Secure Source Coding With a Helper

Ravi Tandon, *Member, IEEE*, Sennur Ulukus, *Member, IEEE*, and Kannan Ramchandran, *Fellow, IEEE*

***Abstract*—We consider a secure lossless source coding problem with a rate-limited helper. In particular, Alice observes an independent and identically distributed (i.i.d.) source X^n and wishes to transmit this source losslessly to Bob over a rate-limited link of capacity not exceeding R_x. A helper, say Helen, observes an i.i.d. correlated source Y^n and can transmit information to Bob over another link of capacity not exceeding R_y. A passive eavesdropper (say Eve) can observe the coded output of Alice, i.e., the link from Alice to Bob is public. The uncertainty about the source X^n at Eve (denoted by Δ) is measured by the conditional entropy $\frac{H(X^n|J_x)}{n}$, where J_x is the coded output of Alice and n is the block length. We completely characterize the rate-equivocation region for this secure source coding model, where we show that *Slepian–Wolf binning* of X^n with respect to the coded side information received at Bob is optimal. We next consider a modification of this model in which Alice also has access to the coded output of Helen. We call this model as the two-sided helper model. For the two-sided helper model, we characterize the rate-equivocation region. While the availability of side information at Alice does not reduce the rate of transmission from Alice, it significantly enhances the resulting equivocation at Eve. In particular, the resulting equivocation for the two-sided helper case is shown to be $\min(H(X), R_y)$, i.e., one bit from the two-sided helper provides one bit of uncertainty at Eve. From this result, we infer that Slepian–Wolf binning of X is suboptimal and one can further decrease the information leakage to the eavesdropper by utilizing the side information at Alice. We, finally, generalize both of these results to the case in which there is additional uncoded side information W^n available at Bob and characterize the rate-equivocation regions under the assumption that $Y^n \rightarrow X^n \rightarrow W^n$ forms a Markov chain.**

***Index Terms*—Equivocation, helper problem, lossless source coding.**

I. Introduction

THE study of information-theoretic secrecy was initiated by Shannon in [1]. Following Shannon's work, significant contributions were made by Wyner [2] who established the rate-equivocation region of a degraded broadcast channel. Wyner's result was generalized to the case of a general broadcast channel by Csiszar and Korner [3]. Recently, there has been a resurgence of activity in studying multiterminal and vector extensions of [2] and [3].

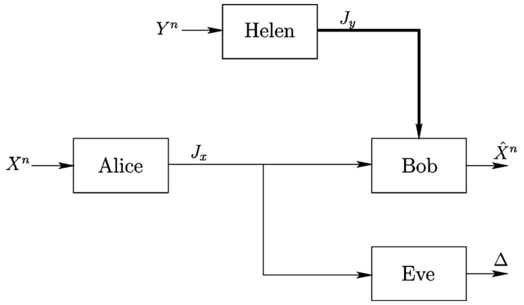

Fig. 1. One-sided helper.

In this paper, we investigate a secure transmission problem from a source coding perspective. In particular, we first consider a simple setup consisting of four terminals. Terminal 1 (say Alice) observes an i.i.d. source X^n which it intends to transmit losslessly to terminal 2 (say Bob). A malicious but passive user (say Eve) can observe the coded output of Alice. In other words, the communication link between Alice and Bob is public (or insecure). It is clear that since the malicious user gets the same information as the legitimate user, there cannot be any positive secret rate of transmission, i.e., some information about X^n will be leaked to Eve. On the other hand, if there is a helper, say Helen, who observes an i.i.d. source Y^n which is correlated with the source X^n and transmits information over a *secure* rate-limited link to Bob, then one can aim for creating uncertainty at the eavesdropper (see Fig. 1[1]). For the model shown in Fig. 1, we completely characterize the rate-equivocation region. From our result, we observe that the classical achievability scheme of Ahlswede and Korner [4] and Wyner [5] for source coding with rate-limited side information is robust in the presence of a passive eavesdropper. By robust, we mean that in the presence of a passive adversary, there is no need to change the original scheme as it achieves the maximum possible equivocation at Eve.

Next, we consider the model where Alice also has access to the coded output of Helen and completely characterize the rate-equivocation region. We will call this model the two-sided helper model (see Fig. 2). From our result, we observe that the availability of additional coded side information at Alice allows her to increase uncertainty of the source at Eve even though the rate needed by Alice to transmit the source losslessly to Bob remains the same. This observation is in contrast with the case of insecure source coding with side information where providing coded side information to Alice is of no value in terms of reducing Alice's transmission rate [4].

We finally extend these results to the case in which there is additional *uncoded* correlated side information W^n available

Manuscript received October 29, 2009; revised November 29, 2012; accepted December 03, 2012. Date of publication January 04, 2013; date of current version March 13, 2013. This work was supported by the National Science Foundation under Grants CCF 04-47613, CCF 05-14846, CNS 07-16311, and CCF 07-29127. This paper was presented in part at the 47th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 2009.

R. Tandon is with the Department of Electrical and Computer Engineering and the Hume Center for National Security and Technology, Virginia Tech, Blacksburg, VA 24060 USA (e-mail: tandonr@vt.edu).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

K. Ramchandran is with the Wireless Foundation, Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA 94704 USA (e-mail: kannanr@eecs.berkeley.edu).

Communicated by I. Kontoyiannis, Associate Editor At Large.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2012.2236973

[1] In Figs. 1 and 2, secure links are shown by **bold** lines.

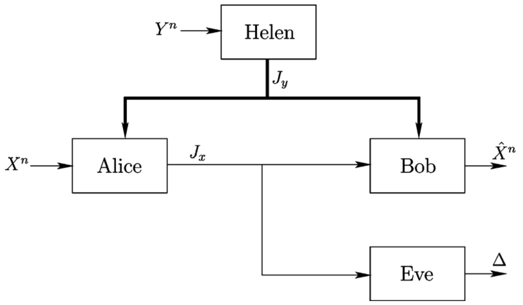

Fig. 2. Two-sided helper.

to Bob. We completely characterize the rate-equivocation region for this model when $Y^n \rightarrow X^n \rightarrow W^n$ forms a Markov chain. We explicitly compute the rate-equivocation region for the cases of one-sided helper and two-sided helper for a pair of binary symmetric sources. We show that having access to Helen's coded output at Alice yields a strictly larger equivocation than the case of one-sided helper.

Related Work: The secure source coding setup shown in Fig. 1 was considered in [6] where it was also assumed that Eve has access to additional correlated side information Z^n. Inner and outer bounds for the rate-equivocation region were provided for this setup, which do not match in general. The rate-equivocation region was completely characterized in [6] for the case when Bob has complete uncoded side information Y^n and Eve has additional side information Z^n. This result also follows from [7] where a similar three terminal setup was studied and the maximum uncertainty at Eve was characterized under the assumption of no rate constraint in the lossless transmission of the source to Bob. A similar model was also studied in [8] where Bob intends to reconstruct both X^n and Y^n losslessly. It was shown that Slepian–Wolf binning suffices for characterizing the rate-equivocation region when the eavesdropper does not have additional correlated side information. This setup was generalized in [9] to the case when the eavesdropper has additional side information Z^n, and inner and outer bounds were provided, which do not match in general.

In [10], a multireceiver secure broadcasting problem was studied, where Alice intends to transmit a source X^n to K legitimate users. The kth user has access to a correlated source Y_k^n, where $Y_k^n = X^n \oplus B_k^n$, for $k = 1, \ldots K$, and the eavesdropper has access to Z^n, where $Z^n = X^n \oplus E^n$, and the noise sequences $(B_1^n, \ldots, B_K^n, E^n)$ are mutually independent and also independent of the source X^n. Furthermore, it was assumed that Alice also has access to $(Y_1^n, \ldots Y_K^n)$. For sources with such modulo-additive structure, it was shown that to maximize the uncertainty at the eavesdropper, Alice cannot do any better than describing the error sequences $(B_1^n, \ldots, B_K^n)$ to the legitimate users. This model is related to the two-sided helper model shown in Fig. 2; see Section II-B for details. Extensions of the lossless secure source coding problems to the case of lossy secure source coding settings have been recently investigated in [15] and [16].

Summary of Main Results: In Section II-A, we present the rate-equivocation region for the case of one-sided helper. We show that Slepian–Wolf binning alone at Alice is optimal for this case. We present the rate-equivocation region for the case of two-sided helper in Section II-B. For the case of two-sided helper, Alice utilizes the coded-side information received from Helen as follows: she can narrow down the set of uncertainty about X^n-sequences at Bob given the output received from Helen. She only sends the residual information necessary to decode X^n at Bob. We show that the resulting equivocation of this scheme is $\min(H(X), R_y)$, i.e., one secure (two-sided) bit from Helen results in one bit of equivocation at Eve. From this result, we demonstrate the insufficiency of Slepian–Wolf binning at Alice by explicitly utilizing the side information at Alice. This observation is further highlighted in Section III where we compare the rate-equivocation regions of two-sided helper and one-sided helper cases for a pair of binary symmetric sources. For this example, we show that for all $R_y > 0$, the information leakage to the eavesdropper for the two-sided helper is strictly less than the case of one-sided helper. We finally generalize these results to the case when there is additional side information W^n at Bob. For the case in which $Y \rightarrow X \rightarrow W$, we characterize the tradeoff of rates and equivocation. For the case of two-sided helper, the optimal resulting equivocation at Eve is $\min(H(X), R_y + I(X;W))$, i.e., the net equivocation resulting from coded and uncoded side information is *additive* in nature. By additive, we mean the following: suppose that W^n was not present, then the equivocation would be $\min(H(X), R_y)$ from our result of two-sided helper. On the other hand, if $R_y = 0$, then we know from [7] that the optimal equivocation is given by $I(X;W)$. Thus, in the presence of both uncoded and coded side-information, the net equivocation is $R_y + I(X;W)$ till it saturates to $H(X)$. Parts of this paper have been presented in [11].

II. Main Results

A. One-Sided Helper

We consider the following source coding problem. Alice observes an n-length source sequence X^n, which is intended to be transmitted losslessly to Bob. The coded output of Alice can be observed by the malicious user Eve. Moreover, Helen observes a correlated source Y^n and there exists a noiseless rate-limited channel from Helen to Bob. We assume that the link from Helen to Bob is a secure link and the coded output of Helen is not observed by Eve (see Fig. 1). The sources (X^n, Y^n) are generated i.i.d. according to $p(x, y)$, where $p(x, y)$ is defined over the finite product alphabet $\mathcal{X} \times \mathcal{Y}$. The aim of Alice is to create maximum uncertainty at Eve regarding the source X^n while losslessly transmitting the source to Bob.

An $(n, 2^{nR_x}, 2^{nR_y})$ code for this model consists of an encoding function at Alice, $f_x : X^n \rightarrow \{1, \ldots, 2^{nR_x}\}$, an encoding function at Helen, $f_y : Y^n \rightarrow \{1, \ldots, 2^{nR_y}\}$, and a decoding function at Bob, $g : \{1, \ldots, 2^{nR_x}\} \times \{1, \ldots, 2^{nR_y}\} \rightarrow X^n$. The uncertainty about the source X^n at Eve is measured by $H(X^n|f_x(X^n))/n$. The probability of error in the reconstruction of X^n at Bob is defined as $P_e^n = \Pr(g(f_x(X^n), f_y(Y^n)) \neq X^n)$. A triple (R_x, R_y, Δ) is achievable if for any $\epsilon > 0$, there exists a $(n, 2^{nR_x}, 2^{nR_y})$ code such that $P_e^n \leq \epsilon$ and $H(X^n|f_x(X^n))/n \geq \Delta$. We denote the set of all achievable (R_x, R_y, Δ) rate triples as $\mathcal{R}_{\text{1-sided}}$.

The main result is given in the following theorem.

Theorem 1: The set of achievable rate triples $\mathcal{R}_{1-\text{sided}}$ for secure source coding with one-sided helper is given as

$$\mathcal{R}_{\text{1-sided}} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|V) \quad (1)$$
$$R_y \geq I(Y;V) \quad (2)$$
$$\Delta \leq I(X;V)\Big\} \quad (3)$$

where the joint distribution of the involved random variables is as follows:

$$p(x,y,v) = p(x,y)p(v|y) \quad (4)$$

and it suffices to consider such distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 2$.

The proof of Theorem 1 is given in the Appendix.

We note that inner and outer bounds for source coding model considered in this section were presented in [6, Th. 3.1] although these bounds do not match in general. These bounds match when Bob has complete uncoded side information Y^n, i.e., when $R_y \geq H(Y)$.

The achievability scheme which yields the rate region described in Theorem 1 is summarized as follows.

1) Helen describes the source Y^n to Bob through a coded output V^n.
2) Alice performs Slepian–Wolf binning of the source X^n with respect to the coded side information, V^n, available at Bob.

Therefore, this result shows that the achievable scheme of Ahlswede and Korner [4] and Wyner [5] is optimal in the presence of an eavesdropper. Moreover, upon dropping the security constraint, Theorem 1 yields the result of [4] and [5].

B. Two-Sided Helper

We next consider the following modification of the model considered in Section II-A. In this model, Alice also has access to the coded output of Helen besides the source sequence X^n (see Fig. 2). An $(n, 2^{nR_x}, 2^{nR_y})$ code for this model consists of an encoding function at Alice, $f_x : X^n \times \{1, \ldots, 2^{nR_y}\} \rightarrow \{1, \ldots, 2^{nR_x}\}$, an encoding function at Helen, $f_y : Y^n \rightarrow \{1, \ldots, 2^{nR_y}\}$, and a decoding function at Bob, $g : \{1, \ldots, 2^{nR_x}\} \times \{1, \ldots, 2^{nR_y}\} \rightarrow X^n$. The uncertainty about the source X^n at Eve is measured by $H(X^n|f_x(X^n))/n$. The probability of error in the reconstruction of X^n at Bob is defined as $P_e^n = \Pr(g(f_x(X^n, f_y(Y^n)), f_y(Y^n)) \neq X^n)$. A triple (R_x, R_y, Δ) is achievable if for any $\epsilon > 0$, there exists a $(n, 2^{nR_x}, 2^{nR_y})$ code such that $P_e^n \leq \epsilon$ and $H(X^n|f_x(X^n))/n \geq \Delta$. We denote the set of all achievable (R_x, R_y, Δ) rate triples as $\mathcal{R}_{\text{2-sided}}$.

The main result is given in the following theorem.

Theorem 2: The set of achievable rate triples $\mathcal{R}_{\text{2-sided}}$ for secure source coding with two-sided helper is given as

$$\mathcal{R}_{\text{2-sided}} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|V) \quad (5)$$
$$R_y \geq I(Y;V) \quad (6)$$
$$\Delta \leq \min(H(X), R_y)\Big\} \quad (7)$$

where the joint distribution of the involved random variables is as follows:

$$p(x,y,v) = p(x,y)p(v|y) \quad (8)$$

and it suffices to consider such distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 2$.

The proof of Theorem 2 is given in the Appendix.

The achievability scheme which yields the rate region described in Theorem 2 is summarized as follows.

1) Helen describes the source Y^n to both Bob and Alice through a coded output V^n.
2) Given the coded output V^n, Alice can narrow down the set of conditionally typical X^n-sequences, which are approximately $2^{nH(X|V)}$. Furthermore, for n sufficiently large, the observed x^n-sequence would belong to this set with high probability. Alice sends the index of the observed sequence corresponding to the conditionally typical set for the received coded output.

Therefore, the main difference between the achievability schemes for Theorems 1 and 2 is at the encoding at Alice. Our encoding scheme at Alice for the case of two-sided helper comprises of the following key step: using the coded side information and the source sequence, Alice narrows down the uncertainty at Bob by considering the set of typical X-sequences given the coded output from Helen. She then transmits the index to which the observed X^n-sequence falls in this set. The key observation is that the helper's output is two-sided and *secure* (i.e., only available at Alice and Bob), and Eve only gets to observe the index of the X sequence sent by Alice. Without any knowledge of the V^n-sequence, from Eve's point of view, the correct X^n-sequence could have resulted from any of the 2^{nR_y} conditionally typical sets, each corresponding to the total number of V^n-sequences, and thus, the resulting equivocation at Eve is $\min(H(X), R_y)$.

Remark 1: Besides reflecting the fact that the uncertainty at Eve can be strictly larger than the case of a one-sided helper, Theorem 2 has another interesting interpretation. If Alice and Helen can use sufficiently large rates to securely transmit the source X^n to Bob, then the helper can simply transmit a secret key of entropy $H(X)$ to both Alice and Bob. Alice can then use this secret key to losslessly transmit the source to Bob in perfect secrecy by using a one-time pad [1]. In other words, when R_x and R_y are larger than $H(X)$, one can immediately obtain this result from Theorem 2 by selecting V to be independent of (X, Y) and uniformly distributed on $\{1, \ldots, |\mathcal{X}|\}$. Perhaps the most interesting aspect of the result in Theorem 2 is that for an arbitrary R_y, the two-sided coded output V plays the dual role of providing security and reducing rate of transmission from Alice.

Remark 2: Now consider the model where the side information Y^n is of the form $Y^n = X^n \oplus B^n$, where $|\mathcal{B}| = |\mathcal{X}|$, and B^n is independent of X^n. Moreover, assume that the side information Y^n is available to both Alice and Bob in an *uncoded* manner. For this model, it follows from [10] that, to maximize the uncertainty at the eavesdropper, Alice cannot do any better than describing the error sequence B^n to Bob. Note that our two-sided helper model differs from this model in two aspects:

first, in our case, the common side information available to Alice and Bob is *coded* and rate-limited, second, the sources in our model do not have to be in modulo-additive form.

C. Additional Uncoded Side Information at Bob

We next present extensions of Theorems 1 and 2 to the case in which Bob has additional correlated side information W^n, and we assume that $Y \rightarrow X \rightarrow W$ forms a Markov chain.

Theorem 3: The set of achievable rate triples $\mathcal{R}^W_{\text{1-sided}}$ for secure source coding with one-sided helper and side information W at Bob is given as

$$\mathcal{R}^W_{\text{1-sided}} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|W,V) \quad (9)$$
$$R_y \geq I(Y;V|W) \quad (10)$$
$$\Delta \leq I(X;V,W)\Big\} \quad (11)$$

where the joint distribution of the involved random variables is as follows:

$$p(x,w,y,v) = p(x,w)p(y|x)p(v|y) \quad (12)$$

and it suffices to consider such distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 3$.

Theorem 4: The set of achievable rate triples $\mathcal{R}^W_{\text{2-sided}}$ for secure source coding with two-sided helper and side information W at Bob is given as

$$\mathcal{R}^W_{\text{2-sided}} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|W,V) \quad (13)$$
$$R_y \geq I(Y;V|W) \quad (14)$$
$$\Delta \leq \min(H(X), R_y + I(X;W))\Big\} \quad (15)$$

where the joint distribution of the involved random variables is as follows:

$$p(x,w,y,v) = p(x,w)p(y|x)p(v|y) \quad (16)$$

and it suffices to consider such distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 3$.

The proofs of Theorems 3 and 4 are given in the Appendix.

III. Example: Binary Symmetric Sources

In this section, we compare the rate-equivocation tradeoffs presented in Theorems 1 and 2 for a pair of binary sources.

Let X and Y be binary sources with $X \sim \text{Ber}(1/2)$, $Y \sim \text{Ber}(1/2)$ and $X = Y \oplus E$, where $E \sim \text{Ber}(\delta)$. For this pair of sources, the region described in Theorem 1 can be completely characterized as

$$\mathcal{R}_{\text{1-sided}}(R_y) = \big\{(R_x, \Delta) : R_x \geq h(\delta * h^{-1}(1-R_y))$$
$$\Delta \leq 1 - h(\delta * h^{-1}(1-R_y))\big\} \quad (17)$$

and the region in Theorem 2 can be completely characterized as

$$\mathcal{R}_{\text{2-sided}}(R_y) = \big\{(R_x, \Delta) : R_x \geq h(\delta * h^{-1}(1-R_y))$$
$$\Delta \leq \min(R_y, 1)\big\} \quad (18)$$

where $h(.)$ is the binary entropy function, and $a * b = a(1-b) + b(1-a)$.

We start with the derivation of (17). Without loss of generality, we assume that $R_y \leq H(Y)$. Achievability follows by selecting $V = Y \oplus N$, where $N \sim \text{Ber}(\alpha)$, where

$$\alpha = h^{-1}(1-R_y). \quad (19)$$

Substituting, we obtain

$$H(X|V) = h(\delta * h^{-1}(1-R_y)) \quad (20)$$
$$I(X;V) = 1 - h(\delta * h^{-1}(1-R_y)) \quad (21)$$

which completes the achievability. Note that Y is independent of E, and the random variables X, Y, and V form a Markov chain, i.e., $X \rightarrow Y \rightarrow V$. Using this Markov chain, the converse follows by simple application of Mrs. Gerber's lemma [12] as follows. Let us be given $R_y \in (0,1)$. We have

$$R_y \geq I(Y;V) \quad (22)$$
$$= H(Y) - H(Y|V) \quad (23)$$
$$= 1 - H(Y|V) \quad (24)$$

which implies $H(Y|V) \geq 1 - R_y$. Mrs. Gerber's lemma states that for $X = Y \oplus E$, with $E \sim \text{Ber}(\delta)$, if $H(Y|V) \geq \beta$, then $H(X|V) \geq h(\delta * h^{-1}(\beta))$. We, therefore, have

$$R_x \geq H(X|V) \quad (25)$$
$$\geq h(\delta * h^{-1}(1-R_y)) \quad (26)$$

and

$$\Delta \leq I(X;V) \quad (27)$$
$$= H(X) - H(X|V) \quad (28)$$
$$= 1 - H(X|V) \quad (29)$$
$$\leq 1 - h(\delta * h^{-1}(1-R_y)). \quad (30)$$

This completes the converse.

The rate from Alice, R_x and the equivocation Δ for the cases of one-sided and two-sided helper are shown in Fig. 3 for the case when $\delta = 0.05$. For the one-sided helper, we can observe a tradeoff in the amount of information Alice needs to send versus the uncertainty at Eve. For small values of R_y, Alice needs to send more information thereby leaking out more information to Eve. The amount of information leaked (i.e., $I(X;V) = H(X) - \Delta$) has a one to one relationship to the information sent by Alice. On the other hand, for the case of two-sided helper, the uncertainty at the eavesdropper is always strictly larger than the uncertainty in the one-sided case. Also note that for this pair of sources, perfect secrecy is possible for the case of two-sided helper when $R_y \geq H(Y)$ which is not possible for the case of one-sided helper.

IV. Conclusion

In this paper, we considered several secure source coding problems. We first provided the characterization of the rate-equivocation region for a secure source coding problem with coded side information at the legitimate user. We next extended this result to the case in which the helper is two-sided, i.e., its

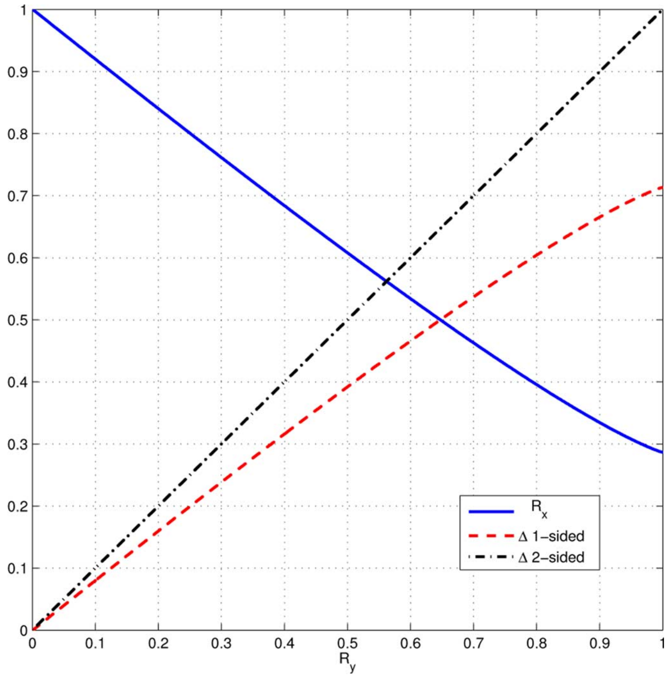

Fig. 3. Rate-equivocation region for a pair of binary symmetric sources.

output is available at both Alice and Bob. We characterized the rate-equivocation region for the case of two-sided helper. The value of two-sided coded side information is emphasized by comparing the respective equivocations for a pair of binary sources. It is shown that Slepian–Wolf binning alone is insufficient and using our achievable scheme, one attains strictly larger uncertainty at the eavesdropper than the case of one-sided helper. Finally, these results are extended to the case in which Bob has access to additional uncoded side information W. Under the assumption that $Y \to X \to W$ forms a Markov chain, the rate-equivocation tradeoffs have been characterized for both one-sided and two-sided scenarios.

Appendix

Proof of Theorem 1:

A) Achievability: Fix the distribution $p(x, y, v) = p(x, y)p(v|y)$.

1) Codebook generation at Helen: From the conditional probability distribution $p(v|y)$ compute $p(v) = \sum_y p(y)p(v|y)$. Generate 2^{nR_y} codewords $v(l)$ independently according to $\prod_{i=1}^n p(v_i)$, where $l = 1, \ldots, 2^{nR_y}$.
2) Codebook generation at Alice: Randomly bin the x^n sequences into $2^{nH(X|V)}$ bins and index these bins as $m = 1, \ldots, M$, where $M = 2^{nH(X|V)}$.
3) Encoding at Helen: On observing the sequence y^n, Helen tries to find a sequence $v(l)$ such that $(v(l), y^n)$ are jointly typical. From rate-distortion theory, we know that there exists one such sequence as long as $R_y \geq I(V; Y)$. Helen sends the index l of the sequence $v(l)$.
4) Encoding at Alice: On observing the sequence x^n, Alice finds the bin index m_X in which the sequence x^n falls and transmits the bin index m_X.
5) Decoding at Bob: On receiving l and the bin index m_X, Bob tries to find a unique x^n sequence in bin m_X such that $(v(l), x^n)$ are jointly typical. This is possible since the number of x^n sequences in each bin is roughly $2^{nH(X)}/2^{nH(X|V)}$ which is $2^{nI(X;V)}$. The existence of an x^n such that $(v(l), x^n)$ are jointly typical is guaranteed by the Markov lemma [13] and the uniqueness is guaranteed by the properties of jointly typical sequences [13].
6) Equivocation:

$$\begin{aligned} H(X^n|m_X) &= H(X^n, m_X) - H(m_X) && (31)\\ &= H(X^n) + H(m_X|X^n) - H(m_X) && (32)\\ &= H(X^n) - H(m_X) && (33)\\ &\geq H(X^n) - \log(M) && (34)\\ &= H(X^n) - nH(X|V) && (35)\\ &= nI(X; V). && (36)\end{aligned}$$

Therefore

$$\Delta \leq I(X; V) \tag{37}$$

is achievable. This completes the achievability part.

B) Converse: Let the output of the helper be J_y, and the output of Alice be J_x, i.e.,

$$\begin{aligned} J_y &= f_y(Y^n) && (38)\\ J_x &= f_x(X^n). && (39)\end{aligned}$$

First note that, for noiseless reconstruction of the sequence X^n at the legitimate decoder, we have by Fano's inequality

$$H(X^n|J_x, J_y) \leq n\epsilon_n. \tag{40}$$

We start by obtaining a lower bound on R_x, the rate of Alice, as follows:

$$\begin{aligned} nR_x &\geq H(J_x) && (41)\\ &\geq H(J_x|J_y) && (42)\\ &= H(X^n, J_x|J_y) - H(X^n|J_x, J_y) && (43)\\ &\geq H(X^n, J_x|J_y) - n\epsilon_n && (44)\\ &\geq H(X^n|J_y) - n\epsilon_n && (45)\\ &= \sum_{i=1}^n H(X_i|X^{i-1}, J_y) - n\epsilon_n && (46)\\ &= \sum_{i=1}^n H(X_i|V_i) - n\epsilon_n && (47)\\ &= nH(X_Q|V_Q, Q) - n\epsilon_n && (48)\\ &= nH(X|V) - n\epsilon_n && (49)\end{aligned}$$

where (44) follows by (40). In (47), we have defined

$$V_i = (J_y, X^{i-1}). \tag{50}$$

In (49), we have defined

$$X = X_Q, \quad V = (Q, V_Q) \tag{51}$$

where Q is uniformly distributed on $\{1, \ldots, n\}$ and is independent of all other random variables.

Next, we obtain a lower bound on R_y, the rate of the helper,

$$\begin{align} nR_y &\geq H(J_y) \tag{52}\\ &\geq I(J_y;Y^n) \tag{53}\\ &= \sum_{i=1}^{n} I(J_y, Y^{i-1}; Y_i) \tag{54}\\ &= \sum_{i=1}^{n} I(J_y, Y^{i-1}, X^{i-1}; Y_i) \tag{55}\\ &\geq \sum_{i=1}^{n} I(J_y, X^{i-1}; Y_i) \tag{56}\\ &= \sum_{i=1}^{n} I(V_i; Y_i) \tag{57}\\ &= nI(V_Q; Y_Q|Q) \tag{58}\\ &= nI(V;Y) \tag{59} \end{align}$$

where (55) follows from the Markov chain

$$X^{i-1} \rightarrow (J_y, Y^{i-1}) \rightarrow Y_i \tag{60}$$

and in (59), we have defined $Y = Y_Q$.

We now have the main step, i.e., an upper bound on the equivocation rate of the eavesdropper

$$\begin{align} H(X^n|J_x) &= H(X^n, J_y|J_x) - H(J_y|X^n, J_x) \tag{61}\\ &= H(J_y|J_x) - H(J_y|X^n, J_x) + H(X^n|J_x, J_y) \tag{62}\\ &= H(J_y|J_x) - H(J_y|X^n) + H(X^n|J_x, J_y) \tag{63}\\ &\leq H(J_y) - H(J_y|X^n) + H(X^n|J_x, J_y) \tag{64}\\ &\leq I(J_y; X^n) + n\epsilon_n \tag{65}\\ &= \sum_{i=1}^{n} I(J_y; X_i|X^{i-1}) + n\epsilon_n \tag{66}\\ &= \sum_{i=1}^{n} I(J_y, X^{i-1}; X_i) + n\epsilon_n \tag{67}\\ &= \sum_{i=1}^{n} I(X_i; V_i) + n\epsilon_n \tag{68}\\ &= nI(X_Q; V_Q|Q) + n\epsilon_n \tag{69}\\ &= nI(X;V) + n\epsilon_n \tag{70} \end{align}$$

where (63) follows from the Markov chain

$$J_x \rightarrow X^n \rightarrow J_y \tag{71}$$

and (65) follows from (40). This implies

$$\Delta \leq I(X;V). \tag{72}$$

Also note that the following is a Markov chain:

$$V \rightarrow Y \rightarrow X. \tag{73}$$

Therefore, the joint distribution of the involved random variables is

$$p(x,y,v) = p(x,y)p(v|y). \tag{74}$$

From support lemma [14], it can be shown that it suffices to consider such joint distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 2$.

In (50), we have defined the auxiliary random variable as $V_i = (J_y, X^{i-1})$. We remark here that the converse for Theorem 1 can also be proved by defining, $V_i = (J_y, Y^{i-1})$ as in [13, Sec. 14.8]. Note that due to the fact that the sources (X^n, Y^n) are generated in an i.i.d. manner, the following is a Markov chain:

$$(J_y, Y^{i-1}, X^{i-1}) \rightarrow Y_i \rightarrow X_i. \tag{75}$$

This is due to the fact that X_i does not carry any extra information about $(J_y = f_y(Y^n), Y^{i-1}, X^{i-1})$ that is not there in Y_i. Therefore, (75) implies that the following are also valid Markov chains:

$$\begin{align} (J_y, X^{i-1}) &\rightarrow Y_i \rightarrow X_i \tag{76}\\ (J_y, Y^{i-1}) &\rightarrow Y_i \rightarrow X_i \tag{77} \end{align}$$

and the converse for Theorem 1 can be proved by defining $V_i = (J_y, X^{i-1})$ or $V_i = (J_y, Y^{i-1})$.

Proof of Theorem 2:

A) Achievability: Fix the distribution $p(x,y,v) = p(x,y)p(v|y)$.

1) Codebook generation at Helen: From the conditional probability distribution $p(v|y)$ compute $p(v) = \sum_y p(y)p(v|y)$. Generate 2^{nR_y} codewords $v(l)$ independently according to $\prod_{i=1}^{n} p(v_i)$, where $l = 1, \ldots, 2^{nR_y}$.
2) Encoding at Helen: On observing the sequence y^n, Helen tries to find a sequence $v(l)$ such that $(v(l), y^n)$ are jointly typical. If there exists such a sequence $v(l)$, it sends the index l to Alice and Bob; otherwise, it sends a fixed index $l = 0$.
3) Encoding at Alice: The key difference from the one-sided helper case is in the encoding at Alice. Let $\mathcal{E}_H = 1$ denote the event that the encoding at Helen succeeds, i.e., there exists at least one l such that $(v(l), y) \in T^n_{YV}$. The probability of this event can be made arbitrarily close to 1, for n sufficiently large as long as $R_y \geq I(Y;V)$. If $\mathcal{E}_H = 1$, Alice receives the index l of the sequence $v(l)$, otherwise it receives the fixed index $l = 0$.

   Conditioned on the event $\mathcal{E}_H = 1$, we note the following:
   a) $P(L = l|\mathcal{E}_H = 1) \approx 2^{-nR_y}$, for $l = 1, \ldots, 2^{nR_y}$, i.e., any of the L indices are approximately equally likely[2] to be sent given $\mathcal{E}_H = 1$ for n sufficiently large.
   b) For each possible sequence $v(l)$ received from Helen, and given that $(v(l), y^n) \in T^n_{YV}$, we denote the set of conditional typical X-sequences given $v(l)$ as $T^n_{X|v(l)}$, for $l = 1, \ldots, 2^{nR_y}$.
   c) From Markov lemma, we have that $P((X^n, v(l)) \in T_{X|v(l)}|\mathcal{E}_H = 1, L = l) \geq 1 - \epsilon_n$, where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$, i.e., the observed x^n sequence at Alice will

[2] Formally, by the notation $P(A = a) \approx 2^{-nR}$, we refer to the following: $P(A = a) \in [2^{-n(R+\delta_n)}, 2^{-n(R-\delta_n)}]$, for some sequence δ_n such that $\delta_n \rightarrow 0$ as $n \rightarrow \infty$.

belong to the conditional typical set $T^n_{X|v(l)}$ with high probability.

d) For n sufficiently large, we have $|T^n_{X|v(l)}| \approx 2^{nH(X|V)}$. Enumerate the sequences as $j = 1, \ldots, 2^{nH(X|V)}$.

e) The set of x-sequences belonging to $T^n_{X|v(l)}$ are approximately uniformly distributed, i.e., $P(X^n = x^n | X^n \in T^n_{X|v(l)}) \approx 2^{-nH(X|V)}$.

f) For any $l \neq l'$, the sets $T^n_{X|v(l)}$ and $T^n_{X|v(l')}$ are disjoint, i.e., $|T^n_{X|v(l)} \cap T^n_{X|v(l')}| \leq \epsilon_n$, where $\epsilon_n \to 0$ as $n \to \infty$.

On observing the sequence x^n and obtaining $v(l)$ from Helen, Alice sends the index j corresponding to the conditionally typical set $T^n_{X|v(l)}$.

4) Decoding at Bob: On receiving the pair $(v(l), j)$ from Alice and Helen, Bob declares its estimate of X as the jth x^n-sequence belonging to the set $T^n_{X|v(l)}$. For n sufficiently large, decoding at Bob will succeed with high probability.

5) Equivocation:

$$\begin{aligned} &H(X^n|J_x)\\ &\geq H(X^n|J_x, \mathcal{E}_H) \quad (78)\\ &= \sum_j P(J_x = j, \mathcal{E}_H = 1) H(X^n|J_x = j, \mathcal{E}_H = 1)\\ &\quad + \sum_j P(J_x = j, \mathcal{E}_H = 0) H(X^n|J_x = j, \mathcal{E}_H = 0) \quad (79)\\ &\geq \sum_j P(J_x = j, \mathcal{E}_H = 1) H(X^n|J_x = j, \mathcal{E}_H = 1). \quad (80) \end{aligned}$$

Next, we note that given $J_x = j$ and $\mathcal{E}_H = 1$, X^n can take 2^{nR_y} values, i.e., there are a total of 2^{nR_y} x^n-sequences, each corresponding to the jth sequence in the (approximately) disjoint sets $T^n_{X|v(l)}$, for $l = 1, \ldots, 2^{nR_y}$, and each equally likely. Therefore, we have $P(X^n = x^n | J_x = j, \mathcal{E}_H = 1) \approx 2^{-nR_y}$. Using this, we next lower bound each of the conditional entropy terms appearing in the summation of (80) as follows:

$$\begin{aligned} &H(X^n|J_x = j, \mathcal{E}_H = 1)\\ &= \sum_{x^n: J_x = j, \mathcal{E}_H = 1} P(X^n = x^n | J_x = j, \mathcal{E}_H = 1) \cdot\\ &\qquad \log\left(\frac{1}{P(X^n = x^n | J_x = j, \mathcal{E}_H = 1)}\right) \quad (81)\\ &\geq \sum_{x^n: J_x = j, \mathcal{E}_H = 1} P(X^n = x^n | J_x = j, \mathcal{E}_H = 1) \cdot\\ &\qquad \log\left(\frac{1}{2^{-n(R_y - \epsilon_n)}}\right) \quad (82)\\ &= n(R_y - \epsilon_n) \cdot\\ &\qquad \sum_{x^n: J_x = j, \mathcal{E}_H = 1} P(X^n = x^n | J_x = j, \mathcal{E}_H = 1) \quad (83)\\ &= n(R_y - \epsilon_n). \quad (84) \end{aligned}$$

Substituting (84) into (80), we obtain

$$\begin{aligned} &H(X^n|J_x)\\ &\geq \sum_j P(J_x = j, \mathcal{E}_H = 1) H(X^n|J_x = j, \mathcal{E}_H = 1) \quad (85)\\ &\geq n(R_y - \epsilon_n) \sum_j P(J_x = j, \mathcal{E}_H = 1) \quad (86)\\ &\geq n(R_y - \epsilon_n)(1 - \epsilon_n). \quad (87) \end{aligned}$$

Normalizing (87) by n and taking the limit $n \to \infty$, we obtain

$$\begin{aligned} \lim_{n\to\infty} \frac{H(X^n|J_x)}{n} &\geq R_y \quad (88)\\ &\geq \min(H(X), R_y). \quad (89) \end{aligned}$$

B) Converse: The only difference in the converse part for the case of two-sided helper is for the equivocation at the eavesdropper:

$$\begin{aligned} H(X^n|J_x) &= H(X^n, J_y|J_x) - H(J_y|X^n, J_x) \quad (90)\\ &= H(J_y|J_x) - H(J_y|X^n, J_x) + H(X^n|J_x, J_y) \quad (91)\\ &\leq H(J_y|J_x) + n\epsilon_n \quad (92)\\ &\leq H(J_y) + n\epsilon_n \quad (93)\\ &\leq nR_y + n\epsilon_n \quad (94) \end{aligned}$$

where (92) follows from Fano's inequality. Furthermore, we have the trivial upper bound $H(X^n|J_x) \leq H(X^n) = nH(X)$. This implies the desired bound for equivocation:

$$\Delta \leq \min(H(X), R_y). \quad (95)$$

Proofs of Theorems 3 and 4:

A) Converse Proofs: The proofs for lower bounds on R_x and R_y for both Theorems 3 and 4 are the same and we present these jointly. Later in this section, we present separate proofs for equivocation for each of the theorems.

Let the coded output of the helper be denoted as J_y, and the output of Alice be denoted as J_x, i.e.,

$$J_y = f_y(Y^n), \qquad \text{and} \qquad J_x = f_x(X^n, J_y). \quad (96)$$

First note that, for noiseless reconstruction of the sequence X^n at Bob, we have by Fano's inequality

$$H(X^n|J_x, J_y, W^n) \leq n\epsilon_n. \quad (97)$$

We start by obtaining a lower bound on R_x, the rate of Alice, as follows:

$$nR_x \geq H(J_x) \tag{98}$$
$$\geq H(J_x|J_y, W^n) \tag{99}$$
$$= H(X^n, J_x|J_y, W^n) - H(X^n|J_x, J_y, W^n) \tag{100}$$
$$\geq H(X^n, J_x|J_y, W^n) - n\epsilon_n \tag{101}$$
$$\geq H(X^n|J_y, W^n) - n\epsilon_n \tag{102}$$
$$= \sum_{i=1}^{n} H(X_i|X^{i-1}, J_y, W^n) - n\epsilon_n \tag{103}$$
$$= \sum_{i=1}^{n} H(X_i|J_y, X^{i-1}, W_{i+1}^n, W_i) - n\epsilon_n \tag{104}$$
$$\geq \sum_{i=1}^{n} H(X_i|J_y, Y^{i-1}, X^{i-1}, W_{i+1}^n, W_i) - n\epsilon_n \tag{105}$$
$$= \sum_{i=1}^{n} H(X_i|V_i, W_i) - n\epsilon_n \tag{106}$$
$$= nH(X|V, W) - n\epsilon_n \tag{107}$$

where (101) follows by (97) and (104) follows from the following Markov chain:

$$W^{i-1} \rightarrow (J_y, X^{i-1}, W_{i+1}^n, W_i) \rightarrow X_i \tag{108}$$

and in (106), we have defined

$$V_i \triangleq (J_y, Y^{i-1}, X^{i-1}, W_{i+1}^n). \tag{109}$$

We next obtain a lower bound on R_y:

$$nR_y \geq H(J_y) \tag{110}$$
$$\geq H(J_y|W^n) \tag{111}$$
$$\geq I(Y^n; J_y|W^n) \tag{112}$$
$$= \sum_{i=1}^{n} H(Y_i|W_i) - H(Y^n|J_y, W^n) \tag{113}$$
$$= \sum_{i=1}^{n} H(Y_i|W_i) - \sum_{i=1}^{n} H(Y_i|W_i, J_y, Y^{i-1}, W_{i+1}^n, W^{i-1}) \tag{114}$$
$$= \sum_{i=1}^{n} H(Y_i|W_i) - \sum_{i=1}^{n} H(Y_i|W_i, J_y, Y^{i-1}, W_{i+1}^n) \tag{115}$$
$$= \sum_{i=1}^{n} H(Y_i|W_i) - \sum_{i=1}^{n} H(Y_i|W_i, J_y, Y^{i-1}, X^{i-1}, W_{i+1}^n) \tag{116}$$
$$= \sum_{i=1}^{n} H(Y_i|W_i) - \sum_{i=1}^{n} H(Y_i|W_i, V_i) \tag{117}$$
$$= nI(Y; V|W) \tag{118}$$

where in (115) and (116), we have used the Markov chain

$$(Y_i, J_y, W_i) \rightarrow Y^{i-1} \rightarrow (X^{i-1}, W^{i-1}) \tag{119}$$

which follows from the fact that the sources $\{X_i, Y_i, W_i\}_{i=1}^n$ are generated i.i.d., and J_y is a function of Y^n.

1) Equivocation: one-sided helper

We have the following sequence of upper bounds on the equivocation rate of the eavesdropper:

$$H(X^n|J_x)$$
$$= H(X^n, J_y, W^n|J_x) - H(J_y, W^n|X^n, J_x) \tag{120}$$
$$= H(J_y, W^n|J_x) - H(J_y, W^n|X^n, J_x) + H(X^n|J_x, J_y, W^n) \tag{121}$$
$$\leq H(J_y, W^n|J_x) - H(J_y, W^n|X^n, J_x) + n\epsilon_n \tag{122}$$
$$= H(J_y, W^n|J_x) - H(J_y, W^n|X^n) + n\epsilon_n \tag{123}$$
$$\leq H(J_y, W^n) - H(J_y, W^n|X^n) + n\epsilon_n \tag{124}$$
$$= I(X^n; J_y, W^n) + n\epsilon_n \tag{125}$$
$$= \sum_{i=1}^{n} I(X_i; J_y, W^n|X^{i-1}) + n\epsilon_n \tag{126}$$
$$= \sum_{i=1}^{n} I(X_i; J_y, W^n, X^{i-1}) + n\epsilon_n \tag{127}$$
$$\leq \sum_{i=1}^{n} I(X_i; J_y, W^n, X^{i-1}, Y^{i-1}) + n\epsilon_n \tag{128}$$
$$= \sum_{i=1}^{n} I(X_i; W_i, J_y, W_{i+1}^n, X^{i-1}, Y^{i-1}) + n\epsilon_n \tag{129}$$
$$= \sum_{i=1}^{n} I(X_i; W_i, V_i) + n\epsilon_n \tag{130}$$
$$= nI(X; W, V) + n\epsilon_n. \tag{131}$$

2) Equivocation: two-sided helper

We have the following sequence of upper bounds on the equivocation rate of the eavesdropper:

$$H(X^n|J_x)$$
$$= H(X^n, J_y, W^n|J_x) - H(J_y, W^n|X^n, J_x) \tag{132}$$
$$= H(J_y, W^n|J_x) - H(J_y, W^n|X^n, J_x) + H(X^n|J_x, J_y, W^n) \tag{133}$$
$$\leq H(J_y) + H(W^n) - H(W^n|X^n, J_x) + n\epsilon_n \tag{134}$$
$$= H(J_y) + H(W^n) - H(W^n|X^n) + n\epsilon_n \tag{135}$$
$$= H(J_y) + nI(X; W) + n\epsilon_n \tag{136}$$
$$\leq n(R_y + I(X; W)) + n\epsilon_n \tag{137}$$

where (134) follows from (97), and (135) follows from the fact that $Y^n \rightarrow X^n \rightarrow W^n$, and hence $J_x \rightarrow X^n \rightarrow W^n$, since J_x is a function of (X^n, J_y).

Furthermore, we have the trivial upper bound $H(X^n|J_x) \leq H(X^n) = nH(X)$. This implies the desired bound for equivocation:

$$\Delta \leq \min(H(X), R_y + I(X; W)). \tag{138}$$

B) Achievability:

1) Achievability for two-sided Helper

The achievability proof for Theorem 4 closely follows that of Theorem 2.

1) Encoding at Helen: As in the proof for Theorem 2, Helen generates $2^{nI(V;Y)}$ i.i.d. sequences, $v(l)$ from the distribution $p(v)$. Next, she independently bins these sequences in $2^{nI(Y;V|W)}$ bins; and enumerates these bin indices as $b_v = 1, 2, \ldots, 2^{nI(Y;V|W)}$. Upon observing y^n, she searches for a $v(l)$ such that $(v(l), y^n)$ are joint typical. If successful, it transmits the bin-index of the chosen v-sequence. The number of sequences in each bin is approximately $2^{nI(V;W)}$ and thus upon receiving the bin-index $B(V)$ from Helen, Bob can correctly decode the v-sequence (using joint typical decoding). Also, since $Y \to X \to W$, we have $I(V;W) \le I(V;X)$, and hence Alice can also correctly decode the v-sequence. As in the previous section, we denote $\mathcal{E}_H = 1$ as the event that Helen's encoding is successful, the probability of which can be made arbitrarily close to 1 by making n sufficiently large and by choosing $R_y \ge I(Y;V) - I(Y;W) = I(Y;V|W)$.
2) Encoding at Alice: Given that $\mathcal{E}_H = 1$, a random X^n sequence will belong to the conditional typical set $T^n_{X|\hat{v}(l)}$, where $\hat{v}(l)$ is the v-sequence that Alice decodes upon receiving the bin-index $B(V)$. Alice further bins the set of x-sequences belonging to $T^n_{X|\hat{v}(l)}$ into $2^{nH(X|W,V)}$ bins and denotes these as $b_x = 1, \ldots, 2^{nH(X|W,V)}$, so that the number of x-sequences in each bin is approximately $2^{nI(X;W|V)}$. Alice sends the bin-index $B(X)$ in which the observed x^n-sequence falls corresponding to the conditionally typical set $T^n_{X|\hat{v}(l)}$. The total rate required by Alice is therefore $H(X|W,V)$.
3) Decoding at Bob: Upon receiving $B(V)$ from Helen and $B(X)$ from Alice, Bob first decodes v by searching for a unique $\hat{v} \in B(V)$ such that $(\hat{v}, w^n)$ are joint typical. The probability of decoding error in estimating v at Bob goes to 0 as $n \to \infty$ since the number of v sequences in each bin is approximately $2^{nI(V;W)}$. Bob then looks in the $B(X)$th bin in the set $T^n_{X|\hat{v}}$; and searches for a unique $\hat{x}^n$ in this set such that $(\hat{x}^n, \hat{v}, w^n)$ are joint typical. This step will lead to a successful decoding at Bob since the number of x-sequences in each such bin is approximately $2^{nI(X;W|V)}$.
4) Equivocation: As in the proof for Theorem 2, we follow the same sequence of lower bounds to arrive at

$$\begin{aligned} &H(X^n|B(X)) \\ &\ge \sum_j P(B(X)=j, \mathcal{E}_H = 1) \cdot \\ &\qquad H(X^n|B(X)=j, \mathcal{E}_H = 1). \end{aligned} \tag{139}$$

We next note that conditioned on the event $\mathcal{E}_H = 1$, and given $B(X) = j$, there are a total of $2^{nI(X;W|V)}$ sequences in each of the bins; and each bin could have resulted from any of the $2^{n(R_y+I(W;V))}$ v-sequences. Thus, there are a total of $2^{n(R_y+I(W;V)+I(X;W|V))} = 2^{n(R_y+I(X;W))}$ equally likely x^n-sequences conditioned on $B(X) = j$ and $\mathcal{E}_H = 1$. We therefore have $P(X^n = x^n|B(X) = j, \mathcal{E}_H = 1) \approx 2^{-n(R_y+I(X;W))}$. Using this, we can bound

$$\begin{aligned} &H(X^n|B(X)=j, \mathcal{E}_H = 1) \\ &\qquad \ge n(R_y + I(X;W) - \epsilon_n). \end{aligned} \tag{140}$$

Upon substituting (140) into (139), and letting $n \to \infty$, we obtain at the resulting equivocation of this scheme as

$$\begin{aligned} \lim_{n\to\infty} \frac{H(X^n|B(X))}{n} & \\ &\ge R_y + I(X;W) &(141)\\ &\ge \min(H(X), R_y + I(X;W)). &(142) \end{aligned}$$

2) Achievability for one-sided Helper.

Encoding at Helen remains the same as the two-sided helper case, i.e., Helen quantizes Y^n to V^n and performs binning with respect to W^n. The encoding at Alice is to independently and uniformly bin the set of X-sequences in $2^{nH(X|W,V)}$ bins and it sends the bin index $B(X^n)$. The only difference is in the equivocation proof:

$$\begin{aligned} &H(X^n|B(X^n)) \\ &= H(X^n) - I(X^n; B(X^n)) &(143)\\ &= nH(X) - H(B(X^n)) + H(B(X^n)|X^n) &(144)\\ &= nH(X) - H(B(X^n)) &(145)\\ &\ge nH(X) - \log(|B(X^n)|) &(146)\\ &\ge nH(X) - \log(2^{nH(X|W,V)}) &(147)\\ &= nI(X;W,V) &(148) \end{aligned}$$

where in (145), we used the fact that $B(X^n)$ is a deterministic function of X^n. We, therefore, have

$$\lim_{n\to\infty} \frac{H(X^n|B(X))}{n} \ge I(X;W,V). \tag{149}$$

ACKNOWLEDGMENT

We are grateful to the Associate Editor Ioannis Kontoyiannis and the anonymous reviewers for their helpful suggestions.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1335–1387, Jan. 1975.
[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[4] R. Ahlswede and J. Korner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 6, pp. 629–637, Nov. 1975.

[5] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 3, pp. 294–300, May 1975.

[6] D. Gunduz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Inf. Theory Workshop*, 2008, pp. 169–173.

[7] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. IEEE Inf. Theory Workshop*, 2007, pp. 442–447.

[8] W. Luh and D. Kundur, "Distributed keyless secret sharing over noiseless channels," in *Proc. IEEE Global Commun. Conf.*, 2007, pp. 44–48.

[9] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, 2008, pp. 111–115.

[10] L. Grokop, A. Sahai, and M. Gastpar, "Discriminatory source coding for a noiseless broadcast channel," in *Proc. IEEE Int. Symp. Inf. Theory*, 2005, pp. 77–81.

[11] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Proc. 47th Annu. Allerton Conf. Commun., Control Comput.*, 2009, pp. 1061–1068.

[12] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications-I," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 6, pp. 769–772, Nov. 1973.

[13] T. M. Cover and J. A. Thomas*, Elements of Information Theory*. New York: Wiley, 1991.

[14] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981.

[15] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, arXiv:1105.1658, submitted for publication.

[16] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. 48th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, 2010, pp. 733–739.

Ravi Tandon (S'03–M'09) received the B.Tech. degree in Electrical Engineering from the Indian Institute of Technology (IIT), Kanpur in 2004 and the Ph.D. degree in Electrical and Computer Engineering from the University of Maryland, College Park in 2010. From 2010 until 2012, he was a post-doctoral research associate with Princeton University. In 2012, he joined Virginia Polytechnic Institute and State University (Virginia Tech) at Blacksburg, where he is currently a Research Assistant Professor in the Department of Electrical and Computer Engineering and also with the Hume Center for National Security and Technology. His research interests are in network information theory, communication theory for wireless networks and information theoretic security.

Dr. Tandon is a recipient of the Best Paper Award at the Communication Theory symposium at the 2011 IEEE Global Telecommunications Conference.

Sennur Ulukus (S'90–M'98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010) and IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). She served as a Guest Editor for the *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks (2012), IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks (2011), IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.

Kannan Ramchandran (F'05) received the Ph.D. degree in 1993 from Columbia University, New York. He is currently a Professor of Electrical Engineering and Computer Science at the University of California at Berkeley, where he has been since 1999. Prior to that, he was with the University of Illinois at Urbana-Champaign from 1993 to 1999, and was at AT&T Bell Laboratories from 1984 to 1990. He is a Fellow of the IEEE and has won numerous awards including the Eli Jury thesis award at Columbia, a couple of Best Paper awards from the IEEE Signal Processing Society, a Hank Magnusky Scholar award at Illinois, an Okawa Foundation Research Prize at Berkeley, an Outstanding Teaching Award from the EECS Department at UC Berkeley, and has coauthored several best student paper awards at conferences and workshops. His current research interests include distributed signal processing and coding for wireless systems, coding for distributed storage, peer-to-peer networking and video content delivery, security, and multiuser information and communication theory.