that satisfy  $H(C|A, V) = 0$  and the Markov chain conditions  $U - A - (C, E)$  and  $V - C - (A, E)$ .

*Definition 3.2:* We define  $\mathcal{R}_{in}$  as the convex hull of the set of all  $(R_A, R_C, \Delta)$  for which there exists  $(U, V) \in \mathcal{P}_{in}$  such that

$$R_C \geq I(C; V), \quad (1)$$

$$R_A \geq H(A|V), \quad (2)$$

$$\Delta \leq [I(A; V|U) - I(A; E|U)]^+, \quad (3)$$

$$\Delta \leq \min\{R_C - H(C|A), I(A; C)\} \text{ and} \quad (4)$$

$$\Delta \geq [H(A|E) - R_A]^+, \quad (5)$$

where  $[x]^+ = \max\{x, 0\}$ , and  $\mathcal{R}_{out}$  as the convex hull of the set of all  $(R_A, R_C, \Delta)$  for which there exists  $(U, V) \in \mathcal{P}_{out}$  such that (1)-(5) hold.

Our main result is the following inner and outer bounds on the set of all achievable triplets of Definition 2.1.

*Theorem 3.1:*  $\mathcal{R}_{in} \subseteq \mathcal{R} \subseteq \mathcal{R}_{out}$ .

*Proof:* The sketch of the proof is given in Appendix I. ■

When the eavesdropper has no side information, i.e.,  $E$  is constant, then the inner and outer bounds become tight. The following corollary can be obtained similar to Theorem 3.1.

*Corollary 3.2:* When there is no side information at the eavesdropper, the compression-equivocation rate region is characterized by

$$R_C \geq H(C|A),$$

$$R_A \geq H(A|C),$$

$$R_A + R_C \geq H(A, C), \text{ and}$$

$$[H(A) - R_A]^+ \leq \Delta \leq \min\{I(A; C), R_C - H(C|A)\}.$$

We skip the proof, which can also be obtained as a special case of the result in [7]. The achievability is simply from the usual Slepian-Wolf compression, that is, we let  $U$  be constant.

## IV. UNCODED SIDE INFORMATION AT BOB

A special case of Theorem 3.1 is obtained when we have  $R_C \geq H(C)$ , that is,  $C^N$  can be recovered by Bob with an arbitrarily small probability of error. Equivalently, we can assume that the side information sequence  $B^N = C^N$  is available directly to Bob. The compression-equivocation rate region for this special case is given as below, which can be obtained from Theorem 3.1.

*Corollary 4.1:* For uncoded side information  $B^N$  at Bob,  $(R_A, \Delta)$  is an achievable compression-equivocation rate pair if and only if,

$$R_A \geq H(A|B), \quad (6)$$

$$0 \leq \Delta \leq [I(A; B|U) - I(A; E|U)]^+, \text{ and} \quad (7)$$

$$R_A + \Delta \geq H(A|E), \quad (8)$$

for some  $U$  such that  $U - A - (B, E)$  form a Markov chain.

While Corollary 4.1 requires an auxiliary codebook generated by  $U$  in the general case to conceal the source from the eavesdropper, in [9] we show that, when Bob's side information  $B$  is *less noisy* [2] than Eve's side information  $E$ , Slepian-Wolf binning achieves the highest possible equivocation rate, i.e., (7) is maximized by a constant  $U$ . Furthermore, when Bob's side information is a stochastically degraded version of Eve's side information, no positive equivocation rate is achievable, and  $\Delta = 0$ .

In [9], we also show that the availability of either Bob's or Eve's side information at Alice potentially increases the equivocation rate of the eavesdropper, while the compression rate bound on  $R_A$  remains intact. When Alice does not have access to  $B^N$ ,  $\Delta = 0$  if  $B$  is independent of  $A$ . However, when  $B^N$  is available to Alice, it is useful even if they are independent. This scenario is equivalent to Shannon's secret key model, in which a secure key, independent of the message, at rate  $H(B)$  is shared by Alice and Bob.

*Lemma 4.2:* If  $B$  is independent of  $(A, E)$  and available to Alice as well, then  $(R_A, \Delta)$  is achievable if and only if

$$\begin{aligned} R_A &\geq H(A) \text{ and} \\ 0 \leq \Delta &\leq \min\{H(B), H(A|E)\}. \end{aligned}$$

*Proof:* The achievability follows by first compressing the source  $A^N$  and then encrypting the compressed source bits with the secure shared key  $B^N$ , i.e., one time pad. The converse can be obtained from Corollary 4.1. ■

Now we compare two scenarios of having Eve's side information at Alice or Bob. When  $E^N$  is available to Bob, the side information of Eve becomes physically degraded version of Bob's side information, and Slepian-Wolf compression would suffice [9]. The compression-equivocation rate region is characterized by

$$\begin{aligned} R_A &\geq H(A|B, E) \\ 0 \leq \Delta &\leq I(A; B|E) \text{ and} \\ R_A + \Delta &\geq H(A|E). \end{aligned}$$

Note that, having  $E^N$  at Bob helps decrease the compression rate bound on  $R_A$  as well. Furthermore, as shown in [9] providing  $E^N$  to Alice in addition to Bob would not help.

On the other hand, when  $E^N$  is available to Alice, the compression-equivocation rate region is given by [9]  $R_A \geq H(A|B)$ ,  $0 \leq \Delta \leq I(A; B|E)$  and  $R_A + \Delta \geq H(A|E)$ . Comparing the two regions when  $E^N$  is available to Alice or to Bob, we see that the latter requires a smaller compression rate due to a better side information at the receiver, while the equivocation rates are equal.

## V. MULTIPLE LEGITIMATE RECEIVERS/EAVESDROPPERS

Consider  $K$  legitimate receivers, each with its own correlated side information  $B_k$  for  $k = 1, \dots, K$ , that want to receive Alice's information reliably, while there is only one eavesdropper Eve. In the absence of an eavesdropper, a rate of  $\max_k H(A|B_k)$  is necessary and sufficient for simultaneous reliable transmission to all the receivers [11].

From Corollary 4.1, considering each receiver separately, the equivocation rate is bounded as  $\Delta \leq \max\{H(A|E, U_k) - H(A|B_k, U_k)\}$  where the maximization is over  $U_k$  satisfying the Markov chain  $U_k - A - (B_k, E)$  for  $k = 1, \dots, K$ . The minimum of these individual equivocation rate bounds serves as an upper bound; however, achievability of it together with  $R_A \geq \max_k H(A|B_k)$  does not follow directly. The achievability proof outlined in Appendix I requires an auxiliary codeword to be decoded by the receiver. However, for multiple receivers, the auxiliary codebook  $U_k$  that maximizes the equivocation rate for one of the users, might not be decodable by another user. Imposing such a decoding constraint requires a total transmission rate of  $\max_k I(A; U_k|B_k) + \max_k H(A|B_k, U_k)$ , which might be greater than  $\max_k H(A|B_k)$ , the required rate without the secrecy constraint.

Below, we give the compression-equivocation rate region in case of multiple receivers for two special cases. Proofs are omitted due to space limitation.

*Corollary 5.1:* If  $A - B_k - E$  form a Markov chain for all  $k = 1, \dots, K$ , then  $(R_A, \Delta)$  is achievable if and only if,

$$\begin{aligned} R_A &\geq \max_k H(A|B_k), \\ \Delta &\leq \min_k \{H(A|E) - H(A|B_k)\}, \text{ and} \\ R_A + \Delta &\geq H(A|E). \end{aligned}$$

*Corollary 5.2:* If  $A - B_1 - \dots - B_K$  form a Markov chain, then  $(R_A, \Delta)$  is achievable if and only if,

$$\begin{aligned} R_A &\geq H(A|B_K), \\ \Delta &\leq \max\{I(A, B_K|U) - I(A; E|U)\}, \text{ and} \\ R_A + \Delta &\geq H(A|E), \end{aligned}$$

where the maximization is over auxiliary random variables  $U$  such that  $U - A - (B_1, \dots, B_K, E)$  form a Markov chain.

In Corollary 5.1, due to the degradedness of  $E$  with respect to  $B_k$ 's, picking a constant  $U$  is optimal for all receivers. In Corollary 5.2, we use the auxiliary codebook  $U$  that is chosen with respect to the worst receiver side information  $B_K$ .

Similarly, there may be multiple non-cooperating eavesdroppers all of which have their own correlated side information. Suppose there are  $K$  eavesdroppers, the  $k$ -th of which has side information  $E_k$ . We have  $K$  equivocation rates defined as

$$\Delta_k \triangleq \frac{H(A^N | f_A(A^N), E_k^N)}{N} \text{ for } k = 1, \dots, K.$$

This time, we pick the auxiliary codebook that simultaneously achieves the corresponding equivocation rates  $\Delta_k$ .

*Corollary 5.3:*  $(R, \Delta)$  is achievable for the multiple eavesdropper scenario if and only if,

$$\begin{aligned} R_A &\geq H(A|B), \\ \Delta_k &\leq [H(A|E_k, U) - H(A|B, U)]^+, \text{ and} \\ R_A + \Delta_k &\geq H(A|E_k), \end{aligned}$$

for  $k = 1, \dots, K$  for some auxiliary random variable satisfying the Markov chain condition  $U - A - (B, E_1, \dots, E_K)$ .

## VI. CONCLUSION

In this paper, we have considered secure distributed compression in the presence of an eavesdropper. We have studied the case in which one of the transmitters is wire-tapped by an eavesdropper and we have shown that secure communication can be achieved with the help of the second transmitter who has its own correlated side information and a secure link to the legitimate receiver. We have provided inner and outer bounds to the compression-equivocation rate region for the model studied. We have also considered availability of side information at the transmitters, multiple legitimate receivers or multiple eavesdroppers. Future directions include extension to the lossy compression scenario.

### APPENDIX I PROOF OF THEOREM 3.1

*Inner bound:* We fix  $p(u|a)$  and  $p(v|c)$  satisfying the conditions in the theorem. Then we generate  $2^{N(I(A;U)+\epsilon_1)}$  independent codewords of length  $N$ ,  $U^N(w_1)$ ,  $w_1 \in \{1, \dots, 2^{N(I(A;U)+\epsilon_1)}\}$ , with distribution  $\prod_{i=1}^N p(u_i)$ . We randomly bin all  $U^N(w_1)$  sequences into  $2^{N(I(A;U|V)+\epsilon_2)}$  bins, calling them the auxiliary bins. For each codeword  $U^N(w_1)$ , we denote the corresponding auxiliary bin index as  $a(w_1)$ . On the other hand, we randomly bin all  $A^N$  sequences into  $2^{N(H(A|V,U)+\epsilon_3)}$  bins, calling them the source bins, and denote the corresponding bin index as  $s(A^N)$ . We also generate  $2^{N(I(C;V)+\epsilon_4)}$  independent codewords  $V^N(w_2)$  of length  $N$ ,  $w_2 \in \{1, \dots, 2^{N(I(C;V)+\epsilon_4)}\}$ , with distribution  $\prod_{i=1}^N p(v_i)$ .

For each typical outcome of  $A^N$ , Alice finds a jointly typical  $U^N(w_1)$ . Then she reveals  $a(w_1)$ , the auxiliary bin index of  $U^N(w_1)$ , and  $s(A^N)$ , the source bin index of  $A^N$ , to both Bob and Eve; that is, the encoding function  $f_A$  of Alice is composed of the pair  $(a(w_1), s(A^N))$ . Using standard techniques, it is possible to show that we have such a unique index pair with high probability. Charlie observes the outcome of its source  $C^N$ , finds a jointly typical  $V^N(w_2)$  with  $C^N$ , and sends the index  $w_2$  of  $V^N$  over the private channel to Bob. With high probability there will be a unique  $w_2$  such that  $C^N$  and  $V^N(w_2)$  are jointly typical.

Bob, having access to  $w_2$  and the auxiliary bin index  $a(w_1)$ , can find the jointly typical  $U^N(w_1)$  correctly with high probability. Then using  $U^N$ , the source bin index  $s(A^N)$  and  $V^N(w_2)$ , Bob can reliably decode  $A^N$ . Since  $H(C|A, V) = 0$ , knowing  $A^N$  and  $V^N$  correctly, Bob can find the correct  $C^N$  with high probability as well. Letting  $\epsilon_i \rightarrow 0$  for  $i = 1, 2, 3$  and 4, we can make the total communication rate of Alice arbitrarily close to  $I(A; U|V) + H(A|U, V) = H(A|V)$  and the rate of Charlie to  $I(C; V)$ . Since (1)-(2) hold, these rates can be communicated to Bob while having arbitrarily small error probability for sufficiently large  $N$ .

The equivocation rate can be lower bounded as follow:

$$\begin{aligned} H(A^N | a(w_1), s(A^N), E^N) &= H(A^N) - I(A^N; a(w_1), E^N) \\ &\quad - I(A^N; s(A^N) | E^N, a(w_1)) \\ &\geq H(A^N) - I(A^N; U^N, E^N) - H(s(A^N)) \end{aligned} \quad (9)$$

$$\begin{aligned} &\geq H(A^N | U^N, E^N) - NH(A|V, U) - N\epsilon_3 \quad (10) \\ &= N[H(A|U, E) - H(A|V, U) - \epsilon_3] \\ &= N[I(A; V|U) - I(A; E|U) - \epsilon_3], \end{aligned}$$

where (9) follows from the data processing inequality; and (10) follows from the fact that  $s(A^N)$  is a random variable over a set of size  $2^{N(H(A|V,U)+\epsilon_3)}$ .

For  $(U, V) \in \mathcal{P}_{in}$ , we can show that

$$\begin{aligned} I(A; V|U) - I(A; E|U) &\leq I(A; C) \text{ and} \\ I(A; V|U) - I(A; E|U) &\leq R_C - H(C|A) \end{aligned}$$

Hence (4) is not active in the inner bound.

Finally, we also have

$$\begin{aligned} &\frac{1}{N} H(A^N | a(w_1), s(A^N), E^N) \\ &= \frac{1}{N} [H(A^N | E^N) - I(A^N; a(w_1), s(A^N) | E^N)] \\ &\geq H(A|E) - \frac{1}{N} H(a(w_1), s(A^N)) \\ &\geq H(A|E) - R_A. \end{aligned}$$

*Outer bound:* We define

$$J \triangleq f_A(A^N) \text{ and } K \triangleq f_C(C^N).$$

From Fano's inequality, we have

$$H(A^N, C^N | J, K) \leq N\delta(P_e^N), \quad (11)$$

where  $\delta(\cdot)$  is a non-negative function with  $\lim_{x \rightarrow 0} \delta(x) = 0$ .

Define  $U_i \triangleq (J, A^{i-1}, E^{i-1})$  and  $V_i \triangleq (K, C^{i-1})$ . Note that both  $U_i - A_i - (C_i, E_i)$  and  $V_i - C_i - (A_i, E_i)$  form Markov chains. Then, we have the following chain of inequalities:

$$\begin{aligned} NR_C &\geq H(K) \\ &\geq I(C^N; K) \\ &= \sum_{i=1}^N I(C_i; K | C^{i-1}) \end{aligned} \quad (12)$$

$$= \sum_{i=1}^N I(C_i; K, C^{i-1}) = \sum_{i=1}^N I(C_i; V_i), \quad (13)$$

where (12) follows from the chain rule. We also have

$$\begin{aligned} NR_A &\geq H(J) \geq H(J|K) \\ &= H(A^N, J|K) - H(A^N|J, K) \\ &\geq H(A^N|K) - N\delta(P_e^N) \end{aligned} \quad (14)$$

$$\geq \sum_{i=1}^N H(A_i|K, A^{i-1}, C^{i-1}) - N\delta(P_e^N) \quad (15)$$

$$= \sum_{i=1}^N H(A_i|K, C^{i-1}) - N\epsilon \quad (16)$$

$$= \sum_{i=1}^N H(A_i|V_i) - N\delta(P_e^N), \quad (17)$$

where (14) follows from (11) and the nonnegativity of entropy; (15) follows as  $A_i - (K, A^{i-1}) - C^{i-1}$  form a Markov chain; and (16) follows as  $A_i - (K, C^{i-1}) - A^{i-1}$  form a Markov chain.

Next, we have the following set of inequalities:

$$N\delta(P_e^N) \geq H(C^N|J, K) \quad (18)$$

$$\geq H(C^N|A^N, K) \quad (19)$$

$$= \sum_{i=1}^N H(C_i|A_i, K, C^{i-1}) \quad (20)$$

$$= \sum_{i=1}^N H(C_i|A_i, V_i), \quad (21)$$

where (18) follows from (11); (19) follows since conditioning reduces entropy and  $J$  is a function of  $A^N$ ; and (21) follows from the definition of  $V_i$ .

For the equivocation rate converse, we have

$$\begin{aligned} N\Delta &= H(A^N|J, E^N) \\ &= H(A^N|J) - I(A^N; E^N|J) \\ &= H(A^N|J, K) + I(A^N; K|J) - I(A^N; E^N|J) \\ &\leq N\delta(P_e^N) + \sum_{i=1}^N I(A_i; K|J, A^{i-1}) - \sum_{i=1}^N H(E_i|J, E^{i-1}) \\ &\quad + H(E^N|A^N, J) \end{aligned} \quad (22)$$

$$\begin{aligned} &\leq N\delta(P_e^N) + \sum_{i=1}^N I(A_i; K|J, A^{i-1}, E^{i-1}) \\ &\quad - \sum_{i=1}^N H(E_i|J, E^{i-1}, A^{i-1}) + H(E^N|A^N) \end{aligned} \quad (23)$$

$$\begin{aligned} &\leq N\delta(P_e^N) + \sum_{i=1}^N [I(A_i; K, C^{i-1}|J, A^{i-1}, E^{i-1}) \\ &\quad - H(E_i|J, E^{i-1}, A^{i-1}) + H(E_i|A_i)] \end{aligned} \quad (24)$$

$$= \sum_{i=1}^N [I(A_i; V_i|U_i) - H(E_i|U_i) + H(E_i|A_i)] + N\delta(P_e^N) \quad (25)$$

$$= \sum_{i=1}^N [I(A_i; V_i|U_i) - I(A_i; E_i|U_i)] + N\delta(P_e^N) \quad (26)$$

where (22) follows from Fano's inequality and the chain rule; (23) follows from the memoryless property of the source and the side information sequences, and the fact that conditioning reduces entropy; (24) follows from the chain rule and the non-negativity of the mutual information; (25) follows from definitions of  $V_i$  and  $U_i$ ; and finally (26) follows since  $U_i - A_i - E_i$  form a Markov chain.

We also have

$$\begin{aligned} N\delta(P_e^N) &\geq H(A^N, C^N|J, K) \quad (27) \\ &= H(J, K|A^N, C^N) + H(A^N, C^N) - H(J, K) \\ &\geq H(A^N) + H(C^N) - I(A^N; C^N) - H(J) - H(K) \\ &= H(A^N|J) - H(J|A^N) + NH(C|A) - H(K) \\ &\geq H(A^N|J, E^N) + NH(C|A) - NR_C \end{aligned}$$

where (27) follows from (11). We get

$$\delta(P_e^N) \geq \Delta + H(C|A) - R_C, \quad (28)$$

and

$$\begin{aligned} N\delta(P_e^N) &\geq H(A^N, C^N|J, K) \\ &= H(A^N, C^N) - I(A^N, C^N; J, K) \\ &= H(A^N, C^N) - H(A^N) + H(A^N|J) - H(C^N) \\ &\quad + H(C^N|K) + I(K; J) \\ &\geq H(A^N|J, E^N) - I(A^N; C^N) \\ &\geq N\Delta - NI(A; C). \end{aligned}$$

And finally we have

$$\begin{aligned} H(A|E) &\leq \frac{1}{N} H(A^N, J|E^N) \\ &= \frac{1}{N} [H(J|E^N) + H(A^N|E^N, J)] \\ &\leq \frac{H(J)}{N} + \Delta \\ &\leq R_A + \Delta. \end{aligned} \quad (29)$$

Now, we define a new independent random variable  $Q$  uniformly distributed over the set  $\{1, 2, \dots, N\}$ , and  $A \triangleq A_Q$ ,  $E \triangleq E_Q$ ,  $V \triangleq (V_Q, Q)$ , and  $U \triangleq (U_Q, Q)$ . Letting  $N \rightarrow \infty$  and  $P_e^N \rightarrow 0$  we obtain the outer bound in the theorem.

## REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339-348, May 1978.
- [3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part 1: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, July 1993.
- [4] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol.39, no.3, pp.734-742, May 1993.
- [5] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," submitted to *IEEE Trans. Inf. Theory*.
- [6] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," *Proc. IEEE Inf. Theory Workshop*, Lake Tahoe, CA, Sept. 2007.
- [7] W. Luh and D. Kundur, "Separate enciphering of correlated messages for confidentiality in distributed networks," *Proc. IEEE Global Comm. Conf.*, Washington, D.C., Nov. 2007.
- [8] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827-835, May 1997.
- [9] D. Gündüz, E. Erkip and H. V. Poor, "Secure lossless compression with side information," *Proc. IEEE Info. Theory Workshop*, Porto, Portugal, June 2008.
- [10] J. Körner and K. Marton, "A source network problem involving the comparison of two channels," *Trans. Colloq. Inf. Theory*, Keszthely, Hungary, Aug. 1975.
- [11] A. Sgarro, "Source coding with side information at several decoders," *IEEE Trans. Inf. Theory*, vol. 23, pp. 179-182, March 1977.