Transmitter Actions for Secure Integrated Sensing and Communication

Truman Welling[1], Onur Günlü[2], and Aylin Yener[1]
[1]Department of Electrical and Computer Engineering, The Ohio State University
[2]Information Theory and Security Laboratory, Linköping University
welling.78@buckeyemail.osu.edu, onur.gunlu@liu.se, yener@ece.osu.edu

***Abstract*—This work models a secure integrated sensing and communication (ISAC) system as a broadcast channel with action-dependent channel states and output feedback. The transmitted message is split into a common and a secure message, both of which must be recovered at the legitimate receiver, while the secure message needs to be kept secret from the eavesdropper. The transmitter actions, such as beamforming vector design, affect the corresponding state distribution at each channel use. The action sequence is modeled to depend on both the transmitted message and channel output feedback. For perfect channel output feedback, the secrecy-distortion regions are provided for physically-degraded and reversely-physically-degraded secure ISAC channels with transmitter actions. The corresponding rate regions when the entire message should be kept secret are also provided. We illustrate the results by characterizing the secrecy-distortion region of a binary example.**

I. Introduction

Modern communication systems have continuously evolved, improving on existing features and seeking ways to expand functionality. One promising facet currently being explored for future systems is joint communication and sensing [1], [2]. The integration of sensing and communication improves spectral and energy efficiencies of systems and reduces hardware cost [3]. The inherent nature of integrated sensing and communication (ISAC) is that sensing any target makes the communication signal available to them. Therefore, security, e.g., information confidentiality [4], should be a fundamental aspect for the formulation of ISAC systems [5]–[7].

Secure ISAC systems have recently been considered in the literature. In [8], a system securely communicating with a single user while sensing other targets uses artificial noise to obfuscate the message. Another approach in [9] uses artificial noise to secure a full duplex ISAC system. The work in [7] models an ISAC system as a state-dependent broadcast channel with channel output feedback, where one user is an eavesdropper from whom some or all of the message should be kept secret. Sensing is performed at the transmitter by estimating the state based on the channel feedback.

In this paper, we extend the secure ISAC model in [7] to the action-dependent set up by introducing transmitter actions which affect the distribution of the states, as in [10]. The transmitter actions can define, e.g., the design of beamforming vectors with aim to improve the advantage of the legitimate receiver over the eavesdropper.

We determine the secrecy-distortion regions for secure ISAC channels with action-dependent states for physically- and reverse-physically-degraded models. For these results, we assume that the transmitted message consists of common and secure parts, i.e., only the latter should be kept secret from the eavesdropper. This scenario is called partial secrecy, as in [7], [11]. We first consider the case where channel output feedback is available at the channel encoder alone. Then, we show that the rate regions continue to hold when the channel feedback is available at the action encoder as well. Our achievability leverages the output statistics of random binning (OSRB) framework in [12]–[14] to provide strong secrecy. Moreover, we simplify the results for the case where the entire message should be kept secret from the eavesdropper, i.e., there is no common message. This provides full secrecy. We characterize the rate region for a binary stochastically-degraded example.

The proposed secure ISAC model can be viewed as extensions of the wiretap channel with feedback models [15]–[22] as well as channel feedback with actions [10], [23]. One main difference, among others, between our model and those in [10], [23] is that we assume knowledge of the transmitter's actions at the channel encoder, rather than non-causal state knowledge.

In Section II, we define the secure ISAC with transmitter actions model. In Section III, we characterize the secrecy-distortion regions for physically- and reversely-physically-degraded ISAC channels with action-dependent states under partial secrecy. We provide the secrecy-distortion regions under full secrecy in Section IV.

II. Problem Definition

We consider the secure ISAC model depicted in Fig. 1, which consists of three parties: i) a transmitter with a channel encoder, action encoder, and state estimator, ii) a legitimate receiver, and iii) an eavesdropper. The transmitter aims to reliably transmit $M = (M_1, M_2) \in \mathcal{M} = (\mathcal{M}_1 \times \mathcal{M}_2)$ to the legitimate receiver over the state-dependent broadcast channel $P_{Y_1,Y_2,Z|S_1,S_2}$ with action-dependent states (S_1, S_2). The transmitter computes the inputs as $X_i = \mathsf{Enc}\big(M, A_i, Z^{i-1}\big) \in \mathcal{X}$ and $A_i = \mathsf{Enc}_{\text{Act}}\big(M, Z^{i-1}\big) \in \mathcal{A}$, where $\mathsf{Enc}(\cdot)$ and $\mathsf{Enc}_{\text{Act}}(\cdot)$ are encoding functions for the channel input and action, respectively, and $Z^{i-1} \in \mathcal{Z}^{i-1}$ is delayed channel output feedback for all $i = [1 : n]$. The legitimate receiver observes $Y_{1,i} \in \mathcal{Y}_1$ and $S_{1,i} \in \mathcal{S}_1$ and should be able to form a reliable

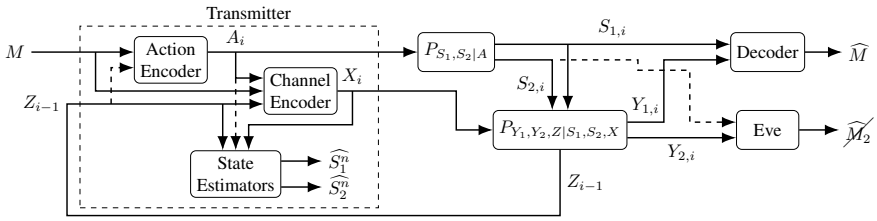

Fig. 1. Secure ISAC model with action-dependent states under partial secrecy, where $M = (M_1, M_2)$ and only M_2 should be kept secret from Eve, for $i = [1:n]$. The action, A_i, is a random function of (M, Z_{i-1}). The channel input, X_i, is a random function of (M, Z_{i-1}, A_i). We consider ISAC with perfect output feedback, where $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$.

estimate $\widehat{M} = \mathsf{Dec}(Y_1^n, S_1^n) \in \widehat{\mathcal{M}}$, where $\mathsf{Dec}(\cdot)$ is a decoding function. The eavesdropper observes $Y_{2,i} \in \mathcal{Y}_2$ and $S_{2,i} \in \mathcal{S}_2$ and should not be able to recover M_2. Finally, the transmitter estimates the states by $\widehat{S_j^n} = \mathsf{Est}_j(A^n, X^n, Z^n) \in \widehat{\mathcal{S}_j^n}$ for $j = 1, 2$, where $\mathsf{Est}_j(\cdot,\cdot,\cdot)$ is an estimation function. All sets $\mathcal{A}, \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{S}_1, \mathcal{S}_2, \widehat{\mathcal{S}_1}, \widehat{\mathcal{S}_2}$ and $\mathcal{Z}$ are finite.

This channel model abstracts an ISAC scenario, where the transmitter has a multi-functional phased array used for both beamforming the transmitter signals, modeled as an action A_i, and observing the resulting reflected waveforms, modeled as the channel output feedback Z_{i-1}, from which they derive information about the legitimate receiver's and eavesdropper's channel states $S_{1,i}$ and $S_{2,i}$, respectively. These states can carry information about, e.g., the locations of the receivers.

To simplify the analysis we consider perfect output feedback, i.e. we have $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$ for all $i = [2:n]$. While perfect output feedback is an integral part of the achievability proofs, some of the converse results continue to hold for generalized feedback. We next define the strong secrecy-distortion region for the secure ISAC model.

Definition 1: A secrecy-distortion tuple (R_1, R_2, D_1, D_2) is *achievable* under partial secrecy if, for any $\delta > 0$, there exists $n \geq 1$, one channel encoder, one action encoder, one decoder, and two estimators $\mathsf{Est}_j(X^n, A^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$, $j \in \{1, 2\}$, such that

$$\frac{1}{n} \log |\mathcal{M}_j| \geq R_j - \delta \qquad \text{for } j = 1, 2 \quad \text{(rate)} \tag{1}$$

$$\Pr\left[(M_1, M_2) \neq (\widehat{M_1}, \widehat{M_2})\right] \leq \delta \qquad \text{(reliability)} \tag{2}$$

$$I(M_2; Y_2^n, S_2^n) \leq \delta \qquad \text{(strong secrecy)} \tag{3}$$

$$\mathbb{E}\left[d_j(S_j^n, \widehat{S_j^n})\right] \leq D_j + \delta \qquad \text{for } j = 1, 2 \quad \text{(distortion)} \tag{4}$$

where $d_j(s^n, \widehat{s^n}) = \frac{1}{n} \sum_{i=1}^n d_j(s_i, \widehat{s}_i)$ for $j = 1, 2$ are bounded per-letter distortion metrics.

The secrecy-distortion region $\mathcal{R}_{\text{PS,Act}}$ is the closure of the set of all achievable tuples under partial secrecy and perfect output feedback. ♢

Remark 1: In [7], the independence of the message and the states allowed the strong secrecy condition (3) to be simplified to $I(M_2; Y_2^n | S_2^n) \leq \delta$. In our model, the action introduces dependence between the message and states, making $I(M_2; S_2^n) \neq 0$, invalidating the simplification $I(M_2; Y_2^n, S_2^n) = I(M_2; Y_2^n | S_2^n)$. Moreover, unlike in [7], the channel input X_i is not independent of the channel states $(S_{1,i}, S_{2,i})$ in our model.

We now define physical degradation for our model, see [2].

Definition 2: An ISAC channel as depicted in Fig.1 is *physically-degraded* if we have

$$\begin{aligned} P_{AXY_1Y_2S_1S_2} &= P_{AX} P_{Y_1S_1Y_2S_2|AX} \\ &= P_{AX} P_{S_1|A} P_{Y_1|S_1X} P_{Y_2S_2|S_1Y_1}. \end{aligned} \tag{5}$$

Similarly, it is *reversely-physically-degraded* if the degradation order is swapped such that

$$\begin{aligned} P_{AXY_1Y_2S_1S_2} &= P_{AX} P_{Y_1S_1Y_2S_2|AX} \\ &= P_{AX} P_{S_2|A} P_{Y_2|S_2X} P_{Y_1S_1|S_2Y_2}. \end{aligned} \tag{6}$$

♢

III. ISAC with Action-dependent States Under Partial Secrecy

We next provide the strong secrecy-distortion regions for the physically- and reverse-physically-degraded secure ISAC channels with transmitter actions. Proof of Theorem 1 is given in Appendix A, see below also for a proof sketch.

Theorem 1: (Physically-degraded): For a physically-degraded ISAC channel with strictly causal feedback available at the action and channel encoders, $\mathcal{R}_{\text{PS,Act}}$ is the union over all joint distributions P_{VAX} of the rate tuples (R_1, R_2, D_1, D_2) satisfying

$$R_1 \leq I(V; Y_1, S_1) \tag{7}$$

$$R_2 \leq \min\{R_2', (I(V; Y_1, S_1) - R_1)\} \tag{8}$$

$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] \qquad \text{for } j = 1, 2 \tag{9}$$

where we have

$$P_{VAXY_1Y_2S_1S_2} = P_{V|AX} P_{AX} P_{S_1|A} P_{Y_1|S_1X} P_{Y_2S_2|S_1Y_1}, \tag{10}$$

$$R_2' = H(Y_1, S_1 | Y_2, S_2) - H(S_1 | Y_1, Y_2, S_2, V) \tag{11}$$

and one can use the deterministic per-letter estimators $\mathsf{Est}_j(a, x, y_1, y_2) = \hat{s}_j$ for $j = 1, 2$ such that

$$\begin{aligned} &\mathsf{Est}_j(a, x, y_1, y_2) \\ &= \operatorname*{argmin}_{\tilde{s} \in \widehat{\mathcal{S}}_j} \sum_{s_j \in \mathcal{S}_j} P_{S_j|AXY_1Y_2}(s_j | a, x, y_1, y_2)\, d_j(s_j, \tilde{s}). \end{aligned} \tag{12}$$

One can also bound $|\mathcal{V}|$ as

$$\min\{|\mathcal{X}| \cdot |\mathcal{A}|,\ |\mathcal{Y}_1| \cdot |\mathcal{S}_1|,\ |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\} + 1. \tag{13}$$

Proof Sketch: For the achievability proof, we leverage a block-Markov coding scheme with $B \geq 2$ blocks, each with

n channel uses, wherein block $b \in [2:B]$, where $[1:n] = \{1,2,\ldots,n\}$ a part of the common message is hidden with a key derived from block $b-1$. We next show reliability and security guarantees for a single block.

Fix P_{VAX} such that there exist per-letter estimators $\mathsf{Est}_j(a,x,y_1,y_2) = \hat{s}_j$ that satisfy $\mathbb{E}[d_j(S_j,\widehat{S}_j))] \leq D_j + \epsilon_n$ for $j=1,2$, where $\epsilon_n \geq 0$ and $\epsilon_n \to 0$ when $n \to \infty$. Let $(V^n, A^n, X^n, Y_1^n, S_1^n, Y_2^n, S_2^n)$ generated independent and identically distributed (i.i.d.) according to (10). To the sequence v^n, we uniformly and independently assign random bin indices $W_{\mathrm{v}_1} \in [1:2^{nR_{\mathrm{v}_1}}]$, $W_{\mathrm{v}_2} \in [1:2^{nR_{\mathrm{v}_2}}]$, $L_{\mathrm{v}} \in [1:2^{n\widetilde{R}_{\mathrm{v}}}]$, and $F_{\mathrm{v}} \in [1:2^{n\widetilde{R}_{\mathrm{v}}}]$. We also assign to y_1^n a random bin index $L_{\mathrm{y}_1} \in [1:2^{n\overline{R}_{\mathrm{y}_1}}]$, and we set $\overline{R}_{\mathrm{y}_1} = \overline{R}_{\mathrm{v}}$. We next choose $F = F_{\mathrm{v}}$ and $M = (M_1, M_2)$ with $M_1 = W_{\mathrm{v}_1}$ and $M_2 = (W_{\mathrm{v}_1}, L_{\mathrm{y}_1} \oplus L_{\mathrm{v}})$, where $\oplus$ is the one-time padding operation. Conceptually, M represents the message (M_1, M_2), whereas F represents the randomness that defines the codebook known to all parties.

The rate conditions on the random bin indices which guarantee reliability and secrecy are as follows.

Reliability: Using a Slepian-Wolf [24] decoder, V^n can be reliably recovered from (Y_1^n, S_1^n, F) if [13, Lemma 1]

$$\widetilde{R}_{\mathrm{v}} > H(V|Y_1,S_1). \tag{14}$$

Secrecy: Using privacy amplification [25, Theorem 1], W_{v_2} and F become almost independent of (Y_2^n, S_2^n) and uniformly distributed if

$$R_{\mathrm{v}_2} + \widetilde{R}_{\mathrm{v}} < H(V|Y_2,S_2). \tag{15}$$

Similarly, L_{y_1} becomes almost independent of (Y_2^n, S_2^n, V^n) and uniformly distributed if

$$\overline{R}_{\mathrm{y}_1} = \overline{R}_{\mathrm{v}} < H(Y_1|Y_2,S_2,V). \tag{16}$$

Then, it follows that $L_{\mathrm{y}_1} \oplus L_{\mathrm{v}}$ is also almost independent of (Y_2^n, S_2^n, V^n). Thus, M_2 is almost independent of the eavesdropper's observations, yielding the strong secrecy condition.

Note that all $(v^n, x^n, y_1^n, y_2^n, s_1^n, s_2^n)$ tuples are in the jointly typical set with high probability. Using the law of total expectation to bounded distortion metrics and the typical average lemma [26, pp. 26], proves that distortion constraints (4) are satisfied. The sufficiency of the deterministic estimators follows similarly to [2, Lemma 1].

By [25, Theorem 1], the distribution induced by the source coding scheme is arbitrarily close in variational distance to the distribution induced by channel coding scheme when

$$\widetilde{R}_{\mathrm{v}} + R_{\mathrm{v}_1} + R_{\mathrm{v}_2} + \overline{R}_{\mathrm{v}} < H(V). \tag{17}$$

Applying Fourier-Motzkin elimination [27] to (14)-(17) and setting $R_1 = R_{\mathrm{v}_1}$ and $R_2 = R_{\mathrm{v}_1} + \overline{R}_{\mathrm{v}}$, we recover (7) and

$$R_2 \leq \min\left\{R_{\mathrm{sec}}, I(V;Y_1,S_1) - R_1\right\} \tag{18}$$

where we have R_{sec} is equal to

$$\left[H(V|Y_2,S_2) - H(V|Y_1,S_1)\right]^+ + H(Y_1|Y_2,S_2,V) \tag{19}$$

with $[b]^+ = \max\{b,0\}$ for $b \in \mathbb{R}$.

The channel with no degradedness assumptions conforms to the Markov chain

$$V - (X,A) - (Y_1,S_1,Y_2,S_2). \tag{20}$$

Combining (5) and (20) provides the Markov chain

$$V - (X,A) - (Y_1,S_1) - (Y_2,S_2). \tag{21}$$

Applying (21) to (19) results in (8).

As the secret key cannot be used in the same block in which it is generated, we turn to the block-Markov coding scheme as described above, and use the secret L_{y_1} in block $b-1$ as a key to secure L_{v} in block b. In the block-Markov coding scheme, there is no secret message M_2 sent in the first block. A union bound on the probability of making a decoding error in each block shows that the reliability condition (2) is asymptotically satisfied. The proof that the secrecy constraint is unaffected across all blocks follows similarly to the proof of [7, Proposition 1].

For the converse proof, assume that for some $\delta_n > 0$, with $\delta_n \to 0$ as $n \to \infty$, there exist an action encoder, channel encoder, decoder, and estimators such that (1)-(4) are satisfied for (R_1, R_2, D_1, D_2). We define $V_i \triangleq (M, M_2, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1})$ such that $V_i - (A_i, X_i) - (Y_{1,i}, Y_{2,i}, S_{1,i}, S_{2,i})$ forms a Markov chain for all $i \in [1:n]$.

Bound on R_1: We have

$$\begin{aligned} nR_1 &\overset{(a)}{\leq} I(M_1; Y_1^n, S_1^n) + n\epsilon_n \qquad (22)\\ &\leq \sum_{i=1}^{n} \big[H\big(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}\big) \\ &\qquad - H\big(Y_{1,i}, S_{1,i}|M, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1}\big) + \epsilon_n\big] \\ &\overset{(b)}{=} \sum_{i=1}^{n} \big[I\big(V_i; Y_{1,i}, S_{1,i}\big) + \epsilon_n\big] \qquad (23) \end{aligned}$$

where (a) follows from Fano's inequality [28] with $\epsilon_n \to 0$ when $\delta_n \to$ and (b) follows from the definition of V_i.

Bound on $R_1 + R_2$: We have

$$n(R_1+R_2) \leq \sum_{i=1}^{n} \big[I\big(V_i; Y_{1,i}, S_{1,i}\big) + \epsilon_n\big] \tag{24}$$

which follows similarly to (23).

Bound on R_2: We obtain

$$\begin{aligned} nR_2 &\overset{(a)}{\leq} I(M_2; Y_1^n, S_1^n, Y_2^n, S_2^n) + n\epsilon_n \\ &= H(Y_1^n, S_1^n|Y_2^n, S_2^n) + I(M_2; Y_2^n, S_2^n) \\ &\qquad - H(Y_1^n, S_1^n|M_2, Y_2^n, S_2^n) + n\epsilon_n \\ &\overset{(b)}{\leq} H(Y_1^n, S_1^n|Y_2^n, S_2^n) + \delta_n \\ &\qquad - H(S_1^n|M, Y_1^n, Y_2^n, S_2^n) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) \\ &\qquad - H(S_{1,i}|M, Y_1^n, S_1^{i-1}, Y_2^n, S_2^n)\big] + n\epsilon_n + \delta_n \end{aligned}$$

$$\stackrel{(c)}{=} \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) - H(S_{1,i}|Y_{1,i}, Y_{2,i}, S_{2,i}, V_i) + \epsilon_n + \frac{1}{n}\delta_n\big] \quad (25)$$

where (a) follows similarly to (22), (b) follows by (3), and (c) is a consequence of the definition of V_i and the Markov chain

$$(Y_{1,i+1}^n, Y_{2,i+1}^n, S_{2,i+1}^n) - (M, Y_1^i, S_1^{i-1}, Y_2^i, S_2^i) - S_{1,i}.$$

The deterministic estimators, for j=1,2, follow from

$$D_j + \delta_n \geq \mathbb{E}\big[d_j(S_j^n, \widehat{S}_j^n)\big] = \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\big[d_j(S_{j,i}, \widehat{S}_{j,i})\big]. \quad (26)$$

Next, introduce a time-sharing random variable Q distributed uniformly on $[1:n]$ which is independent of all other random variables and defining $X = X_Q$, $A = A_Q$, $Y_1 = Y_{1,Q}$, $S_1 = S_{1,Q}$, $Y_1 = Y_{1,Q}$, $S_2 = S_{2,Q}$, and $V = (V_Q, Q)$ so that $V - (X, A) - (Y_1, S_1, Y_2, S_2)$ forms a Markov chain. Letting $\delta_n \to 0$ gives (7)-(9).

The proof of the cardinality bound for V follows from the support lemma [29, Lemma 15.4]. ∎

Remark 2: Note that the converse proof of Theorem 1 does not use the physical degradedness of the channel.

We next provide the secrecy-distortion region for reversely-physically-degraded ISAC channels. Proof of Theorem 2 is given in Appendix B, see below also for a proof sketch.

Theorem 2: (Reverse-physically-degraded): For a reverse-physically-degraded ISAC channel with strictly causal feedback available at the action and channel encoders, $\mathcal{R}_{\text{PS,Act}}$ is the union over all joint distributions P_{VAX} of the rate tuples (R_1, R_2, D_1, D_2) satisfying the rate constraint (7), the distortion constraints in (9), and

$$R_2 \leq \min\{H(Y_1|Y_2, S_2), (I(V; Y_1, S_1) - R_1)\} \quad (27)$$

where

$$P_{VAXY_1Y_2S_1S_2} = P_{V|AX} P_{AX} P_{S_2|A} P_{Y_2|S_2X} P_{Y_1S_1|S_2Y_2} \quad (28)$$

using the estimators in (12) with $|\mathcal{V}|$ bounded above by (13).

Proof Sketch: The proof of Theorem 2 follows similarly to that of Theorem 1, so we highlight the differences below.

Combining the definition of reverse-physical degradation in (6) with the channel Markov chain (20) gives the Markov chain

$$V - (X, A) - (Y_1, S_1) - (Y_2, S_2). \quad (29)$$

For the achievability proof, random binning applied to $(V^n, A^n, X^n, Y_1^n, S_1^n, Y_2^n, S_2^n)$ generated i.i.d. according to (28) in place of (10) yields the conditions (7), (9), and (13). The intermediate steps (18) and (19) also follow similarly, but the simplification differs because we use (29) in place of (21), resulting in (27).

For the converse proof, the bounds on R_1 and $(R_1 + R_2)$ and the distortion constraints follow as in the proof of Theorem 1. Noting Remark 2, we can directly apply the reverse degraded condition in (29) to (8), which simplifies to (27). ∎

For physically-degraded or reversely-physically-degraded secure ISAC channels with strictly causal feedback available at both the action and channel encoders, $\mathcal{R}_{\text{PS,Act}}$ stays the same as given in Theorem 1 and 2. This follows because the Markov chains used in the proofs of Theorems 1 and 2 continue to hold when we introduce dependence on the channel feedback for the actions. This parallels the results on channels with causal knowledge of action-dependent states in [10]. The corresponding model in [10] assumes that S_i is available at the transmitter, while we only assume that A_i, generated by the action encoder before channel use i, is available for use in computing the channel input.

IV. ISAC with Action-dependent States Under Full Secrecy

We next consider secure action-dependent ISAC with full secrecy, i.e., $M = M_2$, or $M_1 = \emptyset$, which is the case when the entire message should be kept secret from the eavesdropper.

Definition 3: A secrecy-distortion tuple (R, D_1, D_2) is *achievable* under full secrecy if, for any $\delta > 0$, there exist $n \geq 1$, one channel encoder, one action encoder, one decoder, and two estimators $\mathsf{Est}_j(X^n, A^n, Y_1^n, Y_2^n) = \widehat{S}_j^n$, $j \in \{1, 2\}$, such that

$$\frac{1}{n}\log|\mathcal{M}| \geq R - \delta \quad \text{(rates)} \quad (30)$$

$$\Pr\big[M \neq \widehat{M}\big] \leq \delta \quad \text{(reliability)} \quad (31)$$

$$I(M; Y_2^n, S_2^n) \leq \delta \quad \text{(strong secrecy)} \quad (32)$$

and the distortion constraints (4) are satisfied.

The secrecy-distortion region $\mathcal{R}_{\text{Act}}$ is the closure of the set of all achievable tuples under full secrecy and perfect output feedback. ◊

We next give the rate region under full secrecy for the physically-degraded channels. Proof of Theorem 3 is given in Appendix C, see below also for a proof sketch.

Theorem 3: (Physically-degraded) For a physically-degraded ISAC channel with strictly causal feedback available at the action and channel encoders, $\mathcal{R}_{Act}$ is the union over all joint distributions P_{AX} of the rate tuples (R, D_1, D_2) satisfying

$$R \leq \min\{H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X, A), I(X, A; Y_1, S_1)\} \quad (33)$$

and the distortion constraints in (9) using the estimators in (12), with distribution (5).

Proof Sketch: The achievability follows by removing V^n, fixing P_{AX}, generating a tuple of random variables i.i.d. according to (5), and performing the random binning on (a^n, x^n), removing W_{V_1}, replacing W_{V_2} with $W_{AX} \in \text{Unif}[1 : 2^{nR_{ax}}]$, and replacing L_V with $L_{AX} \in \text{Unif}[1 : 2^{n\overline{R}_{ax}}]$, and performing the rate simplifications as in the proof of Theorem 1.

We next outline the two bounds on R.

$$nR \stackrel{(a)}{\leq} \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}) - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, M, X_i, A_i)\big] + n\epsilon_n$$

$$\stackrel{(b)}{=} \sum_{i=1}^{n} I(X_i, A_i; Y_{1,i}, S_{1,i}) + n\epsilon_n \tag{34}$$

where (a) follows from Fano's inequality, where $\epsilon_n \to 0$ when $\delta_n \to 0$, and (b) is a result of the Markov chain

$$(Y_{1,i}, S_{1,i}) - (X_i, A_i) - (Y_1^{i-1}, S_1^{i-1}, M).$$

Similar to the bound on R_2 in (25), we have

$$\begin{aligned} nR &\stackrel{(a)}{\leq} \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) \\ &\quad - H(S_{1,i}|Y_{1,i}^n, Y_{2,i}^n, S_{2,i}^n, M, S_1^{i-1}, X_i, A_i)\big] + \delta_n + n\epsilon_n \\ &\stackrel{(b)}{=} \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) \\ &\quad - H(S_{1,i}|Y_{1,i}, Y_{2,i}, S_{2,i}, X_i, A_i)\big] + \delta_n + n\epsilon_n \end{aligned} \tag{35}$$

where (a) follows by Fano's inequality with $\epsilon_n \to 0$ when $\delta_n \to 0$, and the secrecy constraint (32) and (b) follows by application of the Markov chain

$$S_{1,i} - (Y_{1,i}, Y_{2,i}, S_{2,i}, X_i, A_i) - (Y_1^{n\setminus i}, Y_2^{n\setminus i}, S_2^{n\setminus i}, M, S_1^{i-1}).$$

Introducing a time-sharing random variable, applying the distortion bounds in (4), and letting $\delta_n \to 0$ give the result. ∎

We next provide the rate region under full secrecy for the reversely-physically-degraded channels. Proof of Theorem 4 is given in Appendix D, see below also for a proof sketch.

Theorem 4: (Reverse-physically-degraded) For a reverse-physically-degraded ISAC channel with delayed channel feedback available at the action and channel encoders, $\mathcal{R}_{Act}$ is the union over all joint distributions P_{AX} of the rate tuples (R, D_1, D_2) satisfying

$$R \leq \min\{H(Y_1|Y_2, S_2), I(X, A; Y_1, S_1)\} \tag{36}$$

and the distortion constraints in (9) using the estimators in (12), with distribution (6).

Proof Sketch: The achievability proof follows from the steps in the proof of Theorem 3 and performing the rate simplifications as in the proof of Theorem 2. The converse proof follows by simplifying the results of the converse results of Theorem 3 with the reverse-physical-degradation, as in the proof of the converse for Theorem 2. ∎

V. Binary Noiseless Secure ISAC Channels with Action-dependent States

Suppose a secure ISAC scenario with perfect output feedback, full secrecy, and action-dependent multiplicative Bernoulli states. The input, output, and action alphabets are binary. Specifically, we have

$$Y_1 = S_1 \cdot X, \qquad Y_2 = S_2 \cdot X, \tag{37}$$

and

$$\begin{aligned} &P_{S_1S_2|A}(0,0|0) = \lambda, \quad P_{S_1S_2|A}(1,0|0) = (1-\lambda)(1-\alpha), \\ &P_{S_1S_2|A}(0,1|0) = 0, \quad P_{S_1S_2|A}(1,1|0) = (1-\lambda), \alpha \\ &P_{S_1S_2|A}(0,0|1) = 1-\lambda, \quad P_{S_1S_2|A}(1,0|1) = \lambda(1-\alpha), \\ &P_{S_1S_2|A}(0,1|1) = 0, \quad P_{S_1S_2|A}(1,1|1) = \lambda\alpha, \end{aligned} \tag{38}$$

and

$$\begin{aligned} &P_{XA}(0,0) = (1-p)(1-q), \quad P_{XA}(1,0) = pq, \\ &P_{XA}(0,1) = (1-p)q, \quad P_{XA}(1,1) = p(1-q) \end{aligned} \tag{39}$$

with $P_{XAS_1S_2} = P_{XA}P_{S_1S_2|A}$ for fixed $\lambda, \alpha \in [0,1]$. This ISAC channel is stochastically-degraded, i.e., there exists a marginal probability distribution so that the ISAC channel can be represented as (5). The constraints (30)-(32), and (4) in Definition 3 only depend on the marginal distributions of (X, A, Y_1, S_1) and (X, A, Y_2, S_2) when per-letter estimators of the form $\mathsf{Est}_j(x, a, y_j)$ are used for $j = 1, 2$, so the secrecy-distortion region in Theorem 3 is also valid for stochastically-degraded secure ISAC channels.

Define $p * q = (1-p)q + p(1-q)$ and $H_b(x) = -x\log x - (1-x)\log(1-x)$. $X \sim \text{Bern}(p)$ represents a Bernoulli random variable X with probability p of success. Proof of Lemma 1 is given in Appendix E.

Lemma 1: The strong secrecy-distortion region R_{Act} for a binary ISAC channel with transmitter actions and multiplicative Bernoulli states, characterized by (38) for fixed $\lambda, \alpha \in [0,1]$ with Hamming distortion metrics is the union over all $p, q \in [0,1]$, where $X \sim \text{Bern}(p)$ and $A \sim \text{Bern}(p*q)$, of the rate tuples (R, D_1, D_2) satisfying

$$\begin{aligned} R \leq \min\Bigg\{ &\Bigg(\big(1-(1-p)q(1-\alpha\lambda)\big) H_b\Big(\frac{1-\lambda}{1-\alpha\lambda}\Big) \\ &\quad + (1-\alpha)(1-\lambda*p*q) H_b\Big(\frac{p(q*\lambda)}{1-\lambda*p*q}\Big) \\ &\quad - (1-p)(1-q)(1-\alpha+\alpha\lambda) H_b\Big(\frac{\lambda}{1-\alpha+\lambda\alpha}\Big)\Bigg), \\ &\Bigg((1-\lambda)(p*q)\log(1-\lambda) + \lambda(1-p*q)\log\lambda \\ &\quad - (1-\lambda)\big((1-p)(1-q)\log((1-p)(1-q)) - pq\log pq\big) \\ &\quad - \lambda\big((1-p)q\log((1-p)q) + p(1-q)log(p(1-q))\big) \\ &\quad - (\lambda*p*q)\log(\lambda*p*q) + H_b\Big(\frac{q\lambda}{1-q*\lambda}\Big)(1-p)(1-q*\lambda) \\ &\quad + H_b\Big(\frac{q(1-\lambda)}{q*\lambda}\Big) p(q*\lambda)\Bigg)\Bigg\} \end{aligned} \tag{40}$$

$$D_1 \geq (1-p)\min\{\lambda, 1-\lambda\}, \tag{41}$$

$$\begin{aligned} D_2 \geq (1-p)\big((1-q)\min\{1-\alpha+\alpha\lambda, \alpha-\alpha\lambda\} \\ + q\min\{1-\alpha\lambda, \alpha\lambda\}\big). \end{aligned} \tag{42}$$

Acknowledgment

This work was supported in part by the by the U.S. Department of Transportation under Grant 69A3552348327 for the CARMEN+ University Transportation Center, ZENITH Research and Leadership Career Development Fund, and the ELLIIT funding endowed by the Swedish government.

REFERENCES

[1] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30 845–30 857, Feb. 2021.

[2] M. Ahmadipour, M. Kobayashi, M. Wigger, and G. Caire, "An information-theoretic approach to joint sensing and communication," *IEEE Trans. Inf. Theory*, May 2022.

[3] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6g and beyond," *IEEE journal on selected areas in communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[4] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. 2005 Asilomar Conf. On Signals, Systems, and Computers*, 2005, pp. 1747–1751.

[5] O. Günlü, M. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication for binary input additive white Gaussian noise channels," in *IEEE Int. Symp. Joint Commun. Sensing*, Seefeld, Austria, Mar. 2023, pp. 1–6.

[6] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Toward multi-functional 6g wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.

[7] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure integrated sensing and communication," *IEEE Journal on Selected Areas in Information Theory*, 2023.

[8] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, "Robust transmit beamforming for secure integrated sensing and communication," *IEEE Transactions on Communications*, 2023.

[9] A. Bazzi and M. Chafii, "Secure full duplex integrated sensing and communications," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2082–2097, 2024.

[10] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5396–5411, 2010.

[11] J. D. D. Mutangana, R. Tandon, Z. Goldfeld, and S. Shamai, "Wiretap channel with latent variable secrecy," in *Proc. of IEEE Int. Symp. Inf. Theory*, Melbourne, Australia, July 2021, pp. 837–842.

[12] 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, July 1993.

[13] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[14] J. M. Renes and R. Renner, "Noisy channel coding via privacy amplification and information reconciliation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7377–7385, Nov. 2011.

[15] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," *Electron. Notes Discrete Math.*, vol. 21, pp. 155–159, Aug. 2005.

[16] A. Cohen and A. Cohen, "Wiretap channel with causal state information and secure rate-limited feedback," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1192–1203, Mar. 2016.

[17] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[18] B. Dai, A. J. H. Vinck, Y. Luo, and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," in *Proc. of IEEE Int. Symp. Inf. Theory*, Cambridge, MA, July 2012, pp. 244–248.

[19] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[20] G. Bassi, P. Piantanida, and S. Shamai, "The wiretap channel with generalized feedback: Secure communication and key generation," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2213–2233, Apr. 2019.

[21] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[22] M. Tahmasbi, M. R. Bloch, and A. Yener, "Learning an adversary's actions for secret communication," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1607–1624, Mar. 2020.

[23] H. Zhang, L. Yu, and B. Dai, "Feedback schemes for the action-dependent wiretap channel with noncausal state at the transmitter," *Entropy*, vol. 21, no. 3, p. 278, 2019.

[24] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[25] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[26] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge University Press, 2011.

[27] A. Schrijver, *Theory of Linear and Integer Programming*. Chichester, England: John Wiley & Sons, June 1998.

[28] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: John Wiley & Sons, 2012.

[29] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge University Press, 2011.

[30] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

APPENDIX A
PROOF OF THEOREM 1

Proof: **Achievability:** We use the Output Statistics of Random Binning (OSRB) method [25] to prove the achievability. We first define the operationally dual source coding problem to the problem of interest, the ISAC with transmitter actions channel coding problem. From there we define two protocols: Protocol A is coding scheme for the dual source coding problem and Protocol B is a randomized coding scheme for the original ISAC problem.

Fix $p_{VAX}(v,a,x)$ such that there exist per-letter estimators $\mathsf{Est}_j(a,x,y_1,y_2) = \hat{s}_j$ satisfying $\mathbb{E}[d_j(S_j,\widehat{S}_j))] \leq D_j + \epsilon_n$ for $j=1,2$, where $\epsilon_n \geq 0$ and $\epsilon_n \to 0$ when $n \to \infty$. We now formally define Protocols A and B.

Protocol A *(dual source coding problem)*: We generate the tuple of random variables $(V^n, A^n, X^n, Y_1^n, S_1^n, Y_2^n, S_2^n)$ i.i.d. according to (10).

Random Binning: The source encoder observing v^n, uniformly and independently assigns random bin indices $W_{\mathrm{v}_1} \in [1 : 2^{nR_{\mathrm{v}_1}}]$, $W_{\mathrm{v}_2} \in [1 : 2^{nR_{\mathrm{v}_2}}]$, $L_{\mathrm{v}} \in [1 : 2^{n\overline{R}_{\mathrm{v}}}]$, and $F_{\mathrm{v}} \in [1 : 2^{n\widetilde{R}_{\mathrm{v}}}]$. We also assign to y_1^n a random bin index $L_{\mathrm{y}_1} \in [1 : 2^{n\overline{R}_{\mathrm{y}_1}}]$ and we set $\overline{R}_{\mathrm{y}_1} = \overline{R}_{\mathrm{v}}$. The legitimate receiver uses a Slepian-Wolf [24] decoder $P^{SW}(\hat{v}^n|y_1^n, s_1^n, f_{\mathrm{v}})$ to recover the estimate $\hat{v}^n$ from $(y_1^n, s_1^n, f_{\mathrm{v}})$. Since transmitter in the original problem has perfect output feedback, we assume the source encoder has access to (y_1^n, y_2^n). Therefore, both the source encoder and the legitimate receiver can compute L_{y_1}. The eavesdropper observes $(y_2^n, s_2^n, f_{\mathrm{v}})$.

The random pmf, denoted P, induced by the random binning in Protocol A is

$$\begin{aligned}
&P(v^n, a^n, x^n, y_1^n, s_1^n, y_2^n, s_2^n, w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, l_{\mathrm{y}_1}, f_{\mathrm{v}}, \hat{v}^n) \\
&\quad = p(v^n, a^n, x^n, y_1^n, s_1^n, y_2^n, s_2^n) P(w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, f_{\mathrm{v}}|v^n) \\
&\qquad \times P(l_{\mathrm{y}_1}|y_1^n) P^{SW}(\hat{v}^n|y_1^n, s_1^n, f_{\mathrm{v}}) \\
&\quad = P(w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, f_{\mathrm{v}}, v^n) p(a^n, x^n|v^n) \\
&\qquad \times P(y_1^n, s_1^n, y_2^n, s_2^n, l_{\mathrm{y}_1}|a^n, x^n) P^{SW}(\hat{v}^n|y_1^n, s_1^n, f_{\mathrm{v}})
\end{aligned}$$

$$= P(w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, f_{\mathrm{v}}) P(v^n | w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, f_{\mathrm{v}}) p(a^n, x^n | v^n) \times p(y_1^n, s_1^n, y_2^n, s_2^n | a^n, x^n) P(l_{\mathrm{y}_1} | y_1^n) P^{SW}(\hat{v}^n | y_1^n, s_1^n, f_{\mathrm{v}}). \quad (43)$$

Protocol B *(channel coding problem assisted with shared randomness)*: Assume the existence and public dissemination of the shared randomness F_{v} to all parties, the transmitter, legitimate receiver, and the eavesdropper, where F_{v} distributed uniformly over $[1 : 2^{n\widetilde{R}_{\mathrm{v}}}]$. We also assume the existence of a secret key K, uniformly selected from $[1 : 2^{n\overline{R}_{\mathrm{v}}}]$, which is securely shared between the transmitter and legitimate receiver. We will later remove K using a block-Markov coding scheme, in which we will replace K with L_{y_1}. Conceptually, we define the message $M = (M_1, M_2)$ choosing the public message $M_1 = W_{\mathrm{v}_1}$, i.e. the message with no security requirement, and the private message $M_2 = (W_{\mathrm{v}_2}, L)$, i.e. the message that should be secured from the eavesdropper. Note that L is not a random bin index.

The coding scheme proceeds as follows: the transmitter selects two messages $m_1 \in \text{Unif}[1 : 2^{nR_{\mathrm{v}_1}}]$ and $m_2 \in \text{Unif}[1 : 2^{n(R_{\mathrm{v}_2}+\overline{R}_{\mathrm{v}})}]$ independent of each other and F_{v}. The messages can be represented as $m_1 = w_{\mathrm{v}_1}$ and $m_2 = (w_{\mathrm{v}_2}, l)$, where $l \in [1 : 2^{n\overline{R}_{\mathrm{v}}}]$. The transmitter obtains l_{v} by securing l via the one-time padding operation using K, i.e., $l_{\mathrm{v}} = l \oplus K$. The transmitter generates v^n according to $P(v^n | w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, F_{\mathrm{v}})$ as in (43). After n-channel uses, the transmitter, legitimate receiver, and eavesdropper observe $(v^n, a^n, x^n, y_1^n, y_2^n, f_{\mathrm{v}})$, $(y_1^n, s_1^n, f_{\mathrm{v}})$, and $(y_2^n, s_2^n, f_{\mathrm{v}})$, respectively. From here both the transmitter and legitimate receiver can generate l_{y_1} according to $P(l_{\mathrm{y}_1} | y_1^n)$ from (43). The legitimate receiver will use the same Slepian-Wolf decoder from Protocol A, $P^{SW}(\hat{v}^n | y_1^n, s_1^n, f_{\mathrm{v}})$, to find its estimate $\hat{v}^n$.

The distribution induced by Protocol B, denoted $\widehat{P}$, is

$$\widehat{P}(v^n, a^n, x^n, y_1^n, s_1^n, y_2^n, s_2^n, w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, l_{\mathrm{y}_1}, f_{\mathrm{v}}, \hat{v}^n) = \text{Unif}[1 : 2^{n\widetilde{R}_{\mathrm{v}}}] \cdot \text{Unif}[1 : 2^{nR_{\mathrm{v}_1}}] \cdot \text{Unif}[1 : 2^{n(R_{\mathrm{v}_2}+\overline{R}_{\mathrm{v}})}] \times P(v^n | w_{\mathrm{v}_1}, w_{\mathrm{v}_2}, l_{\mathrm{v}}, f_{\mathrm{v}}) p(a^n, x^n | v^n) \times p(y_1^n, s_1^n, y_2^n, s_2^n | a^n, x^n) P(l_{\mathrm{y}_1} | y_1^n) P^{SW}(\hat{v}^n | y_1^n, s_1^n, f_{\mathrm{v}}). \quad (44)$$

The distributions induced by Protocols A and B are approximately the same when the random binning indices $(W_{\mathrm{v}_1}, W_{\mathrm{v}_2}, L_{\mathrm{v}}, F_{\mathrm{v}})$ are almost mutually independent and uniformly distributed. More specifically, following [25, Theorem 1], as $n \to \infty$ the total variational distance between P and $\hat{P}$ goes to zero when

$$R_{\mathrm{v}_1} + R_{\mathrm{v}_2} + \overline{R}_{\mathrm{v}} + \widetilde{R}_{\mathrm{v}} < H(V). \quad (45)$$

Now we find the conditions that guarantee reliability and security for Protocol A.

Reliability: The rate condition that guarantees reliability is exactly that for which the Slepian-Wolf can successfully recover v^n from $(y_1^n, s_1^n, f_{\mathrm{v}})$. By [25, Lemma 1], imposing the constraint

$$\widetilde{R}_{\mathrm{v}} < H(V | Y_1, S_1) \quad (46)$$

implies that in the expectation over the random binning the total variational distance between $P^{SW}(\hat{v}^n | y_1^n, s_1^n, f_{\mathrm{v}})$ and $\mathbb{1}\{v^n = \hat{v}^n\}$ goes to zero as $n \to \infty$, giving reliability for Protocol A. Reliability for Protocol B follows from triangle inequality and a combination of the reliability for protocol A and the vanishing expected variational distance between (43) and (44).

Security: In order to show that Protocol B is secure, we find the rate conditions that show L_{y_1} and W_{v_2} are secure. To do this, we show that the random binning indices are independent of the eavesdroppers observations and uniformly distributed. We later show that L is secure through application of the secret key K.

Using [25, Theorem 1], L_{y_1} becomes almost independent of (V^n, Y_2^n, S_2^n) and uniformly distributed if

$$\overline{R}_{\mathrm{y}_1} = \overline{R}_{\mathrm{v}} < H(Y_1 | V, Y_2, S_2). \quad (47)$$

More specifically, (47) in the expectation over the random binning, the total variational distance between $P(L_{\mathrm{v}}, V^n, Y_2^n, S_2^n)$ and $\text{Unif}[1 : 2^{n\overline{R}_{\mathrm{y}_1}}] \cdot p(V^n, Y_2^n, S_2^n)$ goes to zero as $n \to \infty$.

A similar application of [25, Theorem 1] shows indices F_{v} and W_{v_2} become almost independent of (Y_2^n, S_2^n) and uniformly distributed if

$$\widetilde{R}_{\mathrm{v}} + R_{\mathrm{v}_2} < H(V | Y_2, S_2) \quad (48)$$

i.e., in the expectation over the random binning, the total variational distance between $P(F_{\mathrm{v}}, W_{\mathrm{v}_2}, Y_2^n, S_2^n)$ and $\text{Unif}[1 : 2^{n\widetilde{R}_{\mathrm{v}}}] \cdot \text{Unif}[1 : 2^{nR_{\mathrm{v}_2}}] \cdot p(Y_2^n, S_2^n)$ goes to zero as $n \to \infty$.

Using the properties of variational distance between distributions found in [25, Lemma 4], it follows that W_{v_2} and L_{y_1} are also secure in Protocol B. The uniformity and independence of K with all other random variables in addition to the uniformity of L means the one-time padding secures L from the eavesdropper, i.e. makes L independent of $(Y_2^n, S_2^n, F_{\mathrm{v}})$.

Performing Fourier-Motzkin elimination [27] on (45)-(48) to remove $\widetilde{R}_{\mathrm{v}}$ gives

$$R_{\mathrm{v}_1} < I(V; Y_1, S_1) - R_{\mathrm{v}_2} - \overline{R}_{\mathrm{v}}, \quad (49)$$

$$R_{\mathrm{v}_2} < \big[H(V | Y_2, S_2) - H(V | Y_1, S_1)\big]^+, \quad (50)$$

$$\overline{R}_{\mathrm{v}} < H(Y_1 | Y_2, S_2, V) \quad (51)$$

where $[b]^+ = \max\{0, b\}$, and (50) follows since all rates must be non-negative. For any $\epsilon > 0$ the rate

$$R_1 = R_{\mathrm{v}_1} = I(V; Y_1, S_1) - \epsilon \quad (52)$$

is achievable. For any R_1 less than or equal to (52), the rate

$$R_2 = R_{\mathrm{v}} + \overline{R}_{\mathrm{v}} = \min\big\{R_{\mathrm{sec}}, I(V; Y_1, S_1) - R_1\big\} - 2\epsilon,$$

where

$$R_{\mathrm{sec}} = \big[H(V | Y_2, S_2) - H(V | Y_1, S_1)\big]^+ + H(Y_1 | Y_2, S_2, V) \quad (53)$$

is achievable.

The channel with no degradedness assumptions conforms to the Markov chain in (20), which, when combined with (5) and (20) provides the Markov chain (21).

We can now perform the following simplifications

$$\begin{aligned}
R_{\text{sec}} &= \big[H(V|Y_2,S_2) - H(V|Y_1,S_1)\big]^+ + H(Y_1|Y_2,S_2,V) \\
&\overset{(a)}{=} H(V|Y_2,S_2) - H(V|Y_1,S_1) + H(Y_1|Y_2,S_2,V) \\
&\overset{(b)}{=} H(V,Y_1|Y_2,S_2) - H(V|Y_1,S_1,Y_2,S_2) \\
&= H(Y_1|Y_2,S_2) + I(V;S_1|Y_1,Y_2,S_2) \\
&= H(Y_1|Y_2,S_2) + H(S_1|Y_1,Y_2,S_2) - H(S_1|Y_1,Y_2,S_2,V) \\
&= H(Y_1,S_1|Y_2,S_2) - H(S_1|Y_1,Y_2,S_2,V) \qquad (54)
\end{aligned}$$

where (a) follows from the data processing inequality [28] and (21), and (b) follows from (21). Thus, we achieve (7) and (8).

The distortion constraints follow since all $(v^n, x^n, y_1^n, y_2^n, s_1^n, s_2^n)$ tuples are in the jointly typical set w. h. p. Using the law of total expectation to bounded distortion metrics and the typical average lemma [26, pp. 26], we see that the distortion constraints (4) are satisfied. The sufficiency of the deterministic estimators in (12) follows from [2, Lemma 1], where $(S^n, (X^n, Z^n), \hat{S}^n)$ is replaced with $(S_j^n, (X^n, A^n, Y_1^n, Y_2^n), \hat{S}_j^n)$ for $j = 1, 2$ and noting that $(X^{n\setminus i}, A^{n\setminus i}, Y_1^{n\setminus i}, Y_2^{n\setminus i}, \hat{S}_{j,i}) - (X_i, A_i, Y_{1,i}, Y_{2,i}) - S_{j,i}$ forms a Markov chain.

Now we need to derandomize Protocol B and remove the dependence on a secret key. The existence of a specific realization f of F such that the reliability and secrecy properties of B still holds follow from the standard method in [25].

Finally, we remove the secret key from Protocol B by chaining over multiple blocks as in [30] and [7]. We will use a block-Markov coding scheme consisting of $B \geq 2$ blocks, each with n channel uses. For the discussion of the block-Markov coding scheme alone, we will denote the random variables corresponding to the transmissions in block b with a superscript b and a sequence of random variables from blocks i to j, with $0 \leq i \leq j \leq B$, denoted with a superscript $i:j$, e.g., the random bin index for W_{v_1} block b is $W_{\text{v}_1}^b$. We let $M = M^{1:B} = (M_1^{1:B}, M_2^{1:B})$. Noting that in each block b, a secret key $L_{\text{y}_1}^b$ is generated known to the transmitter and legitimate receiver after the completion of block b. We set $M_2^1 = \emptyset$, i.e., no secure message is sent during the first block, and $L_{\text{y}_1}^{b-1}$ is used as K from Protocol B during block $b \geq 2$.

Since the distortion constraints are satisfied for a single block, they will be satisfied when aggregated across all blocks. The rate change for R_2 is negligible for B large, while R_1 remains the same. We finally need to show that the reliability and secrecy performance is unaffected by the block-Markov coding scheme. The asymptotic reliability performance follows from a union bound on

$$\lim_{n\to\infty} P\left[\left\{\widehat{M}_1^{1:B} \neq M_1^{1:B} \text{ or } \widehat{M}_2^{1:B} \neq M_2^{1:B}\right\}\right]. \qquad (55)$$

The single block security analysis shows that leakage between M_2 and the eavesdropper's observations within a single block is negligible, but, in order to show that the secrecy performance is unaffected by the block-Markov coding scheme we need to show that the leakage between the secure message, $M_2^{1:B} = (W_{\text{v}_2}^{1:B}, L^{1:B})$, and the eavesdropper's observations over all blocks, $(\mathbf{Y}_2^{1:B}, \mathbf{S}_2^{1:B})$, where the bold faced random variables are n-letter random variables, is negligible, i.e., $I(W_{\text{v}_2}^{1:B}, L^{1:B}; \mathbf{Y}_2^{1:B}, \mathbf{S}_2^{1:B})$ vanishes asymptotically. We make slight modifications to the approach in [7] to show that security holds across all blocks.

For convenience, we denote $W^b = W_{\text{v}_2}^b$, $K^b = L_{\text{y}_1}^b$, $L_{\text{v}}^b = L^b \oplus K^b$, and $\mathbf{Z}^b = (\mathbf{Y}_2^b, \mathbf{S}_2^b)$. We have

$$\begin{aligned}
&I(W^{1:B}, L^{1:B}; \mathbf{Z}^B) \\
&= \sum_{b=1}^{B-1} \big(I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I((W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b})\big) \\
&\qquad + I(W^{1:B}, L^{1:B}; \mathbf{Z}^1) \\
&\overset{(a)}{=} \sum_{b=1}^{B-1} \big(I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I((W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b})\big) \qquad (56)
\end{aligned}$$

where (a) follows since $\mathbf{Z}^1$ is independent of future messages $(W^{2:B}, L^{2:B})$ and no secure message is transmitted in the first block. Without loss of generality, we consider the term in the sum corresponding to block b, we see

$$\begin{aligned}
&I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b}) \\
&\quad = I(W^{1:B}, L^{1:B}; \mathbf{Z}^{b+1}|\mathbf{Z}^{1:b}) \\
&\quad = I(W^{1:b+1}, L^{1:b+1}; \mathbf{Z}^{b+1}|\mathbf{Z}^{1:b}) \\
&\qquad\quad + I(W^{b+2:B}, L^{b+2:B}; \mathbf{Z}^{b+1}|\mathbf{Z}^{1:b}, W^{1:b+1}, L^{1:b+1}) \\
&\quad \leq I(W^{1:b+1}, L^{1:b+1}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}) \\
&\qquad\quad + I(W^{b+2:B}, L^{b+2:B}; \mathbf{Z}^{1:b+1}, W^{1:b+1}, L^{1:b+1}) \\
&\quad \overset{(a)}{=} I(W^{1:b+1}, L^{1:b+1}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}) \\
&\quad = I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) \\
&\qquad\quad + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}|W^{b+1}, L^{b+1}) \\
&\quad \overset{(b)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) \\
&\qquad\quad + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}) \\
&\quad \overset{(c)}{\leq} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) \\
&\qquad\quad + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}, K^b) \\
&\quad = I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; K^b) \\
&\qquad\quad + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}|K^b) \\
&\quad \overset{(d)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; K^b) \\
&\quad \overset{(e)}{\leq} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}, K^{b-1}; K^b) \\
&\quad \overset{(f)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b) \qquad (57)
\end{aligned}$$

where (a) and (b) follow since future messages are independent of past messages and observations; (c) follows by adding a non-negative term in order to introduce K^b to break dependence across blocks; (d) follows since

$$(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}) - K^b - (\mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}) \qquad (58)$$

forms a Markov chain; (e) follows by adding K^{b-1} in again to break dependence across blocks, and (f) follows since we have the Markov chain

$$(W^{1:b-1}, L^{1:b-1}, \mathbf{Z}^{1:b-1}) - (W^b, L^b, \mathbf{Z}^b, K^{b-1}) - K_b. \quad (59)$$

Combining (57) with (56) gives

$$I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:B}) \leq \sum_{b=1}^{B-1} \Big(I\big(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}\big) + I\big(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b\big) \Big). \quad (60)$$

Now we show that the two quantities $I\big(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}\big)$ and $I\big(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b\big)$ asymptotically vanish across all blocks. The first term can be written as

$$\begin{aligned} &I\big(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}\big) \\ &\quad = I\big(W^{b+1}; \mathbf{Z}^{b+1}\big) + I\big(L^{b+1}; \mathbf{Z}^{b+1} | W^{b+1}\big) \\ &\quad \overset{(a)}{=} I\big(W^{b+1}; \mathbf{Z}^{b+1}\big) + I\big(L^{b+1}; \mathbf{Z}^{b+1}, W^{b+1}\big) \\ &\quad \overset{(b)}{=} I\big(W^{b+1}; \mathbf{Z}^{b+1}\big) + I\big(L^{b+1}; L_{\mathrm{v}}^b\big) \\ &\quad \overset{(c)}{=} I\big(W^{b+1}; \mathbf{Z}^{b+1}\big) + H\big(L_{\mathrm{v}}^b\big) - H\big(K^b\big) \\ &\quad \overset{(d)}{\leq} I\big(W^{b+1}; \mathbf{Z}^{b+1}\big) + n\overline{R}_{\mathrm{v}} - H\big(K^b\big) \end{aligned} \quad (61)$$

where (a) follows since W^{b+1} and L^{b+1} are independent, (b) follows by the data processing inequality and $L^{b+1} - L_{\mathrm{v}}^b - (\mathbf{Z}^{b+1}, W^{b+1})$, (c) follows since $H(L_{\mathrm{v}}^b | L^b) = H(K^b)$, and (d) follows from the rate condition on L_{v}^b. The condition (48) guarantees that $I(W^{b+1}; \mathbf{Z}^{b+1})$ vanishes across all blocks, while (47) makes K^b uniform, causing $n\overline{R}_{\mathrm{v}} - H\big(K^b\big)$ to vanish across all blocks. The independence of the secret key with other random variables $K^b = L_{\mathrm{y}_1}$ in a single block, see (47), implies that $I\big(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b\big)$ vanishes across all blocks as $n \to \infty$.

Converse: For the converse proof, assume that for some $\delta_n > 0$, with $\delta_n \to 0$ as $n \to \infty$, there exist an action encoder, channel encoder, decoder, and estimators such that (1)-(4) are satisfied for (R_1, R_2, D_1, D_2). We define

$$V_i \triangleq (M_1, M_2, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1}) \quad (62)$$

such that $V_i - (A_i, X_i) - (Y_{1,i}, Y_{2,i}, S_{1,i}, S_{2,i})$ forms a Markov chain for all $i \in [1:\ n]$.

Using Fano's inequality [28] we obtain

$$H(M; Y_1^n, S_1^n) \leq n\epsilon_n \quad (63)$$

where $n\epsilon_n = H_b(\delta_n) + \delta_n(R_1 + R_2)n$. Note that $\epsilon_n \to 0$ as $\delta_n \to 0$.

Bound on R_1: We have

$$\begin{aligned} nR_1 &\overset{(a)}{\leq} I(M_1; Y_1^n, S_1^n) + n\epsilon_n \\ &= \sum_{i=1}^n \big[H\big(Y_{1,i}, S_{1,i} | Y_1^{i-1}, S_1^{i-1}\big) \\ &\qquad - H\big(Y_{1,i}, S_{1,i} | M_1, Y_1^{i-1}, S_1^{i-1}\big) + \epsilon_n \big] \\ &\leq \sum_{i=1}^n \big[H\big(Y_{1,i}, S_{1,i}\big) \\ &\qquad - H\big(Y_{1,i}, S_{1,i} | M, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1}\big) + \epsilon_n \big] \\ &\overset{(b)}{=} \sum_{i=1}^n \big[I\big(V_i; Y_{1,i}, S_{1,i}\big) + \epsilon_n \big] \end{aligned} \quad (64)$$

where (a) follows from Fano's inequality (63) and (b) follows from the definition of V_i (62).

Bound on $R_1 + R_2$: Similar to the bound on R_1, we have

$$\begin{aligned} n(R_1 + R_2) &\overset{(a)}{\leq} I(M; Y_1^n, S_1^n) + n\epsilon_n \\ &= \sum_{i=1}^n \big[H\big(Y_{1,i}, S_{1,i} | Y_1^{i-1}, S_1^{i-1}\big) \\ &\qquad - H\big(Y_{1,i}, S_{1,i} | M, Y_1^{i-1}, S_1^{i-1}\big) + \epsilon_n \big] \\ &\leq \sum_{i=1}^n \big[H\big(Y_{1,i}, S_{1,i}\big) \\ &\qquad - H\big(Y_{1,i}, S_{1,i} | M, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1}\big) + \epsilon_n \big] \\ &\overset{(b)}{=} \sum_{i=1}^n \big[I\big(V_i; Y_{1,i}, S_{1,i}\big) + \epsilon_n \big] \end{aligned} \quad (65)$$

where (a) follows from Fano's inequality (63) and (b) follows from the definition of V_i (62).

Bound on R_2: We obtain

$$\begin{aligned} nR_2 &\overset{(a)}{\leq} I(M_2; Y_1^n, S_1^n, Y_2^n, S_2^n) + n\epsilon_n \\ &= H(Y_1^n, S_1^n | Y_2^n, S_2^n) + I(M_2; Y_2^n, S_2^n) \\ &\qquad - H(Y_1^n, S_1^n | M_2, Y_2^n, S_2^n) + n\epsilon_n \\ &\overset{(b)}{\leq} H(Y_1^n, S_1^n | Y_2^n, S_2^n) + \delta_n \\ &\qquad - H(S_1^n | M, Y_1^n, Y_2^n, S_2^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) \\ &\qquad - H(S_{1,i} | M, Y_1^n, S_1^{i-1}, Y_2^n, S_2^n) \big] + n\epsilon_n + \delta_n \\ &\overset{(c)}{=} \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) \\ &\qquad - H(S_{1,i} | M, Y_1^i, S_1^{i-1}, Y_2^i, S_2^i) \big] + n\epsilon_n + \delta_n \\ &\overset{(d)}{=} \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) \\ &\qquad - H(S_{1,i} | M, Y_{1,i}, Y_{2,i}, S_{2,i}, V_i) \big] + n\epsilon_n + \delta_n \end{aligned} \quad (66)$$

where (a) follows similarly to (22), (b) follows since the secrecy constraint (3) is satisfied, and (c) is a consequence of the Markov chain

$$(Y_{1,i+1}^n, Y_{2,i+1}^n, S_{2,i+1}^n) - (M, Y_1^i, S_1^{i-1}, Y_2^i, S_2^i) - S_{1,i}$$

and (d) follows from definition of V_i, see (62).

The deterministic estimators, for j=1,2, follow from

$$D_j + \delta_n \geq \mathbb{E}\big[d_j(S_j^n, \widehat{S_j^n})\big] = \frac{1}{n} \sum_{i=1}^n \mathbb{E}\big[d_j(S_{j,i}, \widehat{S}_{j,i})\big]. \quad (67)$$

Next, we introduce a time-sharing random variable Q distributed uniformly on $[1:n]$ which is independent of all other random variables. This allows us to represent the bounds on R_1 (64) and R_1+R_2 (65) as

$$\begin{aligned} R_1 &\le \sum_{i=1}^{n} \big[I\big(V_Q; Y_{1,Q}, S_{1,Q}|Q=i\big)+\epsilon_n\big] \\ &= I\big(V_Q; Y_{1,Q}, S_{1,Q}|Q\big)+\epsilon_n \\ &= I\big(V_Q, Q; Y_{1,Q}, S_{1,Q}\big) - I\big(Q; Y_{1,Q}, S_{1,Q}\big)+\epsilon_n \\ &\le I\big(V_Q, Q; Y_{1,Q}, S_{1,Q}\big)+\epsilon_n \end{aligned} \tag{68}$$

and

$$R_1+R_2 \le I\big(V_Q, Q; Y_{1,Q}, S_{1,Q}\big)+\epsilon_n \tag{69}$$

and the bound on R_2 given in (66) as

$$\begin{aligned} R_2 &\le \sum_{i=1}^{n} \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i}) \\ &\quad - H(S_{1,i}|M, Y_{1,i}, Y_{2,i}, S_{2,i}, V_i)\big]+n\epsilon_n+\delta_n \\ &= \sum_{i=1}^{n} \big[H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q}, Q=i) \\ &\quad - H(S_{1,Q}|M, Y_{1,Q}, Y_{2,Q}, S_{2,Q}, V_Q, Q=i)\big]+n\epsilon_n+\delta_n \\ &= H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q}, Q) \\ &\quad - H(S_{1,i}|M, Y_{1,Q}, Y_{2,Q}, S_{2,Q}, V_Q, Q)+n\epsilon_n+\delta_n \\ &\le H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q}) \\ &\quad - H(S_{1,i}|M, Y_{1,Q}, Y_{2,Q}, S_{2,Q}, V_Q, Q)+n\epsilon_n+\delta_n. \end{aligned} \tag{70}$$

Defining $X=X_Q$, $A=A_Q$, $Y_1=Y_{1,Q}$, $S_1=S_{1,Q}$, $Y_1=Y_{1,Q}$, $S_2=S_{2,Q}$, and $V=(V_Q,Q)$ so that $V-(X,A)-(Y_1,S_1,Y_2,S_2)$ forms a Markov chain and letting $\delta_n \to 0$ gives the conditions in the statement of the theorem, (7)-(9).

The proof of the cardinality bound for V follows from the support lemma [29, Lemma 15.4]. ∎

Appendix B
Proof of Theorem 2

Proof: The proof of Theorem 2 follows similarly to that of Theorem 1 in Appendix A, we highlight the modifications below.

Achievability: The creation of Protocols A and B follow as in Appendix A up to the recovery of the rate conditions (52) and (53). Combining the definition of reverse-physical degradation in (6) with the channel Markov chain (20) gives the Markov chain (29), which we can use to perform the following simplification on R_{sec} from (53)

$$\begin{aligned} R_{\text{sec}} &= \big[H(V|Y_2,S_2)-H(V|Y_1,S_1)\big]^+ + H(Y_1|Y_2,S_2,V) \\ &\overset{(a)}{=} H(Y_1|Y_2,S_2,V) \\ &\overset{(b)}{=} H(Y_1|Y_2,S_2) \end{aligned} \tag{71}$$

where (a) follows since an application of (29) and the data processing inequality implies that $H(V|Y_2,S_2) \le H(V|Y_1,S_1)$, and (b) follows from (29). We thus have the rate conditions of the theorem, (7), (9), and (27). The distortion constraints, viability of per-letter deterministic estimators, derandomization, and analysis of the block-Markov coding scheme follow from the same argument in Appendix A.

Converse: Noting that the converse proof in Appendix A does not use degradation, thus, the rate constraint on R_1 (7) and distortion constraints (9) holds here as well. We can simplify constraint on R_2', see (11), in (8) as

$$\begin{aligned} R_2' &\le H(Y_1,S_1|Y_2,S_2) - H(S_1|Y_1,Y_2,S_2,V) \\ &= H(Y_1,S_1|Y_2,S_2) - H(S_1,Y_1|Y_2,S_2,V) + H(Y_1|Y_2,S_2,V) \\ &\overset{(a)}{=} H(Y_1,S_1|Y_2,S_2) - H(S_1,Y_1|Y_2,S_2) + H(Y_1|Y_2,S_2) \\ &= H(Y_1|Y_2,S_2) \end{aligned} \tag{72}$$

where (a) follows from the reverse-physical degradation, see (29). This gives

$$R_2 \le \min\big\{H(Y_1|Y_2,S_2), I(V;Y_1,S_1)-R_1\big\} \tag{73}$$

giving the converse. ∎

Appendix C
Proof of Theorem 3

Proof: **Achievability:** The achievability loosely follows by removing V^n and using (X^n,A^n) in its place in the proof of Theorem 1.

We fix P_{AX} and generate a tuple of random variables i.i.d. according to (5). Protocols A and B are defined as in Appendix A with the following modifications. The random binning is performed on (a^n,x^n) instead of v^n, the random binning index W_{v_1} is removed, W_{v_2} is replaced with $W_{\text{ax}} \in \text{Unif}[1:2^{nR_{\text{ax}}}]$, F_{v} is replace with $F_{\text{ax}} \in \text{Unif}[1:2^{n\overline{R}_{\text{ax}}}]$, and L_{v} is replaced by $L_{\text{ax}} \in \text{Unif}[1:2^{n\overline{R}_{\text{ax}}}]$. We continue to use L and L_{y_1} defined therein. We define $M=(W_{\text{ax}},L)$, the entirety of which should be kept secret from the eavesdropper.

The distributions induced by Protocols A and B are approximately the same when

$$R_{\text{ax}}+\overline{R}_{\text{ax}}+\widetilde{R}_{\text{ax}} < H(A,X) \tag{74}$$

by [25, Theorem 1].

By [25, Lemma 1] we get reliability, i.e., the eavesdropper can recover (a^n,x^n) from $(f_{\text{ax}},y_1^n,s_1^n)$, when

$$\widetilde{R}_{\text{ax}} < H(A,X|Y_1,S_1). \tag{75}$$

Security follows when

$$\overline{R}_{\text{y}_1} = \overline{R}_{\text{ax}} < H(Y_1|A,X,Y_2,S_2) \tag{76}$$

since L_{y_1} becomes almost independent of (A^n,X^n,Y_2,S_2) by [25, Theorem 1]. Similarly, by [25, Theorem 1] F_{ax} and W_{ax} are uniformly distributed and independent of (Y_2^n,S_2^n) when

$$\widetilde{R}_{\text{ax}}+R_{\text{ax}} < H(A,X|Y_2,S_2). \tag{77}$$

Performing Fourier-Motzkin Elimination on (74) - (77), we have

$$R_{\text{ax}} + \overline{R}_{\text{ax}} < I(A, X; Y_1, S_1) \tag{78}$$

$$R_{\text{ax}} < \left[H(A, X|Y_2, S_2) - H(A, X|Y_1, S_1)\right]^+ \tag{79}$$

$$\overline{R}_{\text{ax}} < H(Y_1|Y_2, S_2, A, X). \tag{80}$$

Choosing $R = R_{\text{ax}} + \overline{R}_{\text{ax}}$, we have that for any $\epsilon > 0$

$$R = \min\big\{I(A, X; Y_1, S_1), \big[H(A, X|Y_2, S_2) - H(A, X|Y_1, S_1)\big]^+ + H(Y_1|Y_2, S_2, A, X)\big\} - \epsilon \tag{81}$$

is achievable. Using the physical-degradation, we can simplify the rate condition

$$\begin{aligned}
&\big[H(A, X|Y_2, S_2) - H(A, X|Y_1, S_1)\big]^+ + H(Y_1|Y_2, S_2, A, X)\\
&\overset{(a)}{=} H(A, X|Y_2, S_2) - H(A, X|Y_1, S_1) + H(Y_1|Y_2, S_2, A, X)\\
&\overset{(b)}{=} H(A, X, Y_1|Y_2, S_2) - H(A, X|Y_1, S_1, Y_2, S_2)\\
&= H(Y_1|Y_2, S_2) + I(A, X; S_1|Y_1, Y_2, S_2)\\
&= H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X, A)
\end{aligned} \tag{82}$$

where (a) and (b) follow since $(A, X) - (Y_1, S_1) - (Y_2, S_2)$ forms a Markov chain. The rate constraint in the theorem, (33) follows by combining (82) with (81).

The distortion constraints, optimality of per-letter deterministic estimators, derandomization of Protocol B, and the removal of the secret key and subsequent block-Markov coding scheme secrecy analysis follow from the same argument Appendix A.

Converse: We assume that for some $\delta_n > 0$, with $\delta_n \to 0$ as $n \to \infty$, there exists an action encoder, decoder, and estimators such that the rate, reliability, and secrecy conditions (30)-(32) and the distortion constraints (4) are satisfied for (R, D_1, D_2).

By Fano's inequality we obtain

$$H(M; Y_1^n, S_1^n) \le n\epsilon_n \tag{83}$$

where $n\epsilon_n = H_b(\delta_n) + \delta_n(R)n$, noting that $\epsilon_n \to 0$ as $\delta_n \to 0$.

We next outline the two bounds on R.

$$\begin{aligned}
nR &\overset{(a)}{\le} I(M; Y_1^n, S_1^n)\\
&= \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}) - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, M)\big] + n\epsilon_n\\
&\le \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i}) - H(Y_{1,i}, S_{1,i}|Y_1^{i-1}, S_1^{i-1}, M, X_i, A_i)\big] + n\epsilon_n\\
&\overset{(b)}{=} \sum_{i=1}^n I(X_i, A_i; Y_{1,i}, S_{1,i}) + n\epsilon_n
\end{aligned} \tag{84}$$

where (a) follows from Fano's inequality (83), and (b) is a result of the Markov chain

$$(Y_{1,i}, S_{1,i}) - (X_i, A_i) - (Y_1^{i-1}, S_1^{i-1}, M).$$

We can also bound R as

$$\begin{aligned}
nR &\overset{(a)}{\le} I(M; Y_1^n, S_1^n) + n\epsilon_n\\
&\le I(M; Y_1^n, S_1^n, Y_2^n, S_2^n) + n\epsilon_n\\
&= H(Y_1^n, S_1^n|Y_2^n, S_2^n) + H(Y_2^n, S_2^n) - H(Y_2^n, S_2^n|M)\\
&\quad - H(Y_1^n, S_1^n|M, Y_2^n, S_2^n) + n\epsilon_n\\
&= H(Y_1^n, S_1^n|Y_2^n, S_2^n) + I(M; Y_2^n, S_2^n)\\
&\quad - H(Y_1^n, S_1^n|M, Y_2^n, S_2^n) + n\epsilon_n\\
&\overset{(b)}{\le} H(Y_1^n, S_1^n|Y_2^n, S_2^n) + \delta_n\\
&\quad - H(S_1^n|M, Y_1^n, Y_2^n, S_2^n) + n\epsilon_n\\
&\le \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i})\\
&\quad - H(S_{1,i}|Y_{1,i}^n, Y_{2,i}^n, S_{2,i}^n, M, S_1^{i-1}, X_i, A_i)\big] + \delta_n + n\epsilon_n\\
&\overset{(c)}{=} \sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i})\\
&\quad - H(S_{1,i}|Y_{1,i}, Y_{2,i}, S_{2,i}, X_i, A_i)\big] + \delta_n + n\epsilon_n
\end{aligned} \tag{85}$$

where (a) follows by Fano's inequality (83), b follows from the secrecy constraint (32) and (c) follows by application of the Markov chain

$$S_{1,i} - (Y_{1,i}, Y_{2,i}, S_{2,i}, X_i, A_i) - (Y_1^{n\setminus i}, Y_2^{n\setminus i}, S_2^{n\setminus i}, M, S_1^{i-1}).$$

Next, we introduce a time-sharing random variable Q distributed uniformly on $[1:n]$ which is independent of all other random variables. This allows us to represent the bounds on R as follows

$$\begin{aligned}
R &\le \frac{1}{n}\sum_{i=1}^n I(X_i, A_i; Y_{1,i}, S_{1,i}) + \epsilon_n\\
&= \frac{1}{n}\sum_{i=1}^n I(X_Q, A_Q; Y_{1,Q}, S_{1,Q}|Q = i) + \epsilon_n\\
&= I(X_Q, A_Q; Y_{1,Q}, S_{1,Q}|Q) + \epsilon_n
\end{aligned} \tag{86}$$

and

$$\begin{aligned}
R &\le \frac{1}{n}\sum_{i=1}^n \big[H(Y_{1,i}, S_{1,i}|Y_{2,i}, S_{2,i})\\
&\quad - H(S_{1,i}|Y_{1,i}, Y_{2,i}, S_{2,i}, X_i, A_i)\big] + \frac{1}{n}\delta_n + \epsilon_n\\
&= \frac{1}{n}\sum_{i=1}^n \big[H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q}, Q = i)\\
&\quad - H(S_{1,Q}|Y_{1,Q}, Y_{2,Q}, S_{2,Q}, X_Q, A_Q, Q = i)\big] + \frac{1}{n}\delta_n + \epsilon_n\\
&= H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q}, Q)\\
&\quad - H(S_{1,Q}|Y_{1,Q}, Y_{2,Q}, S_{2,Q}, X_Q, A_Q, Q) + \frac{1}{n}\delta_n + \epsilon_n\\
&\overset{(a)}{\le} H(Y_{1,Q}, S_{1,Q}|Y_{2,Q}, S_{2,Q})\\
&\quad - H(S_{1,Q}|Y_{1,Q}, Y_{2,Q}, S_{2,Q}, X_Q, A_Q) + \frac{1}{n}\delta_n + \epsilon_n
\end{aligned} \tag{87}$$

where (a) follows from $Q - (A_Q, X_Q) - (Y_{1,Q}, S_{1,Q}, Y_{2,Q}, S_{2,Q})$. Defining $X = X_Q$, $A = A_Q$,

$Y_1 = Y_{1,Q}$, $S_1 = S_{1,Q}$, $Y_1 = Y_{1,Q}$, $S_2 = S_{2,Q}$, and $V = (V_Q, Q)$ so that $V - (X, A) - (Y_1, S_1, Y_2, S_2)$ forms a Markov chain and letting $\delta_n \to 0$ gives

$$R \leq \min\big\{I(X, A; Y_1, S_1|Q), \\ H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X, A)\big\}. \quad (88)$$

Since we only need to preserve $I(X, A; Y_1, S_1|Q)$, we can bound $|\mathcal{Q}|$ by 1 by the support lemma [29, Lemma 15.4], resulting in the rate given in the theorem, (33).

The distortion constraints follow as in Appendix A. ∎

Appendix D
Proof of Theorem 4

Proof: **Achievability:** The construction and analysis of Protocols A and B follow as in Appendix C reach the constraint (81) with out the use of degradation, i.e.,

$$R = \min\big\{I(A, X; Y_1, S_1), \big[H(A, X|Y_2, S_2) \\ - H(A, X|Y_1, S_1)\big]^+ + H(Y_1|Y_2, S_2, A, X)\big\} - \epsilon \quad (89)$$

is achievable. Using reverse-physical-degradation, see (29), we can simplify the rate condition

$$\begin{aligned}&\big[H(A, X|Y_2, S_2) - H(A, X|Y_1, S_1)\big]^+ + H(Y_1|Y_2, S_2, A, X) \\ &\overset{(a)}{=} H(Y_1|Y_2, S_2, A, X) \\ &\overset{(b)}{=} H(Y_1|Y_2, S_2) \end{aligned} \quad (90)$$

where (a) and (b) follow since $(A, X) - (Y_2, S_2) - (Y_1, S_1)$ forms a Markov chain. The rate constraint in the theorem, (36) follows by combining (90) with (89).

The distortion constraints and block-Markov coding scheme analysis follow as in Appendix C.

Converse: The converse of Theorem 3 does not use degradation. We apply the reverse-physical-degradation to (33) by performing the following simplification

$$\begin{aligned}&H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X, A) \\ &\overset{(a)}{=} H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2) \\ &= H(Y_1|Y_2, S_2) \end{aligned} \quad (91)$$

where (a) follows since $(A, X) - (Y_2, S_2) - (Y_1, S_1)$. Combining (33) with (91) gives the rate condition in the theorem statement, (36).

∎

Appendix E
Proof of Lemma 1

Proof: The lemma follows from evaluating the strong-secrecy distortion region R_{Act} defined in Theorem 3. We have

$$\begin{aligned}&H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X, A) \\ &= H(S_1|Y_2, S_2) + H(Y_1|S_1, Y_2, S_2) - H(S_1|Y_1, S_2, X, A) \end{aligned} \quad (92)$$

which we evaluate term by term.

For the first term we have

$$\begin{aligned}H(S_1|Y_2, S_2) &\overset{(a)}{=} H(S_1|Y_2, S_2 = 0)p_{S_2}(0) \\ &= H(S_1|Y_2 = 1, S_2 = 0)p_{Y_2S_2}(1, 0) \\ &\quad + H(S_1|Y_2 = 0, S_2 = 0)p_{Y_2S_2}(0, 0) \\ &\overset{(b)}{=} H(S_1|Y_2 = 0, S_2 = 0) \\ &\overset{(c)}{=} H(S_1|S_2 = 0) \\ &= H_b(p_{S_1|S_2}(0, 0)) \\ &= H_b\left(\frac{1-\lambda}{1-\alpha\lambda}\right) \end{aligned} \quad (93)$$

where (a) follows since $H(S_1|Y_2, S_2 = 1) = 0$ because $S_1 = 1$ if $S_2 = 1$, (b) follows since $p_{Y_2S_2}(1, 0) = 0$ and $p_{Y_2S_2}(0, 0) = 1$, and (c) follows since $Y_2 = 0$ if $S_2 = 0$.

Evaluating the second term gives us

$$\begin{aligned}&H(Y_1|S_1, Y_2, S_2) \\ &\overset{(a)}{=} H(Y_1|S_1 = 1, Y_2, S_2)p_{S_1}(1) \\ &\overset{(b)}{=} H(Y_1|S_1 = 1, Y_2, S_2 = 0)p_{S_1S_2}(1, 0) \\ &= H(Y_1|S_1 = 1, Y_2 = 0, S_2 = 0)p_{S_1Y_2S_2}(1, 0, 0) \\ &\quad + H(Y_1|S_1 = 1, Y_2 = 1, S_2 = 0)p_{S_1Y_2S_2}(1, 1, 0) \\ &\overset{(c)}{=} H(Y_1|S_1 = 1, S_2 = 0)p_{S_1S_2}(1, 0) \\ &\overset{(d)}{=} H(X|S_1 = 1)p_{S_1S_2}(1, 0) \\ &= H_b(p_{X|S_1}(1|1))p_{S_1S_2}(1, 0) \\ &= H_b\left(\frac{p(1 - q * \lambda)}{1 - \lambda * p * q}\right)(1 - \alpha)(1 - \lambda * p * q) \end{aligned} \quad (94)$$

where (a) follows since $H(Y_1|S_1 = 0, Y_2, S_2) = 0$ because $Y_1 = 0$ when $S_1 = 0$, (b) follows since $H(Y_1|S_1 = 1, Y_2, S_2 = 1) = 0$ because $Y_1 = Y_2$ if $S_1 = S_2 = 1$, (c) follows since Y_2 must be 0 if $S_2 = 0$, and (d) follows since $(X, A) - S_1 - S_2$ forms a Markov chain and $Y_1 = S_1 \cdot X = X$.

The third term is

$$\begin{aligned}&H(S_1|Y_1, Y_2, S_2, X, A) \\ &\overset{(a)}{=} H(S_1|Y_1, Y_2, S_2 = 0, X, A)p_{S_2}(0) \\ &\overset{(b)}{=} H(S_1|Y_1 = 0, Y_2, S_2 = 0, X, A)p_{Y_1S_2}(0, 0) \\ &\overset{(c)}{=} H(S_1|Y_1 = 0, Y_2 = 0, S_2 = 0, X, A)p_{Y_1Y_2S_2}(0, 0, 0) \\ &\overset{(d)}{=} H(S_1|Y_1{=}0, Y_2{=}0, S_2{=}0, X{=}0, A)p_{XY_1Y_2S_2}(0, 0, 0, 0) \\ &\overset{(e)}{=} H(S_1|X{=}0, A, S_2{=}0)p_{XS_2}(0, 0) \\ &= H(S_1|X = 0, A = 0, S_2 = 0)p_{XAS_2}(0, 0, 0) \\ &\quad + H(S_1|X = 0, A = 1, S_2 = 0)p_{XAS_2}(0, 1, 0) \\ &= H_b(p_{S_1|XAS_2}(0|0, 0, 0))p_{XAS_2}(0, 0, 0) \\ &\quad + H_b(p_{S_1|XAS_2}(0|0, 1, 0))p_{XAS_2}(0, 1, 0) \\ &= H_b\left(\frac{\lambda}{1 - \alpha + \lambda\alpha}\right)(1 - p)(1 - q)(1 - \alpha + \alpha\lambda) \\ &\quad + H_b\left(\frac{1-\lambda}{1-\lambda\alpha}\right)(1 - p)q(1 - \lambda\alpha) \end{aligned} \quad (95)$$

where (a) follows since $H(S_1|Y_1, Y_2, S_2 = 1, X, A) = 0$ because $S_1 = 1$ if $S_2 = 1$, (b) follows since we have

$$H(S_1|Y_1 = 1, Y_2, S_2 = 0, X, A) = 0 \tag{96}$$

because $S_1 = 1$ if $Y_1 = 1$, (c) follows since $p_{Y_1Y_2S_2}(0, 1, 0) = 0$ because Y_2 cannot be 1 if $S_2 = 0$, (d) follows since $H(S_1|Y_1 = 0, Y_2 = 0, S_2 = 0, X = 1, A) = 0$ because $S_1 = 0$ if $Y_1 = 0$ and $X = 1$, and (e) follows since Y_1 and Y_2 must be zero if $X = 0$.

Combining (93)-(95) gives the first term in the minimization in (40).

We now calculate the second term in (40), $I(X, A; Y_1, S_1) = H(X, A) - H(X, A|Y_1, S_1)$ in two parts. The first part is given by

$$\begin{aligned} &H(X, A) \\ &= -(1-p)(1-q)\log\big((1-p)(1-q)\big) - pq\log\big(pq\big) \\ &\quad - p(1-q)\log\big(p(1-q)\big) - (1-p)q\log\big((1-p)q\big). \end{aligned} \tag{97}$$

The second part is

$$\begin{aligned} &H(X, A|Y_1, S_1) \\ &\overset{(a)}{=} H(X, A|Y_1, S_1 = 0)p_{S_1}(0) + H(A|X, S_1 = 1)p_{S_1}(1) \\ &\overset{(b)}{=} H(X, A|S_1 = 0)p_{S_1}(0) + H(A|X, S_1 = 1)p_{S_1}(1) \\ &= H(X, A|S_1 = 0)p_{S_1}(0) + H(A|X = 0, S_1 = 1)p_{XS_1}(0, 1) \\ &\quad + H(A|X = 1, S_1 = 1)p_{XS_1}(1, 1) \\ &= H(X, A|S_1 = 0)p_{S_1}(0) + H_b\big(p_{A|XS_1}(1|0,1)\big)p_{XS_1}(0,1) \\ &\quad + H_b\big(p_{A|XS_1}(0|1,1)\big)p_{XS_1}(1,1) \\ &= -(1-p)(1-q)\lambda\log\frac{(1-p)(1-q)\lambda}{\lambda * p * q} \\ &\quad - (1-p)q(1-\lambda)\log\frac{(1-p)q(1-\lambda)}{\lambda * p * q} \\ &\quad - pq\lambda\log\frac{pq\lambda}{\lambda * p * q} - p(1-q)(1-\lambda)\log\frac{p(1-q)(1-\lambda)}{\lambda * p * q} \\ &\quad + H_b\left(\frac{q\lambda}{1-q*\lambda}\right)(1-p)(1-q*\lambda) + H_b\left(\frac{q(1-\lambda)}{q*\lambda}\right)p(q*\lambda) \end{aligned} \tag{98}$$

where (a) follows since $Y_1 = X$ when $S_1 = 1$, and $H(X, A|X, S_1 = 1) = H(A|X, S_1 = 1)$ and (b) follows since $Y_1 = X \cdot S_1 = X \cdot 0 = 0$ is deterministic and thus is independent of (X, A). Combining (97) and (98) gives the second term in the minimization in (40).

Now we calculate the distortion constraints. We will use estimators of the form $\mathsf{Est}_j(x, a, y_j)$. Consider the case where $X = 1$. Then we have $Y_1 = S_1 \cdot X = S_1$. The estimate $\mathsf{Est}_1(1, a, y_1) = y_1$ will always be correct. Consider $Y_2 = S_2 \cdot Y_1 = S_2 \cdot S_1 \cdot X = S_2 \cdot S_1$, then choosing $\mathsf{Est}_2(1, a, y_2) = y_2$ is also error free because S_2 cannot be 1 if $S_1 = 0$.

Now we consider the case where $X = 0$. When estimating Y_1, we get $\mathsf{Est}_1(0, 0, y_1) = \mathbb{1}\{\lambda < 0.5\}$ and $\mathsf{Est}_1(0, 1, y_1) = \mathbb{1}\{\lambda \geq 0.5\}$, equivalent to $\mathsf{Est}_1(0, a, y_1) = a - \mathbb{1}\{\lambda < 0.5\}$. When estimating Y_2, the optimal estimator is equal to $\mathsf{Est}_2(0, 0, y_2) = \mathbb{1}\{\alpha - \alpha\lambda > 0.5\}$ and $\mathsf{Est}_1(0, 1, y_1) = \mathbb{1}\{\alpha\lambda > 0.5\}$. Combining these gives

$$\mathsf{Est}_1(x, a, y_1) = \begin{cases} y_1 & \text{if } x = 0 \\ a - \mathbb{1}\{\lambda < .5\} & \text{if } x = 1 \end{cases} \tag{99}$$

and

$$\mathsf{Est}_1(x, a, y_1) = \begin{cases} y_1 & \text{if } x = 0 \\ \mathbb{1}\{\alpha - \alpha\lambda > .5\} & \text{if } x = 1, a = 0 \\ \mathbb{1}\{\alpha\lambda > .5\} & \text{if } x = 1, a = 1. \end{cases} \tag{100}$$

Using the Hamming distortion metric, the expected distortion for S_1 is (41) and the expected distortion for S_2 is equal to (42).

■