Special Section Correspondence

Distributed Secret Sharing for Discrete Memoryless Networks

William Luh and Deepa Kundur

***Abstract*—This correspondence studies the distributed secret sharing problem which is a twist of the classical secret sharing problem. In this new problem, each user needs to encode his or her own unique secret message without collaboration with other users and without the use of any common secret materials or cryptographic keys. The goal is to ensure that an adversary without access to all of the encoded messages learns as little as possible about the secret messages, while a legitimate joint decoder with all the encoded messages can decode all of them without cryptographic keys. Furthermore the users do not know the channels that will be compromised ahead of time, and thus must protect all channels. Specifically, we study two related variants of this problem. The first problem deals with source coding and secrecy, while the second problem deals with channel coding and secrecy. From the results of these two problems, we conclude that interference is necessary for unconditional secrecy.**

***Index Terms*—Information–theoretic cryptography, secret sharing, wiretap channel.**

I. Introduction

This correspondence considers a twist on the classical secret sharing problem. The challenges in this twist are that we introduce multiple encoding entities, which we call users, each of whom must encode a different (possibly correlated) secret message without collaborating with one another and without using any common secret materials, such as cryptographic keys. As such, encoding is not performed jointly but rather in a distributed manner which is suitable for a distributed network scenario.

In this correspondence, we present theoretical results that outline the fundamental possibilities and impossibilities for different scenarios. In particular, we study two variants of the problem. The first variation is a multiterminal source coding (MSC) problem with secrecy constraints, while the second problem is an interference coding problem with joint decoding and an unconditional secrecy constraint. In both variations, an eavesdropper is permitted to intercept only a proper subset of signals received by the joint decoder.

A. Prior and Related Works

As mentioned in Section I, the first problem variation studied in this correspondence utilizes techniques from MSC [1]. More recent works dealing with secrecy and source coding include [2] and [3].

Our second problem variation uses techniques from wiretap channel theory. The proof techniques encountered in this correspondence are standard in the wiretap channel repertoire. More recent wiretap channels that are related to our work include [4]–[7].

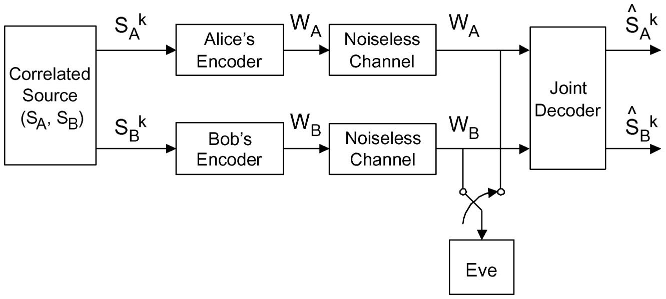

Fig. 1. Distributed source coding for secrecy with the distortion criteria model.

In all of the wiretap channels mentioned before, the particular channel that the wiretapper is exploiting is fixed and known ahead of time to the encoders. In our work, any of the legitimate channels may become a wiretap channel, and the specific channel that will be exploited by the adversary is unknown to the encoders. A second major difference is that in each of the wiretap channels mentioned before, there is at least one legitimate channel that is known to be unexploited. In our work, any of the legitimate channels may become a wiretap channel since it is not known which channels are exploited and which are unexploited.

II. Problem Formulation

This correspondence consists of two similar and related problems corresponding to a negative and positive result regarding distributed secret sharing. The negative result deals with source coding with distortion criteria and the positive result deals with channel coding with interference and joint decoding.

A. Distributed Source Coding for Secrecy With Distortion Criteria

Fig. 1 summarizes the source-coding-only (negative) aspect of our problem. Let $S_A^k \in \mathcal{S}_A^k$ and $S_B^k \in \mathcal{S}_B^k$ denote Alice's and Bob's messages, respectively. Alice's and Bob's messages are generated by a joint discrete memoryless source (DMS) given by (1)

$$P_{S_A,S_B}^k\left(s_A^k, s_B^k\right) = \prod_{i=1}^{k} P_{S_A,S_B}(s_{A,i}, s_{B,i}). \qquad (1)$$

Alice and Bob are to encipher their S_A^k, S_B^k separately without cooperation, creating $W_A \in \mathcal{W}_A$ and $W_B \in \mathcal{W}_B$, respectively, where $\mathcal{W}_A, \mathcal{W}_B$ are finite sets.

The joint decoder receives W_A and W_B, and its goal is to reconstruct S_A^k and S_B^k within some fidelity criteria that will be discussed. Let the quadruple $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$ denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the decoders to reconstruct Alice's and Bob's messages, respectively. Here, $f_A^k : \mathcal{S}_A^k \to \mathcal{W}_A$, $f_B^k : \mathcal{S}_B^k \to \mathcal{W}_B$, $\varphi_A^k : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}_A^k$, and $\varphi_B^k : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}_B^k$, where $\hat{\mathcal{S}}_A^k$ and $\hat{\mathcal{S}}_B^k$ are the finite reconstruction alphabets for Alice and Bob, respectively.

Let $\rho_j^k : \mathcal{S}_j^k \times \hat{\mathcal{S}}_j^k \to \mathbb{R}^+$ be the block distortion measure between j's (e.g., $j = A$ for Alice and $j = B$ for Bob) original message block s_j^k and the decoder's reconstruction $\hat{s}_j^k$. The block distortion measures

Manuscript received October 15, 2007; revised May 22, 2008. First published July 25, 2008; last published August 13, 2008 (projected).The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Christina Fragouli.

The authors are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: luh@ece.tamu.edu; wluh@ieee.org; deepa@ece.tamu.edu).

Digital Object Identifier 10.1109/TIFS.2008.927422

are defined by single-letter distortion measures $\rho_j : \mathcal{S}_j \times \hat{\mathcal{S}}_j \to \mathbb{R}^+$ for $j = A, B$ as in (2)

$$\rho_j^k\left(s_j^k, \hat{s}_j^k\right) = \frac{1}{k}\sum_{i=1}^{k} \rho_j(s_{j,i}, \hat{s}_{j,i}), \quad j = A, B. \tag{2}$$

The distortion pair (D_A, D_B) is achieved if for $j = A, B$

$$\mathbb{E}\left[\rho_j^k\left(S_j^k, \hat{S}_j^k\right)\right] \leq D_j + \epsilon. \tag{3}$$

The (source coding) rates of Alice's and Bob's enciphered messages are defined for $j = A, B$ as

$$R_j \triangleq \frac{\log_2 |\mathcal{W}_j|}{k}. \tag{4}$$

In Fig. 1, the eavesdropper, referred to as Eve, is allowed to select either W_A or W_B, but not both. To justify our definition of secrecy, we require $H(S_A) = H(S_B)$, which would likely be the case if Alice and Bob were sensing the same phenomenon in the same physical space. Depending on which enciphered message Eve selects, the equivocation rates of Eve w.r.t. Alice and Bob are defined for $j = A, B$ as

$$\Delta_j \triangleq \frac{H\left(S_j^k | W_j\right)}{k}. \tag{5}$$

A stronger definition of secrecy would be to replace the numerators in (5) for $j = A, B$ with $H(S_A^k, S_B^k | W_j)$; however, (5) is defined to simplify the model and can be justified as follows. Assume Eve intercepts W_A, then $S_B^k \leftrightarrow S_A^k \leftrightarrow W_A$ forms a Markov chain and using the data-processing inequality, we can show $H(S_A^k|W_A) \leq H(S_B^k|W_A)$, which means that Eve learns less about S_B^k than she does of S_A^k. The desired unconditional secrecy under our secrecy definition occurs when

$$\Delta_j \geq H(S_j) - \epsilon \tag{6}$$

for $j = A, B$ and an arbitrarily small $\epsilon > 0$, which we can also show, implies the stronger $H(S_A^k, S_B^k | W_j)/k \geq H(S_A, S_B) - \epsilon$.

Definition 1: A quadruple (d_A, d_B, r_A, r_B) corresponding to $(\Delta_A, \Delta_B, R_A, R_B)$ is achievable w.r.t (D_A, D_B) if a sequence of encoders and decoders exists $(f_A^k, f_B^k, \varphi_A^k, \varphi_B^k)$ such that as $k \to \infty$

$$R_j \leq r_j + \epsilon \tag{7}$$

$$d_j - \epsilon \leq \Delta_j \leq d_j \tag{8}$$

for $j = A, B$ and $\epsilon > 0$ are arbitrarily small and (3) for $j = A, B$ is also satisfied. In addition, all parties—Alice, Bob, and Eve—have complete knowledge of f_A^k, f_B^k.

B. Discrete Memoryless Wiretap Channel with Interference and Joint Decoding

In the previous problem formulation, the channels are noiseless, which means that the encoded messages never mix as they are transmitted to the joint decoder. In contrast, the problem formulated here allows the encoded messages to mix via interference. Fig. 2 summarizes our second problem.

Alice and Bob each process independent and uniformly distributed messages $W_A \in \mathcal{W}_A$ and $W_B \in \mathcal{W}_B$, respectively, such that $\mathcal{W}_A, \mathcal{W}_B$ are finite sets. These messages may actually be generated from the distributed source coding for secrecy described in the previous section. Let the triple (f_A, f_B, φ) denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the decoder. Here, $f_A : \mathcal{W}_A \to \mathcal{X}_A^n$, $f_B : \mathcal{W}_B \to \mathcal{X}_B^n$, and $\varphi : \tilde{\mathcal{Y}}_A^n \times \tilde{\mathcal{Y}}_B^n \to \hat{\mathcal{W}}_A \times \hat{\mathcal{W}}_B$.

The channel coding rates are defined for $i = 1,2$ by

$$R_i \triangleq \frac{\log_2 |\mathcal{W}_i|}{n} \tag{9}$$

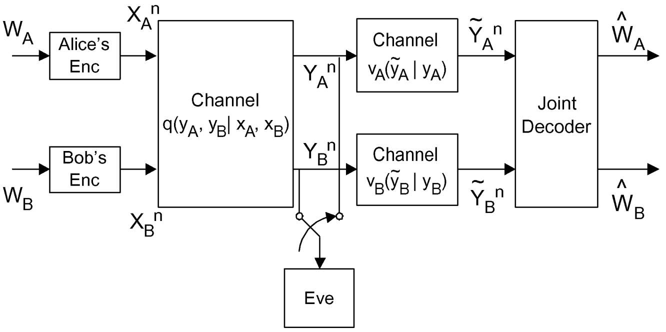

Fig. 2. Discrete memoryless wiretap channel with interference and joint decoding model.

corresponding to the encoders f_A, f_B. We use subscripts 1 and 2 to distinguish this from the source coding rates in (4). For this problem, we are only interested in rates that achieve unconditional secrecy (maximum equivocation), as we shall see this is possible.

Definition 2: A pair (r_1, r_2) corresponding to (R_1, R_2) is achievable if encoders and decoders (f_A, f_B, φ) exist such that as $n \to \infty$

$$R_i > r_i - \epsilon \tag{10}$$

$$\frac{H\left(W_A, W_B | Y_i^n\right)}{n} > R_1 + R_2 - \epsilon \tag{11}$$

$$P_e^{(n)} < \epsilon \tag{12}$$

for $i = A, B$ and $\epsilon > 0$ is arbitrarily small, where

$$P_e^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \cdot \sum_{(w_1,w_2)\in\mathcal{W}_1\times\mathcal{W}_2} \Pr\left\{(\hat{W}_1, \hat{W}_2) \neq (w_1, w_2) | (w_1, w_2)\text{sent}\right\}. \tag{13}$$

In addition, all parties—Alice, Bob, and Eve—have complete knowledge of f_A, f_B (except for any locally generated randomness).

Note that the definition of secrecy and unconditional secrecy here is the standard one. We cannot use the simplification of the first problem because the Markov chain property is destroyed by the interference.

III. Main Results

A. Results for Distributed Source Coding for Secrecy With Distortion Criteria

The capacity region $\mathcal{R}(D_A, D_B)$ is defined to be the set of all quadruples (d_A, d_B, r_A, r_B) that are achievable w.r.t to the distortion criteria (D_A, D_B). Outer and inner regions $\mathcal{R}_{\text{out}}(D_A, D_B)$ and $\mathcal{R}_{\text{in}}(D_A, D_B)$ are defined to be sets such that $\mathcal{R}_{\text{in}}(D_A, D_B) \subseteq \mathcal{R}(D_A, D_B) \subseteq \mathcal{R}_{\text{out}}(D_A, D_B)$. Generally, $\mathcal{R}_{\text{in}}(D_A, D_B) \neq \mathcal{R}_{\text{out}}(D_A, D_B)$ due to the existing gap between the outer and inner regions for the MSC problem [1]. However, in some special cases, the inner and outer regions converge.

Definition 3: Define $\mathcal{P}(D_A, D_B)$ as the set of auxiliary random variables (Q_A, Q_B) jointly distributed with (S_A, S_B) such that:

1) $Q_A \leftrightarrow S_A \leftrightarrow S_B$ and $S_A \leftrightarrow S_B \leftrightarrow Q_B$;
2) functions $F_A : \mathcal{Q}_A \times \mathcal{Q}_B \to \hat{\mathcal{S}}_A$ and $F_B : \mathcal{Q}_A \times \mathcal{Q}_B \to \hat{\mathcal{S}}_B$ exist such that for $j = A, B$

$$\mathbb{E}\left[\rho_j(S_j, \hat{S}_j)\right] \leq D_j \text{ where } \hat{S}_j = F_j(Q_A, Q_B). \tag{14}$$

Theorem 1 (Outer Region): For a fixed $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$, define $\mathcal{R}_o(Q_A, Q_B)$ to be the set of all (d_A, d_B, r_A, r_B) that satisfy

$$0 \le d_A \le H(S_A) \tag{15}$$
$$0 \le d_B \le H(S_B) \tag{16}$$
$$d_A + d_B \le H(S_A) + H(S_B) - I(S_A, S_B; Q_A, Q_B) \tag{17}$$
$$r_A \ge I(Q_A; S_A, S_B | Q_B) \tag{18}$$
$$r_B \ge I(Q_B; S_A, S_B | Q_A) \tag{19}$$
$$r_A + r_B \ge I(S_A, S_B; Q_A, Q_B) \tag{20}$$
$$r_A + d_A \ge H(S_A) \tag{21}$$
$$r_B + d_B \ge H(S_B). \tag{22}$$

Then

$$\mathcal{R}_{\text{out}}(D_A, D_B) \triangleq \bigcup_{(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)} \mathcal{R}_o(Q_A, Q_B)$$

is an outer region.

Theorem 1 is proved in [8].

Theorem 2 (Inner Region): For a fixed $(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)$, define $\mathcal{R}_i(Q_A, Q_B)$ to be the set of all (d_A, d_B, r_A, r_B) that satisfy

$$0 \le d_A \le H(S_A) \tag{23}$$
$$0 \le d_B \le H(S_B) \tag{24}$$
$$\begin{aligned} d_A + d_B \le\, & I(S_A; S_B) + H(S_A | S_B, Q_A) \\ & + H(S_B | S_A, Q_B) \end{aligned} \tag{25}$$
$$r_A \ge I(S_A; S_B, Q_A | Q_B) \tag{26}$$
$$r_B \ge I(S_B; S_A, Q_B | Q_A) \tag{27}$$
$$\begin{aligned} r_A + r_B \ge\, & H(S_A, S_B) - H(S_A | S_B, Q_A) \\ & - H(S_B | S_A, Q_B). \end{aligned} \tag{28}$$

Then

$$\mathcal{R}_{\text{in}}(D_A, D_B) \triangleq \bigcup_{(Q_A, Q_B) \in \mathcal{P}(D_A, D_B)} \mathcal{R}_i(Q_A, Q_B)$$

is an inner region.

Theorem 2 is proved in Appendix A, which is a simpler version of the one found in [8].

B. Results for Discrete Memoryless Wiretap Channel With Interference and Joint Decoding

Similar to the previous negative results, we derive sufficiency and necessity theorems. The outer region is now denoted $\mathcal{C}_{\text{out}}$ while the inner region is denoted by $\mathcal{C}_{\text{in}}$.

Theorem 3 (Outer Region): Let $\mathcal{C}_{\text{out}}$ be the set of (r_1, r_2) that satisfy (29), as shown in the equation at the bottom of the page, where the distribution factors are

$$\begin{aligned} P_{J, V_A, V_B, X_A, X_B, Y_A, Y_B, \tilde{Y}_A, \tilde{Y}_B} = \, & P_J P_{V_A | J} P_{V_B | J} \\ & \cdot P_{X_A | V_A} P_{X_B | V_B} P_{Y_A, Y_B | X_A, X_B} P_{\tilde{Y}_A | Y_A} P_{\tilde{Y}_B | Y_B}. \end{aligned} \tag{30}$$

Then, $\mathcal{C}_{\text{out}}$ is an outer region.

Theorem 3 is proven in Appendix B and uses standard wiretap channel proof techniques such as in [4]–[7].

Theorem 4 (Inner Region): For a fixed $P_{J, V_A, V_B, X_A, X_B}$ factored as

$$P_{J, V_A, V_B, X_A, X_B} = P_J P_{V_A | J} P_{V_B | J} P_{X_A | V_A} P_{X_B | V_B} \tag{31}$$

where $\mathcal{C}_{\text{inner}}(P_{J, V_A, V_B, X_A, X_B})$ is defined as the set of all (r_1, r_2) such that

$$r_1 = |\bar{R}_1 - U_1|^+ \tag{32}$$
$$r_2 = |\bar{R}_2 - U_2|^+ \tag{33}$$
$$r_1 + r_2 < I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B | J) - I(V_A, V_B; Y_i | J) \tag{34}$$

and

$$0 < U_1 < I(V_A; Y_i | V_B, J) \tag{35}$$
$$0 < U_2 < I(V_B; Y_i | V_A, J) \tag{36}$$
$$I(V_A, V_B; Y_i | J) - \epsilon < U_1 + U_2 < I(V_A, V_B; Y_i | J) \tag{37}$$
$$0 < \bar{R}_1 < I(V_A; Y_A, Y_B | V_B, J) \tag{38}$$
$$0 < \bar{R}_2 < I(V_B; Y_A, Y_B | V_A, J) \tag{39}$$
$$0 < \bar{R}_1 + \bar{R}_2 < I(V_A, V_B; Y_A, Y_B | J) \tag{40}$$

for $i = A, B$. Then

$$\mathcal{C}_{\text{in}} \triangleq \bigcup_{P_{J, V_A, V_B, X_A, X_B}} \mathcal{C}_{\text{inner}}\left(P_{J, V_A, V_B, X_A, X_B}\right) \tag{41}$$

where the distributions factor as in (31) is an inner region.

Theorem 4 is proved in Appendix C and uses standard wiretap channel proof techniques, such as in [4]–[7].

IV. Discussion and Interpretation

A. Distributed Source Coding for Secrecy With Distortion Criteria

From Theorems 1 and 2, we can conclude that unconditional secrecy is impossible. Also, in general, the outer and inner regions do not match. The capacity region is a 4-D hyper-polygon for each (D_A, D_B). Since we are interested in the amount of equivocation (secrecy) that is achievable, Fig. 3 depicts a 2-D projection of the general hyper-polygon onto the variables of interest Δ_A, Δ_B; the polygons are the achievable equivocation rates for Alice and Bob parametrized by their source coding rates R_A, R_B (this relation is not shown in Fig. 3) for various cases.

The worst case (corresponding to the smallest triangle region) occurs when Alice and Bob process different (but correlated) messages under a zero-distortion criterion (i.e., the joint decoder is required to reconstruct each of Alice's and Bob's messages S_A^k, S_B^k perfectly). Neither Alice nor Bob can achieve unconditional secrecy since the diagonal line corresponds to $d_A + d_B = I(S_A, S_B)$, which is strictly less than $H(S_i)$ for $i = A, B$ required for unconditional secrecy [cf. (6)]. Also, the less correlated S_A^k, S_B^k is, the smaller the equivocation rate region is. Note that Alice and Bob can achieve the diagonal

$$r_1 + r_2 \le \min \left\{ \begin{array}{c} \max_{J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B) \leftrightarrow (\tilde{Y}_A, \tilde{Y}_B)} I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B | J) - I(V_A, V_B; \tilde{Y}_A | J), \\ \max_{J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B) \leftrightarrow (\tilde{Y}_A, \tilde{Y}_B)} I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B | J) - I(V_A, V_B; \tilde{Y}_B | J), \\ \max_{J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B)} I(V_A, V_B; Y_A, Y_B | J) - I(V_A, V_B; Y_A | J), \\ \max_{J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B)} I(V_A, V_B; Y_A, Y_B | J) - I(V_A, V_B; Y_B | J) \end{array} \right\} \tag{29}$$

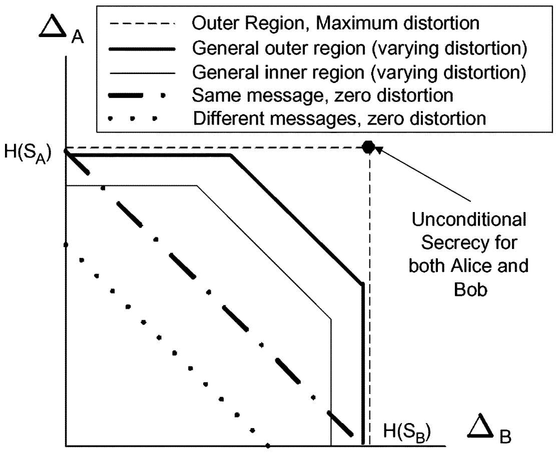

Fig. 3. Equivication rate regions.

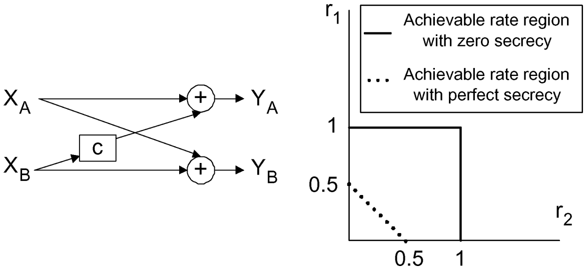
X_A
X_B
c
Y_A
Y_B
r_1
Achievable rate region with zero secrecy
Achievable rate region with perfect secrecy
1
0.5
r_2
0.5
1

Fig. 4. (a) Binary erasure wiretap channel. (b) Comparison of achievable rate regions.

line $d_A + d_B = I(S_A, S_B)$ simply by applying Slepian–Wolf source coding.

Under a zero-distortion criterion, when the correlation is "perfect" in the sense that Alice and Bob are processing the same message (i.e., $S_A^k = S_B^k$), the corresponding equivocation rate region is the largest triangular region. In this case, Alice or Bob may achieve unconditional secrecy, but not simultaneously [e.g., if Alice achieves unconditional secrecy, then Bob has no secrecy (zero equivocation)].

Whereas in the aforementioned two zero-distortion cases, the inner and outer regions match, in general, given nonzero distortion criteria, the inner region does not match the outer region. By allowing distortion upon decoding at the joint decoder, the equivocation rate region becomes a pentagon, with the inner region's smaller pentagon becoming a subset of the outer region's larger pentagon. Increasing distortion increases the vertical and horizontal lines in the pentagon, while reducing the length of the diagonal line.

When the distortion is maximal, the outer region pentagon degenerates (i.e., diagonal disappears) to the square in which case the desired maximum equivocation for Alice and Bob (i.e., unconditional secrecy) is included in the outer region. This shows that unconditional secrecy may be achieved only when the distortion is maximal, which implies nothing useful is sent from Alice and Bob. However, for the inner region when the distortion is maximal, the inner region pentagon does not degenerate to the square. Since the inner region was constructed by source coding alone (as in the aforementioned two zero-distortion cases), we can also conclude that in the general distortion-varying case, it may be possible to do better in terms of secrecy than simply source coding via the MSC described in [1].

B. Discrete Memoryless Wiretap Channel With Interference and Joint Decoding

Theorem 3 suggests there may be (since the result is an outer region) rates that achieve unconditional secrecy. From Theorem 4, it is difficult to see by visual inspection if there are actual rates that do achieve unconditional secrecy. We demonstrate an example using the binary erasure wiretap channel (BE–WC). Let the channel input alphabet be $\mathcal{X} = \{0, 1\}$ for both users, and the channel output alphabet be $\mathcal{Y} = \{0, 1, 2\}$. Let the overall channel be given by

$$Y_A = X_A + \overline{X_B} \tag{42}$$

$$Y_B = X_A + X_B \tag{43}$$

where $\overline{X_B}$ is the binary complement of X_B and addition is the real addition, not the binary field addition. Fig. 4(a) depicts the BE-WC, where the "c" box denotes the complement.[1] For simplicity, we do not include the additional noisy channels $v_A(\cdot|\cdot), v_B(\cdot|\cdot)$. Table I shows the input–output relationship of this BE–WC. Clearly, the joint decoder is able to decode any messages without error since all pairs of (Y_A, Y_B) in Table I are unique; the capacity region for this two-output MAC is described using $\bar{R}_1$ for Alice's rate and $\bar{R}_2$ for Bob's rate. Next, Eve sees either the MAC of (42) or (43). Both of these MACs are statistically identical if we choose $\Pr\{X_A = 0\} = \Pr\{X_B = 0\} = 1/2$. The capacity region for these one-output MACs is described using U_1 for Alice's rate and U_2 for Bob's rate. Setting the random variable J constant, and using the deterministic channels $P_{X_A|V_A}$, $P_{X_B|V_B}$, the capacity regions for the two-output and one-input MACs can be derived and found to be

$$\begin{aligned} \bar{R}_1 &\leq 1 & U_1 &\leq 1 \\ \bar{R}_2 &\leq 1 & U_2 &\leq 1 \\ \bar{R}_1 + \bar{R}_2 &\leq 2 & U_1 + U_2 &\leq \frac{3}{2}. \end{aligned}$$

Furthermore, by (37), we choose $U_1 + U_2 = 3/2$, then the corresponding inner region (rates that achieve unconditional secrecy) can be derived using Theorem 4 and found to be

$$\left\{ (r_1, r_2) : r_1 \geq 0, r_2 \geq 0, r_1 + r_2 \leq \frac{1}{2} \right\}.$$

For example, to achieve $(r_1, r_2) = (0.5, 0)$, choose $\bar{R}_1 = \bar{R}_2 = 1$ and $U_1 = 0.5, U_2 = 1$ (which satisfies $U_1 + U_2 = 1.5$), thus $r_1 = \bar{R}_1 - U_1 = 0.5$ and $\bar{r}_2 = R_2 - U_2 = 0$ according to Theorem 4. To achieve $(r_1, r_2) = (0.25, 0.25)$ [the middle point on the diagonal of the triangle, see Fig. 4(b)] choose $\bar{R}_1 = \bar{R}_2 = 1$ and $U_1 = U_2 = 0.75$ (which satisfies $U_1 + U_2 = 1.5$), thus $r_1 = \bar{R}_1 - U_1 = 0.25$ and $\bar{r}_2 = R_2 - U_2 = 0.25$ according to Theorem 4. To conclude this example, we contrast the achievable rate regions for the binary erasure networks for no secrecy and perfect secrecy in Fig. 4(b). Not surprisingly, the achievable rate region for the perfect secrecy case is a subregion of that without secrecy. Note that Fig. 4(b) is not to be compared with Fig. 3 since the axes are different.

[1] Without complementation, the two outputs would be identical and, thus, one copy would be useless for decoding. This is only the case because the channel is deterministic, which is used in this example for simplicity.

TABLE I
INPUT–OUTPUT TABLE FOR THE BINARY ERASURE WIRETAP CHANNEL

X_A	X_B	Y_A	Y_B
0	0	1	0
0	1	0	1
1	0	2	1
1	1	1	2

V. CONCLUSION

We have shown that in noiseless as well as noisy (but noninterfering) environments, unconditional secrecy is unachievable.[2] Upon showing this negative result, interference is then shown to be necessary for unconditional secrecy. Our coding strategy is restrictive in the sense that both of Eve's channels must be statistically identical, but permits both users to send secret messages.

APPENDIX

A. Proof of Theorem 2

Equations (26)–(28) are directly from [1]. Equation (25) arises from simply MSC, and then sending the source-coded messages without further secrecy coding. The secrecy for Alice and Bob then comes from what was cropped out due to MSC, which are the bracketed terms in (a)

$$\begin{aligned}\Delta_A + \Delta_B &\overset{(a)}{=} (H(S_A) - R_A) + (H(S_B) - R_B)\\ &\overset{(b)}{\leq} H(S_A) + H(S_B) - H(S_A, S_B)\\ &\quad + H(S_A|S_B, Q_A) + H(S_B|S_A, Q_B) \qquad (44)\end{aligned}$$

where (a) follows since approximately $k(H(S_A) - R_A)$ bits (for k sufficiently large) are unknown to Eve given that she possesses the kR_A bits of W_A, and similarly $k(H(S_B) - R_B)$ bits for Bob; (b) follows from (28). The reader can verify that (44) is equivalent to (25).

B. Proof of Theorem 3

The proof makes use of the following lemma.

Lemma 1 (Lemma 4.1 [9]): For arbitrary random variables U, V and sequences of random variables Y^n, Z^n, the following is true:

$$\begin{aligned}&I(U; Y^n|V) - I(U; Z^n|V)\\ &\quad = \sum_{i=1}^{n} \Big(I(U; Y_i|Y^{i-1}, Z_{i+1}, \ldots, Z_n, V)\\ &\qquad\qquad - I(U; Z_i|Y^{i-1}, Z_{i+1}, \ldots, Z_n, V) \Big) \qquad (45)\end{aligned}$$

where $Y^{i-1} = (Y_1, \ldots, Y_{i-1})$.

There are a total of four bounds for the sum of the rates. We prove the first of the two pairs in Theorem 3

$$\begin{aligned}
&n(R_1 + R_2)\\
&\quad = H(W_A, W_B)\\
&\quad = H\left(W_A, W_B|\tilde{Y}_A^n, \tilde{Y}_B^n\right) + I\left(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n\right)\\
&\quad \overset{(a)}{\leq} n\epsilon_n + I\left(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n\right)\\
&\quad \overset{(b)}{=} I\left(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n\right) - I\left(W_A, W_B; \tilde{Y}_A^n\right)\\
&\qquad + I\left(W_A, W_B; \tilde{Y}_A^n\right) + n\epsilon_n\\
&\quad \overset{(c)}{\leq} I\left(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n\right) - I\left(W_A, W_B; \tilde{Y}_A^n\right)\\
&\qquad + I\left(W_A, W_B; Y_A^n\right) + n\epsilon_n\\
&\quad \overset{(d)}{\leq} I\left(W_A, W_B; \tilde{Y}_A^n, \tilde{Y}_B^n\right) - I\left(W_A, W_B; \tilde{Y}_A^n\right)\\
&\qquad + n\epsilon + n\epsilon_n\\
&\quad \overset{(e)}{=} \sum_{i=1}^{n} \Big(I\Big(W_A, W_B; \tilde{Y}_{A,i}, \tilde{Y}_{B,i}|\tilde{Y}_A^{i-1},\\
&\qquad\qquad \tilde{Y}_B^{i-1}, \tilde{Y}_{A,i+1}, \ldots, \tilde{Y}_{A,n}\Big)\\
&\qquad\quad - I\Big(W_A, W_B; \tilde{Y}_{A,i}|\tilde{Y}_A^{i-1}, \tilde{Y}_B^{i-1},\\
&\qquad\qquad \tilde{Y}_{A,i+1}, \ldots, \tilde{Y}_{A,n}\Big)\Big) + n(\epsilon + \epsilon_n)\\
&\quad \overset{(f)}{=} n \sum_{i=1}^{n} \Pr\{\Theta = i\}\\
&\qquad \times \Big(I(W_A, W_B; \tilde{Y}_{A,i}, \tilde{Y}_{B,i}|K_i, \Theta = i)\\
&\qquad\quad - I(W_A, W_B; \tilde{Y}_{A,i}|K_i, \Theta = i)\Big) + n(\epsilon + \epsilon_n)\\
&\quad = n \sum_{i=1}^{n} \Pr\{\Theta = i\}\\
&\qquad \times \Big(I(W_A, W_B; \tilde{Y}_{A,\Theta}, \tilde{Y}_{B,\Theta}|K_\Theta, \Theta = i)\\
&\qquad\quad - I(W_A, W_B; \tilde{Y}_{A,\Theta}|K_\Theta, \Theta = i)\Big) + n(\epsilon + \epsilon_n)\\
&\quad \overset{(g)}{=} n \Big(I(W_A, W_B; \tilde{Y}_{A,\Theta}, \tilde{Y}_{B,\Theta}|K_\Theta, \Theta)\\
&\qquad\quad - I(S_A, S_B; \tilde{Y}_{A,\Theta}|K_\Theta, \Theta)\Big) + n(\epsilon + \epsilon_n)\\
&\quad \overset{(h)}{=} n \Big(I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J) - I(V_A, V_B; \tilde{Y}_A|J)\Big)\\
&\qquad + n(\epsilon + \epsilon_n). \qquad (46)
\end{aligned}$$

The explanations are as follows: (a) Fano's inequality from (12); (c) data-processing inequality on the Markov chain $(W_A, W_B) \leftrightarrow Y_A^n \leftrightarrow \tilde{Y}_A^n$; (d) unconditional secrecy requirement if Eve intercepts Y_A^n [see (11)]; (e) use of Lemma 1; (f) by defining

$$K_i \triangleq \left(\tilde{Y}_A^{i-1}, \tilde{Y}_B^{i-1}, \tilde{Y}_{A,i+1}, \ldots, \tilde{Y}_{A,n}\right) \qquad (47)$$

and defining a uniform RV $\Theta = 1, \ldots, n$ that is independent of all other RVs; (g) definition of conditioning; (h) by defining

$$\begin{aligned}&\tilde{Y}_A \triangleq \tilde{Y}_{A,\Theta}, \tilde{Y}_B \triangleq \tilde{Y}_{B,\Theta}, Y_A \triangleq Y_{A,\Theta}, Y_B \triangleq Y_{B,\Theta}, X_A \triangleq X_{A,\Theta},\\ &X_B \triangleq X_{B,\Theta}, J \triangleq (K_\Theta, \Theta), V_A \triangleq (W_A, J), V_B \triangleq (W_B, J).\end{aligned}$$

Finally, it is easily seen that

$$\begin{aligned}&J \leftrightarrow (V_A, V_B) \leftrightarrow (X_A, X_B) \leftrightarrow (Y_A, Y_B) \leftrightarrow (\tilde{Y}_A, \tilde{Y}_B)\\ &\qquad\qquad \text{and } V_A \leftrightarrow J \leftrightarrow V_B \qquad (48)\end{aligned}$$

form Markov chains where the last chain follows since W_A, W_B are independent.

On the other hand, adding and subtracting $I(W_A, W_B; \tilde{Y}_B)$ in (b) instead of $I(W_A, W_B; \tilde{Y}_A)$ yields a different bound

$$R_1 + R_2 \leq \Big(I(V_A, V_B; \tilde{Y}_A, \tilde{Y}_B|J) - I(V_A, V_B; \tilde{Y}_B|J)\Big) + \epsilon + \epsilon_n$$

with the same Markov chains (48) and the same distribution factorization.

[2] Stochastic encoding can be modeled by virtual noisy channels within the encoders.

The other pair in Theorem 3 is derived in a similar manner with slight differences outlined

$$\begin{aligned}n(R_1+R_2) &= H(W_A,W_B)\\ &= H\left(W_A,W_B|Y_A^n,Y_B^n\right)+I\left(W_A,W_B;Y_A^n,Y_B^n\right)\\ &\overset{(a)}{\leq} H\left(W_A,W_B|\tilde{Y}_A^n,\tilde{Y}_B^n\right)+I\left(W_A,W_B;Y_A^n,Y_B^n\right)\\ &\overset{(b)}{\leq} n\epsilon_n + I\left(W_A,W_B;Y_A^n,Y_B^n\right)\\ &\overset{(c)}{=} I\left(W_A,W_B;Y_A^n,Y_B^n\right)-I\left(W_A,W_B;Y_A^n\right)\\ &\quad + I\left(W_A,W_B;Y_A^n\right)+n\epsilon_n\\ &\overset{(d)}{\leq} I\left(W_A,W_B;Y_A^n,Y_B^n\right)-I\left(W_A,W_B;Y_A^n\right)\\ &\quad + n\epsilon+n\epsilon_n\\ &\overset{(e)}{=} n\left(I(V_A,V_B;Y_A,Y_B|J)-I(V_A,V_B;Y_A|J)\right)\\ &\quad + n(\epsilon+\epsilon_n).\end{aligned}$$

The explanations are as follows: (a) is the data-processing inequality on the Markov chain $(W_A,W_B) \leftrightarrow (Y_A^n,Y_B^n) \leftrightarrow (\tilde{Y}_A^n,\tilde{Y}_B^n)$ (b) Fano's inequality; (d) is the unconditional secrecy requirement if Eve intercepts Y_A^n; (e) is the same approach as in deriving (46), but now with the following Markov chain:

$$J \leftrightarrow (V_A,V_B) \leftrightarrow (X_A,X_B) \leftrightarrow (Y_A,Y_B) \tag{49}$$

in place of the first Markov chain in (48).

On the other hand, adding and subtracting $I(W_A,W_B;Y_B^n)$ in (c) instead of $I(W_A,W_B;Y_A^n)$ gives the final bound

$$R_1+R_2 \leq \left(I(V_A,V_B;Y_A,Y_B|J)-I(V_A,V_B;Y_B|J)\right)+\epsilon+\epsilon_n$$

with the Markov chain in (49) and the same distribution factorization.

C. Proof of Theorem 4

1) Random Codebook Generation: Randomly generate a typical sequence j^n using the distribution $\prod_{i=1}^n P_J(j_i)$ and make this publically known to all parties including the joint decoder and Eve. Generate $2^{n(\bar{R}_1-\delta)}$ sequences v_A^n using the distribution $\prod_{i=1}^n P_{V_A|J}(v_{A,i}|j_i)$ and $2^{n(\bar{R}_2-\delta)}$ sequences v_B^n using the distribution $\prod_{i=1}^n P_{V_B|J}(v_{B,i}|j_i)$ such that (38)–(40) are satisfied.

Alice's codebook is then the arrangement of the v_A^ns in a $2^{\lfloor nr_1 \rfloor} \times 2^{n(U_1-\delta)}$ table, while Bob's codebook is the arrangement of the v_B^ns in a $2^{\lfloor nr_2 \rfloor} \times 2^{n(U_2-\delta)}$ table such that (32)–(37) are satisfied if possible. Suppose Alice's message w_A is indexed such that $w_A \in \{1,\ldots,2^{\lfloor nr_1 \rfloor}\}$ and similarly Bob's message is $w_B \in \{1,\ldots,2^{\lfloor nr_2 \rfloor}\}$. Thus, each entry in Alice and Bob's codebooks can be indexed as $v_A^n(w_A,u_1)$ and $v_B^n(w_B,u_2)$, respectively. In addition as $n \to \infty$, the actual rates R_1, R_2 will satisfy the definition in (10).

2) Encoding: Alice encodes her w_A by randomly choosing a codeword v_A^n from row w_A of her tabular codebook (i.e., randomly and uniformly selecting a column index u_1 resulting in $v_A^n(w_A,u_1)$). She then randomly generates x_A^n (to be sent over the channels) using the distribution $\prod_{i=1}^n P_{X_A|V_A}(x_{A,i}|v_{A,i})$. Similarly, Bob encodes his w_B by randomly choosing a codeword v_B^n from row w_B of his tabular codebook (i.e., randomly selecting a column index u_2 resulting in $v_B^n(w_B,u_2)$). He then randomly generates x_B^n (to be sent over the channels) using the distribution $\prod_{i=1}^n P_{X_B|V_B}(x_{B,i}|v_{B,i})$. Thus, the encoders are both stochastic.

3) Decoding: Let $A_\epsilon^{(n)}(J,V_A,V_B,\tilde{Y}_A,\tilde{Y}_B)$ be the set of jointly typical sequences $(J^n,V_A^n,V_B^n,\tilde{Y}_A^n,\tilde{Y}_B^n)$. Upon receiving $(\tilde{y}_A^n,\tilde{y}_B^n)$, the joint decoder declares the messages $(\hat{w}_A,\hat{w}_B)$ as having been sent if $(j^n,v_A^n(\hat{w}_A,u_1),v_B^n(\hat{w}_B,u_2),\tilde{y}_A^n,\tilde{y}_B^n) \in A_\epsilon^{(n)}(J,V_A,V_B,\tilde{Y}_A,\tilde{Y}_B)$ for any (u_1,u_2) if such a $(\hat{w}_A,\hat{w}_B)$ exists and is unique.

4) Probability of Error Analysis: Define the event $E_{a,b} \triangleq \{(j^n,v_A^n(a,u_1),v_B^n(b,u_2),\tilde{y}_A^n,\tilde{y}_B^n) \in A_\epsilon^{(n)}\}$. By the symmetry of the codebook construction, we can assume without loss of generality that the messages $(w_A,w_B)=(1,1)$ were sent. Thus

$$\begin{aligned}P_e^{(n)} &= \Pr\left\{\text{error}|(w_A,w_B)=(1,1)\right\}\\ &= \Pr\left\{E_{1,1}^c \cup \bigcup_{a\neq 1,u_1} E_{a,1} \cup \bigcup_{b\neq 1,u_2} E_{1,b} \cup \bigcup_{\substack{a\neq 1,b\neq 1\\ u_1,u_2}} E_{a,b}\right\}\\ &\leq \Pr\left\{E_{1,1}^c|(w_A,w_B)=(1,1)\right\}\\ &\quad + \sum_{a\neq 1}\sum_{u_1} \Pr\left\{E_{a,1}|(w_A,w_B)=(1,1)\right\}\\ &\quad + \sum_{b\neq 1}\sum_{u_2} \Pr\left\{E_{1,b}|(w_A,w_B)=(1,1)\right\}\\ &\quad + \sum_{a\neq 1}\sum_{b\neq 1}\sum_{u_1}\sum_{u_2} \Pr\left\{E_{a,b}|(w_A,w_B)=(1,1)\right\}\end{aligned} \tag{50}$$

by the union bound. The first term tends to 0 as $n \to \infty$ by the asymptotic equipartition theorem (AEP). The second term is bounded as follows:

$$\begin{aligned}&\Pr\left\{E_{a\neq 1,1}|(w_A,w_B)=(1,1)\right\}\\ &= \sum_{\substack{(j^n,v_A^n,v_B^n,\tilde{y}_A^n,\tilde{y}_B^n)\\ \in A_\epsilon^{(n)}(J,V_A,V_B,\tilde{Y}_A,\tilde{Y}_B)}} P_J^n(j^n)P_{V_A|J}\left(v_A^n|j^n\right)\\ &\quad \times P_{V_B,\tilde{Y}_A,\tilde{Y}_B|J}^n\left(v_B^n,\tilde{y}_A^n,\tilde{y}_B^n|j^n\right)\\ &\leq \left|A_\epsilon^{(n)}(J,V_A,V_B,\tilde{Y}_A,\tilde{Y}_B)\right| 2^{-n(H(J)-\delta)}2^{-n(H(V_A|J)-\delta)}\\ &\quad \cdot 2^{-n\left(H(V_B,\tilde{Y}_A,\tilde{Y}_B|J)-\delta\right)}\\ &\leq 2^{-n\left(I(V_A;\tilde{Y}_A|V_B,J)-\delta'\right)}.\end{aligned} \tag{51}$$

Using the AEP, the other probabilities are

$$\begin{aligned}\Pr\{E_{1,b\neq 1}|(w_A,w_B)=(1,1)\} &\leq 2^{-n\left(I(V_B;\tilde{Y}_B|V_A,J)-\delta'\right)}\\ \Pr\{E_{a\neq 1,b\neq 1}|(w_A,w_B)=(1,1)\} &\leq 2^{-n\left(I(V_A,V_B;\tilde{Y}_A,\tilde{Y}_B|J)-\delta'\right)}\end{aligned}$$

thus recalling the size and dimensions of the codebooks yields

$$\begin{aligned}P_e^{(n)} &\leq \delta + 2^{n(\bar{R}_1-\delta)}2^{-n\left(I(V_A;\tilde{Y}_A|V_B,J)-\delta'\right)}\\ &\quad + 2^{n(\bar{R}_2-\delta)}2^{-n\left(I(V_B;\tilde{Y}_B|V_A,J)-\delta'\right)}\\ &\quad + 2^{n(\bar{R}_1+\bar{R}_2-\delta)}2^{-n\left(I(V_A,V_B;\tilde{Y}_A,\tilde{Y}_B|J)-\delta'\right)}.\end{aligned} \tag{52}$$

Therefore, if (38)–(40) are satisfied, then the bound in (52) approaches 0 as $n \to \infty$.

5) Secrecy Analysis:

$$\begin{aligned}&H\left(W_A,W_B|Y_i^n\right)\\ &\geq H\left(W_A,W_B|Y_i^n,J^n\right)\\ &= H\left(W_A,W_B,Y_i^n|J^n\right)-H\left(Y_i^n|J^n\right)\\ &= H\left(W_A,W_B,V_A^n,V_B^n,Y_i^n|J^n\right)\\ &\quad - H\left(V_A^n,V_B^n|W_A,W_B,Y_i^n,J^n\right)-H\left(Y_i^n|J^n\right)\\ &= H\left(W_A,W_B,V_A^n,V_B^n|J^n\right)\\ &\quad + H\left(Y_i^n|W_A,W_B,V_A^n,V_B^n,J^n\right)\\ &\quad - H\left(V_A^n,V_B^n|W_A,W_B,Y_i^n,J^n\right)-H\left(Y_i^n|J^n\right)\\ &\overset{(a)}{\geq} H\left(V_A^n,V_B^n|J^n\right)+H\left(Y_i^n|V_A^n,V_B^n,J^n\right)\\ &\quad - H\left(V_A^n,V_B^n|W_A,W_B,Y_i^n,J^n\right)-H\left(Y_i^n|J^n\right)\end{aligned}$$

$$\begin{aligned}
&\overset{(b)}{=} H\left(V_A^n|J^n\right) + H\left(V_B^n|J^n\right) - I\left(Y_i^n; V_A^n, V_B^n|J^n\right) \\
&\quad - H\left(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n\right) \\
&\overset{(c)}{=} n(\bar{R}_1 + \bar{R}_2 - 2\delta) - I\left(Y_i^n; V_A^n, V_B^n|J^n\right) \\
&\quad - H\left(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n\right) \\
&\overset{(d)}{\geq} n(r_1 + r_2 - 2\delta - \epsilon) - H\left(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n\right) \\
&\overset{(e)}{\geq} n(R_1 + R_2 - \epsilon') - H\left(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n\right) \\
&\overset{(f)}{\geq} n(R_1 + R_2 - \epsilon') - n\epsilon_n \qquad (53)
\end{aligned}$$

where (a) is the first term resulting from $H(W_A, W_B, V_A^n, V_B^n|J^n) \geq H(V_A^n, V_B^n|J^n)$ (property of entropy) and the second term is from the encoding process (i.e., knowledge of V_A^n implies knowledge of W_A) and similarly knowledge of V_B^n implies knowledge of W_B; (b) since $H(V_A^n, V_B^n|J^n) = H(V_A^n|J^n) + H(V_B^n|V_A^n, J^n)$ and $V_A^n \leftrightarrow J^n \leftrightarrow V_B^n$ forms a Markov chain from the codebook generation; (c) is from the codebook generation; (d) since $U_1 + U_2 \geq I(V_A, V_B; Y_i^n|J^n)$ is true from (37), and using the definitions of r_1 and r_2 from (32) and (33) yields $\bar{R}_1 - r_1 + \bar{R}_2 - r_2 \geq I(V_A, V_B; Y_i^n|J^n) - \epsilon$; (e) is from the floor operation in the codebook generation; (f) when Eve is given W_A and W_B, she has knowledge of the rows of the codebooks in which the codewords V_A^n and V_B^n were randomly chosen in the encoding process. This reduces the codebooks in which she must search (by using joint typical decoding with her eavesdropped Y_i^n) from the two codebooks in its entirety to just one row of each codebook. Using the same technique as in the Appendix, it can be shown that Eve's average probability of error (which we denote by $P_e^{(n)'}$) is also bounded by quantities that vanish to 0 as $n \to \infty$ based on the random codebook generation if the upper bounds in (35)–(37) are satisfied. Therefore, by Fano's inequality

$$\begin{aligned}
H\left(V_A^n, V_B^n|W_A, W_B, Y_i^n, J^n\right) &\leq 1 + P_e^{(n)'} \log_2\left(|\mathcal{W}_A||\mathcal{W}_B|\right) \\
&\triangleq n\epsilon_n.
\end{aligned}$$

References

[1] J. Barros and S. D. Servetto, "On the rate-distortion region for separate encoding of correlated sources," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, Jun. 29–Jul. 4, 2003, p. 171.

[2] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," presented at the IEEE Information Theory Workshop, Lake Tahoe, CA, Sep. 2–6, 2007.

[3] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 6–11, 2008.

[4] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[5] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," presented at the IEEE Int. Symp. Information Theory, Seattle, WA, Jul. 2006.

[6] Y. Liang and H. V. Poor, "Secrecy capacity region of binary and Gaussian multiple access channels," presented at the Allerton Conf. Communication, Control, and Computing, Urbana, IL, Sep. 26–29, 2006.

[7] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[8] W. Luh and D. Kundur, "Distributed keyless security for correlated data with applications in visual sensor networks," presented at the ACM Multimedia and Security Workshop, Dallas, TX, Sep. 20–21, 2007.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.