

# Secure Integrated Sensing and Communication

Onur Günlü, *Member, IEEE*, Matthieu R. Bloch, *Senior Member, IEEE*,

Rafael F. Schaefer, *Senior Member, IEEE*, and Aylin Yener, *Fellow, IEEE*

## Abstract

This work considers the problem of mitigating information leakage between communication and sensing in systems jointly performing both operations. Specifically, a discrete memoryless state-dependent broadcast channel model is studied in which (i) the presence of feedback enables a transmitter to convey information, while simultaneously performing channel state estimation; (ii) one of the receivers is treated as an eavesdropper whose state should be estimated but which should remain oblivious to part of the transmitted information. The model abstracts the challenges behind security for joint communication and sensing if one views the channel state as a sensitive attribute, e.g., location. For independent and identically distributed states, perfect output feedback, and when part of the transmitted message should be kept secret, a partial characterization of the secrecy-distortion region is developed. The characterization is exact when the broadcast channel is either physically-degraded or reversely-physically-degraded. The partial characterization is also extended to the situation in which the entire transmitted message should

This work has been supported by the German Federal Ministry of Education and Research (BMBF) under the Grant 16KIS1242, German Research Foundation (DFG) under the Grant SCHA 1944/9-1, and National Science Foundation (NSF) under the grants CCF 1955401 and 2148400. Parts of the previous versions of these results were presented at the 2022 IEEE International Symposium on Information Theory in Espoo, Finland in [1].

O. Günlü and R. F. Schaefer are with the Chair of Communications Engineering and Security, University of Siegen, 57076 Siegen, Germany (E-mail: {onur.guenlue, rafael.schaefer}@uni-siegen.de).

M. Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 (E-mail: matthieu.bloch@ece.gatech.edu).

A. Yener is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 (E-mail: yener@ece.osu.edu).

be kept secret. The benefits of a joint approach compared to separation-based secure communication and state-sensing methods are illustrated with binary joint communication and sensing models.

### **Index Terms**

Secure joint communication and sensing, secure integrated sensing and communication, physical layer security, future communication networks.

## **I. INTRODUCTION**

The vision for next generation mobile communication networks includes a seamless integration of the physical and digital world. Key to its success is the network's ability to automatically react to changing environments thanks to tight integration of communication and sensing [2]. For instance, a millimeter wave (mmWave) joint communication and radar system can be used to detect a target or to estimate crucial parameters relevant to communication and adapt the communication scheme accordingly [3]. Integrated sensing and communication (ISAC), also known as joint communication and sensing, techniques are envisioned more broadly as key enablers for a wide range of applications, including connected vehicles and drones [4].

Several information-theoretic studies of ISAC have been initiated, drawing on existing results for joint communication and state estimation [5]–[7]. Motivated by the integration of communication and radar for mmWave vehicular applications, [8] considers a model in which messages are encoded and sent through a state-dependent channel with generalized feedback both to reliably communicate with a receiver and to estimate the channel state by using the feedback and transmitted codewords. The optimal trade-off between the communication rate and channel-state estimation distortion is then characterized for memoryless ISAC channels and independent and identically distributed (i.i.d.) channel states that are causally available at the receiver and estimated at the transmitter by using a strictly causal channel output. Follow up works have extended the model to multiple access channels [9] and broadcast channels [8].

The nature of ISAC mandates the use of a single modality for the communication and sensing

functions so that sensing signals carry information, which then creates situations in which leakage of information may occur. For example, a target illuminated for ranging has the ability to gather potentially sensitive information about the transmitted message [10]. As both sensing and secrecy performance are measured with respect to the signal received at the sensed target, there exists a trade-off between the two [3], [11]. To capture and characterize this trade-off, we extend the ISAC model in [8] by introducing an eavesdropper in the network. The objective of the transmitter is then to simultaneously communicate reliably with the legitimate receiver, estimate the channel state, and hide a part of the message from the eavesdropper. The channel state is modeled as a two-component state capturing the characteristics of each individual receiver, the feedback is modeled as perfect output feedback for simplicity, and the transmitted message is divided into two parts, only one of which should be kept secret (a setup called partial secrecy in [12]). The proposed secure ISAC model can be viewed as extensions of the wiretap channel with feedback models [13]–[21].

#### A. *Summary of Contributions*

Our problem formulation introduces a strong secrecy constraint by considering an eavesdropper whose channel parameters are estimated at the transmitter, but that should be kept ignorant of part of the transmitted message. Even if the state sequence on which the ISAC channel depends is i.i.d., strictly causal channel output feedback improves the secrecy performance. A summary of the main contributions is as follows:

- We develop inner and outer bounds on the secrecy-distortion region of the secure ISAC model under partial secrecy when i.i.d. channel states are causally available at the corresponding receivers. Our achievability proof leverages the output statistics of random binning (OSRB) method [22]–[24]. Our outer bound also holds in the presence of noisy generalized output feedback.
- We simplify the inner and outer bounds on the secrecy-distortion region when the ISAC channel is physically-degraded or reversely-physically-degraded such that the inner and

outer bounds match.

- We develop inner and outer bounds on the secrecy-distortion region under full secrecy, when the entire transmitted message should be kept secret from the eavesdropper. We characterize the exact secrecy-distortion region under full secrecy when the ISAC channel is physically-degraded or reversely-physically-degraded.
- We study a binary noiseless ISAC channel example with multiplicative Bernoulli states to illustrate how secure ISAC methods may outperform separation-based secure communication and state-sensing methods. We also consider noisy more-capable ISAC channels to illustrate the effects of noise on an achievable strong secrecy-distortion region.

### *B. Organization*

In Section II, we introduce the model for secure ISAC under partial secrecy. In Section III, we provide inner and outer bounds on the secrecy-distortion region, specializing them for physically-degraded and reversely-physically-degraded ISAC channels and showing that the bounds match for such channels. In Section IV, we specialize the inner and outer bounds to the full secrecy case. In Section V, we illustrate the benefits of integrating security by design into ISAC by evaluating the rate region for a degraded and noiseless ISAC channel with multiplicative Bernoulli states. We also evaluate an achievable region for a noisy ISAC channel with a state-dependent input transmitted through a binary erasure channel (BEC) for the main channel and a binary symmetric channel (BSC) for the eavesdropper's channel, respectively, by establishing the parameter range for which the ISAC channel is more-capable.

### *C. Notation*

Upper case letters represent random variables and corresponding lower case letters their realizations. A random variable  $X$  has probability distribution  $P_X$ . Calligraphic letters  $\mathcal{X}$  denote sets with sizes  $|\mathcal{X}|$ . A subscript  $i$  denotes the position of a variable in a sequence of variables represented by a superscript, e.g.,  $X^n = X_1, X_2, \dots, X_i, \dots, X_n$ .  $X^{n \setminus i}$  denotes the sequence

$X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n$  and  $X_i^k$  denotes  $X_i, X_{i+1}, \dots, X_k$  for integers  $i \leq k \leq n$ .  $[1 : J]$  denotes the set  $\{1, 2, \dots, J\}$  for an integer  $J \geq 1$ , and  $X \sim \text{Unif}[1 : J]$  represents a uniform distribution over the set  $[1 : J]$ .  $H_b(x) = -x \log x - (1 - x) \log(1 - x)$  with natural logarithms is the binary entropy function.  $X \sim \text{Bern}(p)$  represents a Bernoulli random variable  $X$  with probability  $p$  of success.  $\text{BSC}(\beta)$  denotes a BSC with crossover probability  $\beta$  and  $\text{BEC}(\gamma)$  a BEC with erasure probability  $\gamma$  and erasure symbol  $e$ . The  $*$  operator denotes the operation  $p * \beta = p(1 - \beta) + (1 - p)\beta$ ,  $\oplus$  is the modulo-2 sum, and we define  $[a]^+ = \max\{a, 0\}$  for  $a \in \mathbb{R}$ .

## II. PROBLEM DEFINITION

We consider the secure ISAC model shown in Fig. 1, which includes a transmitter equipped with a state estimator, a legitimate receiver, and an eavesdropper (Eve). The transmitter attempts to reliably transmit a uniformly distributed message  $M = (M_1, M_2) \in \mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$  through a memoryless state-dependent ISAC channel with known statistics  $P_{Y_1 Y_2 Z | S_1 S_2 X}$  and i.i.d. state sequence  $(S_1^n, S_2^n) \in \mathcal{S}_1^n \times \mathcal{S}_2^n$  generated according to a known joint probability distribution  $P_{S_1 S_2}$ . The transmitter calculates the channel inputs  $X^n$  as  $X_i = \text{Enc}_i(M, Z^{i-1}) \in \mathcal{X}$  for all  $i = [1 : n]$ , where  $\text{Enc}_i(\cdot)$  is an encoding function and  $Z^{i-1} \in \mathcal{Z}^{i-1}$  is the delayed channel output feedback. The legitimate receiver that observes  $Y_{1,i} \in \mathcal{Y}_1$  and  $S_{1,i} \in \mathcal{S}_1$  for all channel uses  $i = [1 : n]$  should reliably decode both  $M_1$  and  $M_2$  by forming the estimate  $\widehat{M} = \text{Dec}(Y_1^n, S_1^n)$ , where  $\text{Dec}(\cdot)$  is a decoding function. The eavesdropper that observes  $Y_{2,i} \in \mathcal{Y}_2$  and  $S_{2,i} \in \mathcal{S}_2$  should be kept ignorant of  $M_2$ . Finally, the transmitter estimates the state sequence  $(S_1^n, S_2^n)$  as  $\widehat{S}_j^n = \text{Est}_j(X^n, Z^n) \in \widehat{\mathcal{S}}_j^n$  for  $j = 1, 2$ , where  $\text{Est}_j(\cdot, \cdot)$  is an estimation function. All sets  $\mathcal{S}_1, \mathcal{S}_2, \widehat{\mathcal{S}}_1, \widehat{\mathcal{S}}_2, \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2$ , and  $\mathcal{Z}$  are finite.

This channel model can be viewed as an abstraction of ISAC with a multi-functional phased array, in which a transmitter exploits backscattered waveforms (the channel output feedback  $Z^{i-1}$ ) to infer information about the states ( $S_{1,i}$  and  $S_{2,i}$ ) that affect the transmission in the directions of a legitimate receiver and an eavesdropper.

For simplicity, we consider the perfect output feedback case, in which for all  $i = [2 : n]$  we

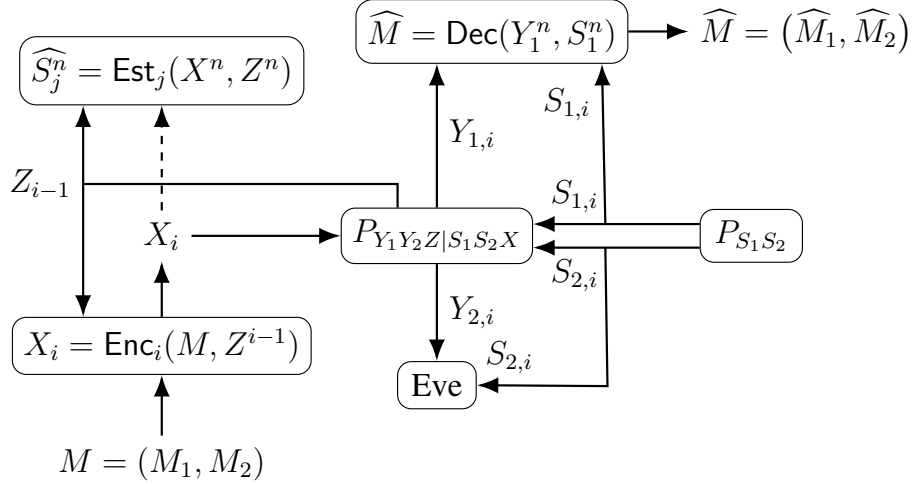


Fig. 1. ISAC model under partial secrecy, where only  $M_2$  should be kept secret from Eve, for  $j = 1, 2$  and  $i = [1 : n]$ . We mainly consider ISAC with perfect output feedback, where  $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$ .

have

$$Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1}). \quad (1)$$

Although the perfect output feedback is explicitly used in our achievability proofs, some of our converse results hold for generalized feedback. Furthermore, the fundamental insights gained from our results can be used to tackle generalized feedback scenarios, for which identifying closed-form characterizations becomes challenging; see, e.g., [18]. We next define the strong secrecy-distortion region for the problem of interest.

**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 exist  $n \geq 1$ , one encoder, one decoder, and two estimators  $\text{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S}_j^n$ ,  $j \in \{1, 2\}$ , such that

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

$$\Pr [(M_1, M_2) \neq (\widehat{M}_1, \widehat{M}_2)] \leq \delta \quad (\text{reliability}) \quad (3)$$

$$I(M_2; Y_2^n | S_2^n) \leq \delta \quad (\text{strong secrecy}) \quad (4)$$

$$\mathbb{E}[d_j(S_j^n, \widehat{S}_j^n)] \leq D_j + \delta \quad \text{for } j=1, 2 \quad (\text{distortions}) \quad (5)$$

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  $\mathcal{R}_{\text{PS,POF}}$  is the closure of the set of all achievable tuples under partial secrecy and perfect output feedback.  $\diamond$

The use of per-letter distortion metrics  $d_j(\cdot, \cdot)$  in conjunction with i.i.d. states reduces the problem to the characterization of a rate distortion region [8], [9]; in fact, past observations are independent of present and future ones, lending the transmitter no state prediction ability to adapt its transmission on the fly. Analyzing ISAC models with memory leads to conceptually different results; see, e.g., [25]–[27]. In practical ISAC applications, only a part of the channel parameters might be relevant for the transmitter [28]. Our results can be extended for such cases by adapting the estimator functions used and not requiring an estimation of the exact state.

**Remark 1.** The strong secrecy condition (4) is equivalent to  $I(M_2; Y_2^n, S_2^n) \leq \delta$  since the transmitted message is independent of the state sequence and  $I(M_2; Y_2^n, S_2^n) = I(M_2; Y_2^n | S_2^n)$ .

### III. ISAC UNDER PARTIAL SECRECY

We next present inner and outer bounds on the secrecy-distortion region  $\mathcal{R}_{\text{PS,POF}}$ .

**Proposition 1 (Inner Bound).** *The region  $\mathcal{R}_{\text{PS,POF}}$  includes the union over all joint distributions  $P_{UVX}$  of the rate tuples  $(R_1, R_2, D_1, D_2)$  such that*

$$R_1 \leq I(U; Y_1 | S_1) \quad (6)$$

$$R_2 \leq \min\{R'_2, (I(V; Y_1 | S_1) - R_1)\} \quad (7)$$

$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j)] \quad \text{for } j = 1, 2 \quad (8)$$

where

$$P_{UVXY_1Y_2S_1S_2} = P_{U|V}P_{V|X}P_XP_{S_1S_2}P_{Y_1Y_2|S_1S_2X}, \quad (9)$$

$$R'_2 = [I(V; Y_1|S_1, U) - I(V; Y_2|S_2, U)]^+ + H(Y_1|Y_2, S_2, V) \quad (10)$$

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

$$\text{Est}_j(x, y_1, y_2) = \underset{\tilde{s}_j \in \hat{\mathcal{S}}_j}{\text{argmin}} \sum_{s_j \in \mathcal{S}_j} P_{S_j|XY_1Y_2}(s_j|x, y_1, y_2) d_j(s_j, \tilde{s}_j). \quad (11)$$

One can limit  $|\mathcal{U}|$  to

$$\min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{S}_1|, |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\} + 2 \quad (12)$$

and  $|\mathcal{V}|$  to

$$(\min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{S}_1|, |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\} + 2) \cdot (\min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{S}_1|, |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\} + 1). \quad (13)$$

Proposition 1 can be interpreted as follows. The rate  $R_1$  in (6) represents a rate of a public message that could be decoded by the eavesdropper. The rate  $R'_2$  in (10) represents the rate of a secret message superposed to the public message.  $R'_2$  is itself the sum of two terms: a first term representing a wiretap-coding rate against an eavesdropper observing the public message; a second term representing a secret key rate extracted from the feedback channel and used as a one-time pad. The operator  $[\cdot]^+$  in (10) indicates that the decoder should have an advantage over the eavesdropper to apply wiretap-coding methods. The minimum operator in (7) merely indicates that the secrecy rate cannot exceed the reliable communication rate. Most importantly, Proposition 1 suggests that secure ISAC systems benefit from the inherent presence of the feedback link, which allows the transmitter to develop situational awareness and extract secret keys from the wireless environment.

*Proof of Proposition 1:* We use the OSRB method [23], [24] for the achievability proof, applying the steps in [29, Section 1.6]; see also [30]. Following [23], we shall first define an operationally dual source coding problem to the original ISAC problem, along with a coding



scheme called *Protocol A*, for which reliability and secrecy analysis is conducted. We shall next define a randomized coding scheme, called *Protocol B*, for the original ISAC problem and show that the joint probability distributions induced by Protocols A and B are almost equal, allowing us to invert the source code proposed for Protocol A to construct a channel code for Protocol B. The achievability proof shall finally follow by derandomizing Protocol B and chaining multiple uses of Protocol B over several blocks.

**Protocol A** (dual source coding problem): We consider a secret key agreement model for an i.i.d. source with distribution  $P_{UVXY_1Y_2S_1S_2}$  as in (9), in which a source encoder observing  $(U^n, V^n, X^n, Y_1^n) \in \mathcal{U}^n \times \mathcal{V}^n \times \mathcal{X}^n \times \mathcal{Y}_1^n$  assigns random bin indices  $M \in \mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$  and  $F \in \mathcal{F}$  to its observations. The index pair  $M = (M_1, M_2)$  should be reliably reconstructed at a legitimate source receiver observing  $(Y_1^n, S_1^n) \in \mathcal{Y}_1^n \times \mathcal{S}_1^n$  and  $F$  to satisfy (3), while keeping  $M_2$  secret from an eavesdropper observing  $(Y_2^n, S_2^n) \in \mathcal{Y}_2^n \times \mathcal{S}_2^n$  and  $F$  to satisfy the strong secrecy constraint (4). Furthermore, we assume that  $P_{UV|X}$  has been chosen so that distortion constraints (5) can be satisfied, i.e., there exist associated per-letter estimators  $\text{Est}_j(x, y_1, y_2) = \hat{S}_j$  for  $j = 1, 2$  such that

$$\mathbb{E}[d_j(S_j^n, \text{Est}_j^n(X^n, Y_1^n, Y_2^n))] \leq D_j + \epsilon'_n \quad (14)$$

where  $\epsilon'_n > 0$  such that  $\epsilon'_n \rightarrow 0$  when  $n \rightarrow \infty$ .

Formally, we construct Protocol A as follows. To each sequence  $u^n$ , we independently and uniformly assign two random bin indices  $(F_u, W_u)$  such that  $F_u \in [1 : 2^{n\tilde{R}_u}]$  and  $W_u \in [1 : 2^{nR_u}]$ . Furthermore, to each sequence  $v^n$ , we independently and uniformly assign three random indices  $(F_v, W_v, L_v)$  such that  $F_v \in [1 : 2^{n\tilde{R}_v}]$ ,  $W_v \in [1 : 2^{nR_v}]$ , and  $L_v \in [1 : 2^{n\bar{R}_v}]$ . Finally, to each sequence  $y_1^n$ , we independently and uniformly assign a random index  $L_{y_1} \in [1 : 2^{n\bar{R}_{y_1}}]$  with  $\bar{R}_{y_1} = \bar{R}_v$ . The index pair  $F = (F_u, F_v)$  shall be transmitted publicly to allow the reliable reconstruction of the source encoder observations at the legitimate source receiver. The index tuple  $W = (W_u, W_v, L_v)$  represent indices that can then be reliably computed at the source receiver, and we shall impose a secrecy constraint on  $W_v$ . The index  $L_{y_1}$ , which is derived from

$y_1^n$  and therefore known at both the source encoder and the legitimate receiver, shall also be subject to a secrecy constraint. We finally set

$$M_1 = W_u \quad \text{and} \quad M_2 = (W_v, L_v \oplus L_{y_1}). \quad (15)$$

We next develop conditions on the bin sizes to ensure the required reliability and secrecy constraints. Using a Slepian-Wolf [31] decoder, the expected value (over the random bin assignments) of the probability of incorrectly reconstructing  $U^n$  from  $(Y_1^n, S_1^n, F_u)$  vanishes exponentially fast when  $n \rightarrow \infty$  if we have [23, Lemma 1]

$$\tilde{R}_u > H(U|Y_1, S_1). \quad (16)$$

Similarly, the probability of incorrectly reconstructing  $V^n$  from  $(Y_1^n, S_1^n, F_v, U^n)$  vanishes exponentially fast if

$$\tilde{R}_v > H(V|Y_1, S_1, U). \quad (17)$$

Using privacy amplification [23, Theorem 1], the expected value of the variational distance between the joint probability distributions  $\text{Unif}[1 : 2^{nR_u}] \cdot \text{Unif}[1 : 2^{n\tilde{R}_u}]$  and  $P_{W_u F_u}$  vanishes exponentially fast when  $n \rightarrow \infty$  if

$$R_u + \tilde{R}_u < H(U). \quad (18)$$

With a slight abuse of terminology, we shall concisely say that the indices  $F_u$  and  $W_u$  then become almost independent and uniformly distributed. Similarly, the indices  $F_v$  and  $W_v$  become almost independent of  $(Y_2^n, S_2^n, U^n)$  and uniformly distributed if

$$R_v + \tilde{R}_v < H(V|Y_2, S_2, U) \quad (19)$$

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

$$\bar{R}_{y_1} = \bar{R}_v < H(Y_1|Y_2, S_2, V, U) \stackrel{(a)}{=} H(Y_1|Y_2, S_2, V) \quad (20)$$

where (a) follows because  $U - V - (Y_1, Y_2, S_2)$  form a Markov chain. Note that  $L_v \oplus L_{y_1}$  is then also almost independent of  $(Y_2^n, S_2^n, V^n, U^n)$  and uniformly distributed.

Finally,  $(F_u, W_u, F_v, W_v, L_v)$  are almost mutually independent and uniformly distributed if

$$R_u + \tilde{R}_u + R_v + \tilde{R}_v + \bar{R}_v < H(U, V). \quad (21)$$

Assuming  $I(V; Y_1, S_1|U) - I(V; Y_2, S_2|U) > 0$  and  $\epsilon > 0$  small enough, a specific choice of rates that satisfies all conditions above is

$$\tilde{R}_u = H(U|Y_1, S_1) + \epsilon \quad (22)$$

$$R_u = H(U) - H(U|Y_1, S_1) - 2\epsilon = I(U; Y_1|S_1) - 2\epsilon \quad (23)$$

$$\tilde{R}_v = H(V|Y_1, S_1, U) + \epsilon \quad (24)$$

$$R_v = H(V|Y_2, S_2, U) - H(V|Y_1, S_1, U) - 2\epsilon = I(V; Y_1|S_1, U) - I(V; Y_2|S_2, U) - 2\epsilon \quad (25)$$

$$\bar{R}_v = \min\{(H(Y_1|Y_2, S_2, U, V) - \epsilon), (H(U, V) - H(U) - H(V|Y_2, S_2, U))\} \quad (26)$$

$$= \min\{(H(Y_1|Y_2, S_2, V) - \epsilon), I(V; Y_2|S_2, U)\}, \quad (27)$$

where we have repeatedly used the independence of  $(U, V)$  with  $(S_1, S_2)$  to simplify the expressions. If  $(I(V; Y_1, S_1|U) - I(V; Y_2, S_2|U)) \leq 0$ , one should set

$$R_v = 0 \quad \text{and} \quad \bar{R}_v = \min\{H(Y_1|Y_2, S_2, V), I(V; Y_1|S_1, U)\} - \epsilon. \quad (28)$$

Combining the above of choices with our definition  $R_1 = R_u$  and  $R_2 = R_v + \bar{R}_v$ , we recover the rate conditions in Proposition 1, satisfying the reliability condition (3) and the secrecy condition (4). Finally, we consider the distortion constraints (5) on the channel state estimations. All  $(u^n, v^n, x^n, y_1^n, y_2^n, s_1^n, s_2^n)$  tuples are in the jointly typical set with high probability and, by applying the law of total expectation to bounded distortion metrics and from the typical average lemma [32, pp. 26], distortion constraints (5) are satisfied; see also [33]. Furthermore, without loss of generality one can use the deterministic per-letter estimators in (11) and the proof follows from the proof of [8, Lemma 1] by replacing  $(S, Z, \hat{S}, d)$  with  $(S_j, (Y_1, Y_2), \hat{S}_j, d_j)$ , respectively, since  $\hat{S}_j - (X, Y_1, Y_2) - S_j$  form a Markov chain for all  $j = 1, 2$ .

This concludes the construction and analysis of Protocol A. Note that Protocol A induces a joint probability distribution  $P_{M_1 M_2 F X^n} P_{S_1^n S_2^n} P_{Y_1^n Y_2^n | S_1^n S_2^n X^n}$  that is asymptotically indistinguishable in variational distance from a distribution of the form

$$\text{Unif}[1 : 2^{n(\tilde{R}_u + \tilde{R}_v)}] \cdot \text{Unif}[1 : 2^{n(R_u + R_v + \bar{R}_v)}] \cdot P_{S_1^n S_2^n} P_{X^n | M_1 M_2 F} P_{Y_1^n Y_2^n | S_1^n S_2^n X^n}. \quad (29)$$

**Protocol B** (random channel coding for the original problem): We now transform Protocol A into another protocol that is suited to the original ISAC problem. Assume that the index pair  $F = (F_u, F_v)$  is generated uniformly at random and disclosed to all parties ahead of the transmission and that the transmitter and the receiver share a secret key  $K \in \text{Unif}[1 : 2^{\bar{R}_{y_1}}]$ . Then, the transmitter encodes a uniformly distributed message  $M_1 = W_u$  and another uniformly distributed message  $M_2 = (W_v, L_v \oplus K)$  according to the distribution  $P_{X^n | M_1 M_2 F}$ , defined by Protocol A. Note that Protocol B induces a joint probability distribution as in (29), which is, as argued above, asymptotically indistinguishable in variational distance from the distribution  $P_{M_1 M_2 F X^n} P_{S_1^n S_2^n} P_{Y_1^n Y_2^n | S_1^n S_2^n X^n}$ , induced by Protocol A. In other words, Protocol B guarantees the exact same asymptotic performance as Protocol A in terms of secrecy, reliability, and distortions subject to the same rate constraints.

**Derandomizing and Chaining Protocol B.** To conclude the achievability, two aspects of Protocol B remain to be fixed to obtain a code for the original JSAC model: i) the public transmission of the index  $F$  should be removed; and ii) the use of the secret key  $K$  should be removed. Following [23], one can argue that there exists a fixed index  $F = f$  such that Protocol B retains its properties, eliminating the need for a public discussion. We skip this standard step for brevity. Most importantly, note that Protocol A allows us to generate a secret key  $L_{y_1}$ . Consequently, if one were to use Protocol B in a block Markov fashion chained over multiple blocks, the key generated in block  $b \geq 1$  can be used as the key for one-time padding in block  $(b + 1)$ , removing the need for a secret key in Protocol B.

Formally, assume that we repeat Protocol B over  $B$  blocks indexed by  $b \in [1 : B]$ . In every block  $b$ , we denote the messages by a superscript  $b$ . In particular, the transmitter attempts to

transmit messages  $W_u^b$ ,  $W_v^b$ , and  $L_v^b$ , as well as generate a key  $L_{y_1}^b$ . In this section alone, we also denote a sequence of variables across blocks  $k$  through  $\ell$  ( $\ell \geq k$ ) by the superscript  $k : \ell$ , e.g.,  $M_1^{k:\ell}$ . In the first block, no message is transmitted and only a key  $L_{y_1}^1$  is generated. In every subsequent block  $b \in [2 : B]$ , the encoder uses Protocol B to transmit a public message  $M_1^b = W_u^b$  and a secret message  $M_2^b = (W_v^b, L_v^b \oplus L_{y_1}^{b-1})$ , and generates a key  $L_{y_1}^b$ . A union bound shows that the asymptotic reliability performance

$$\lim_{n \rightarrow \infty} \Pr \left[ \left\{ \widehat{M}_1^{1:B} \neq M_1^{1:B} \text{ or } \widehat{M}_2^{1:B} \neq M_2^{1:B} \right\} \right] \quad (30)$$

is not affected by the chaining. The proof that secrecy is not affected by the chaining requires a bit more care, as we need to show that  $I(W_v^{1:B}, L_v^{1:B}; \mathbf{Y}_2^{1:B}, \mathbf{S}_2^{1:B})$ , where the bold-face letters represent  $n$ -letter random variables, vanishes across all blocks. This can be done by adapting the approach of [34] and [35] as we show next. To simplify notation, we set  $W^b = W_v^b$ ,  $L^b = L_v^b$ ,  $K^b = L_{y_1}^b$ , and  $\mathbf{Z}^b = (\mathbf{Y}_2^b, \mathbf{S}_2^b)$ .

We have

$$\begin{aligned} I(W^{1:B}, L^{1:B}; \mathbf{Z}^B) &= \sum_{b=1}^{B-1} (I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b})) + I(W^{1:B}, L^{1:B}; \mathbf{Z}^1) \\ &\stackrel{(a)}{=} \sum_{b=1}^{B-1} (I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b})) \end{aligned} \quad (31)$$

where (a) follows since  $I(W^{1:B}, L^{1:B}; \mathbf{Z}^1) = I(W^1, L^1; \mathbf{Z}^1) = 0$  by definition because no message is transmitted in the first block. Focusing on every term in the sum for a given index  $b$ , we obtain

$$\begin{aligned} &I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b+1}) - I(W^{1:B}, L^{1:B}; \mathbf{Z}^{1:b}) \\ &= I(W^{1:B}, L^{1:B}; \mathbf{Z}^{b+1} | \mathbf{Z}^{1:b}) \\ &= I(W^{1:b+1}, L^{1:b+1}; \mathbf{Z}^{b+1} | \mathbf{Z}^{1:b}) + I(W^{b+2:B}, L^{b+2:B}; \mathbf{Z}^{b+1} | \mathbf{Z}^{1:b}, W^{1:b+1}, L^{1:b+1}) \\ &\leq I(W^{1:b+1}, L^{1:b+1}, \mathbf{Z}^{1:b}, \mathbf{Z}^{b+1}) + I(W^{b+2:B}, L^{b+2:B}; \mathbf{Z}^{1:b+1}, W^{1:b+1}, L^{1:b+1}) \\ &\stackrel{(a)}{=} I(W^{1:b+1}, L^{1:b+1}, \mathbf{Z}^{1:b}, \mathbf{Z}^{b+1}) \end{aligned}$$

$$\begin{aligned}
&= I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1} | W^{b+1}, L^{b+1}) \\
&\stackrel{(b)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}) \\
&\stackrel{(c)}{\leq} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}, K^b) \\
&= I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; K^b) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1} | K^b) \\
&\stackrel{(d)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; K^b) \\
&\stackrel{(e)}{\leq} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}, K^{b-1}; K^b) \\
&\stackrel{(f)}{=} I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b) \tag{32}
\end{aligned}$$

where (a) follows because the future messages  $(W^{b+2:B}, L^{b+2:B})$  are independent of past messages and observations  $(\mathbf{Z}^{1:b+1}, W^{1:b+1}, L^{1:b+1})$ , (b) follows similarly because future messages  $(W^{b+1}, L^{b+1})$  are independent of past messages and observations  $(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b})$ , (c) follows by introducing the key  $K^b$  generated in block  $b$  as an attempt to break dependence across blocks, (d) follows because  $I(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}; \mathbf{Z}^{b+1}, W^{b+1}, L^{b+1} | K^b) = 0$  since

$$(W^{1:b}, L^{1:b}, \mathbf{Z}^{1:b}) - K_b - (\mathbf{Z}^{b+1}, W^{b+1}, L^{b+1}) \tag{33}$$

form a Markov chain, (e) follows by introducing  $K^{b-1}$  in an effort to break again dependence, and (f) follows since  $I(W^{1:b-1}, L^{1:b-1}, \mathbf{Z}^{1:b-1}; K^b | W^b, L^b, \mathbf{Z}^b, K^{b-1}) = 0$  since

$$(W^{1:b-1}, L^{1:b-1}, \mathbf{Z}^{1:b-1}) - (W^b, L^b, \mathbf{Z}^b, K^{b-1}) - K_b \tag{34}$$

form a Markov chain. Consequently, we obtain

$$I(W^{1:B}, L^{1:B}; \mathbf{Z}^B) \leq \sum_{b=1}^{B-1} (I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) + I(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b)). \tag{35}$$

All that remains to confirm is that in each block,  $I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1})$  and  $I(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b)$

are asymptotically vanishing. For the first term, note that

$$\begin{aligned}
I(W^{b+1}, L^{b+1}; \mathbf{Z}^{b+1}) &= I(W^{b+1}; \mathbf{Z}^{b+1}) + I(L^{b+1}; \mathbf{Z}^{b+1} | W^{b+1}) \\
&\stackrel{(a)}{=} I(W^{b+1}; \mathbf{Z}^{b+1}) + I(L^{b+1}; \mathbf{Z}^{b+1}, W^{b+1}) \\
&\stackrel{(b)}{\leq} I(W^{b+1}; \mathbf{Z}^{b+1}) + I(L^{b+1}; L^{b+1} \oplus K^b) \\
&\stackrel{(c)}{=} I(W^{b+1}; \mathbf{Z}^{b+1}) + n\bar{R}_v - H(K^b), \tag{36}
\end{aligned}$$

where (a) follows by independence of  $W^{b+1}$  and  $L^{b+1}$ , (b) follows because of the MARKov chain  $L^{b+1} - (L^{b+1} \oplus K^b) - (\mathbf{Z}^{b+1}, W^{b+1})$ , and (c) follows because  $I(L^{b+1}; L^{b+1} \oplus K^b) = (H(L^{b+1} \oplus K^b) - H(L^{b+1} \oplus K^b | L^{b+1})) \leq (n\bar{R}_v - H(K^b))$ . Looking back at Protocols A and B, the secrecy of  $W^{b+1}$  and the uniformity of  $K^b$  guarantee that  $I(W^{b+1}; \mathbf{Z}^{b+1})$  and  $(n\bar{R}_v - H(K^b))$  are exponentially vanishing as  $n \rightarrow \infty$ ; see (19) and (20). Similarly, for the second term, the secrecy of  $K^b$  guarantees directly that  $I(W^b, L^b, \mathbf{Z}^b, K^{b-1}; K^b)$  is exponentially vanishing as  $n \rightarrow \infty$ ; see (20).

Lastly, one can check that the chaining over  $B$  blocks has a negligible effect on the rate of the coding scheme. ■

**Proposition 2** (Outer Bound). *The region  $\mathcal{R}_{\text{PS,POF}}$  is included in the union over all joint distributions  $P_{UVX}$  of the rate tuples  $(R_1, R_2, D_1, D_2)$  satisfying (8) and*

$$R_1 \leq I(V; Y_1 | S_1) \tag{37}$$

$$R_2 \leq \min \left\{ (H(Y_1, S_1 | Y_2, S_2) - H(S_1 | Y_1, Y_2, S_2, V)), (I(V; Y_1 | S_1) - R_1) \right\} \tag{38}$$

where we have (9) and (11). One can limit  $|\mathcal{V}|$  to

$$\min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{S}_1|, |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\} + 1. \tag{39}$$

**Remark 2.** Since we consider perfect feedback as in (1), the outer bound proposed in Proposition 2 is also valid for the general ISAC problem depicted in Fig. 1, in which the feedback  $Z_{i-1}$  can be a noisy version of  $(Y_{1,i-1}, Y_{2,i-1})$ .

*Proof of Proposition 2:* Assume that for some  $\delta_n > 0$  and  $n \geq 1$ , there exist an encoder, decoder, and estimators such that (2)-(5) are satisfied for some tuple  $(R_1, R_2, D_1, D_2)$ . Using Fano's inequality and (3), we have

$$H(M|Y_1^n, S_1^n) \stackrel{(a)}{\leq} H(M|\widehat{M}) \leq n\epsilon_n \quad (40)$$

where (a) allows randomized decoding and  $\epsilon_n = \delta_n(R_1 + R_2) + H_b(\delta_n)/n$  such that  $\epsilon_n \rightarrow 0$  if  $\delta_n \rightarrow 0$ .

Let  $V_i \triangleq (M_1, M_2, Y_1^{i-1}, S_1^{i-1}, Y_2^{i-1}, S_2^{i-1})$  such that  $V_i - X_i - (Y_{1,i}, Y_{2,i}, S_{1,i}, S_{2,i})$  form a Markov chain for all  $i \in [1 : n]$  by definition of the channel statistics.

**Bound on  $R_1$ :** We have

$$\begin{aligned} nR_1 &\stackrel{(a)}{\leq} I(M_1; Y_1^n | S_1^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n (H(Y_{1,i} | S_{1,i}) - H(Y_{1,i} | M_1, M_2, Y_1^{i-1}, S_1^n) + \epsilon_n) \\ &\stackrel{(b)}{\leq} \sum_{i=1}^n (H(Y_{1,i} | S_{1,i}) - H(Y_{1,i} | M_1, M_2, Y_1^{i-1}, S_1^i, Y_2^{i-1}, S_2^{i-1}) + \epsilon_n) \\ &\stackrel{(c)}{=} \sum_{i=1}^n (I(V_i; Y_{1,i} | S_{1,i}) + \epsilon_n) \end{aligned} \quad (41)$$

where (a) follows by (40) and because  $M_1$  and  $S_1^n$  are independent, (b) follows since

$$S_{1,i+1}^n - (M_1, M_2, Y_1^{i-1}, S_1^i) - Y_{1,i} \quad (42)$$

form a Markov chain, and (c) follows from the definition of  $V_i$ .

**Bound on  $(R_1 + R_2)$ :** Similar to (41), we obtain

$$\begin{aligned} n(R_1 + R_2) &\stackrel{(a)}{\leq} I(M_1, M_2; Y_1^n | S_1^n) + n\epsilon_n \\ &\stackrel{(b)}{\leq} \sum_{i=1}^n (H(Y_{1,i} | S_{1,i}) - H(Y_{1,i} | M_1, M_2, Y_1^{i-1}, S_1^i, Y_2^{i-1}, S_2^{i-1}) + \epsilon_n) \\ &\stackrel{(c)}{=} \sum_{i=1}^n (I(V_i; Y_{1,i} | S_{1,i}) + \epsilon_n) \end{aligned} \quad (43)$$

where (a) follows because  $(M_1, M_2, S_1^n)$  are mutually independent and by (40), (b) follows since (42) form a Markov chain, and (c) follows from the definition of  $V_i$ .



**Bound on  $R_2$ :** We obtain

$$\begin{aligned}
nR_2 &\stackrel{(a)}{\leq} I(M_2; Y_1^n, Y_2^n, S_1^n, S_2^n) + n\epsilon_n \\
&\leq H(Y_1^n, S_1^n | Y_2^n, S_2^n) + H(Y_2^n, S_2^n) - H(Y_2^n, S_2^n | M_2) - H(Y_1^n, S_1^n | Y_2^n, S_2^n, M_1, M_2) + n\epsilon_n \\
&\leq H(Y_1^n, S_1^n | Y_2^n, S_2^n) + I(Y_2^n, S_2^n; M_2) - \sum_{i=1}^n H(S_{1,i} | Y_1^n, Y_2^n, S_2^n, M_1, M_2, S_1^{i-1}) + n\epsilon_n \\
&\stackrel{(b)}{\leq} H(Y_1^n, S_1^n | Y_2^n, S_2^n) + \delta_n - \sum_{i=1}^n H(S_{1,i} | Y_1^i, Y_2^i, S_2^i, M_1, M_2, S_1^{i-1}) + n\epsilon_n \\
&\stackrel{(c)}{=} H(Y_1^n, S_1^n | Y_2^n, S_2^n) + \delta_n - \sum_{i=1}^n H(S_{1,i} | Y_{1,i}, Y_{2,i}, S_{2,i}, V_i) + n\epsilon_n \\
&\leq \sum_{i=1}^n (H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) - H(S_{1,i} | Y_{1,i}, Y_{2,i}, S_{2,i}, V_i)) + n\epsilon_n + \delta_n \tag{44}
\end{aligned}$$

where (a) follows by (40), (b) follows by (4) and from Remark 1, and because

$$(Y_{1,i+1}^n, Y_{2,i+1}^n, S_{2,i+1}^n) - (Y_1^i, Y_2^i, S_2^i, M_1, M_2, S_1^{i-1}) - S_{1,i} \tag{45}$$

form a Markov chain, and (c) follows from the definition of  $V_i$ .

**Distortion Bounds:** We have for  $j = 1, 2$

$$(D_j + \delta_n) \stackrel{(a)}{\geq} \mathbb{E}[d_j(S_j^n, \widehat{S}_j^n)] = \frac{1}{n} \sum_{i=1}^n \mathbb{E}[d_j(S_{j,i}, \widehat{S}_{j,i})] \tag{46}$$

where (a) follows by (5), which can be achieved by using the deterministic per-letter estimators in (11).

Introduce a uniformly distributed time-sharing random variable  $Q \sim \text{Unif}[1:n]$  that is independent of other random variables, and define  $Y_1 = Y_{1,Q}$ ,  $S_1 = S_{1,Q}$ ,  $Y_2 = Y_{2,Q}$ ,  $S_2 = S_{2,Q}$ ,  $X = X_Q$ , and  $V = (V_Q, Q)$ , so  $V - X - (Y_1, Y_2, S_1, S_2)$  form a Markov chain. The proof of the outer bound follows by letting  $\delta_n \rightarrow 0$ .

**Cardinality Bounds:** We use the support lemma [36, Lemma 15.4] to prove the cardinality bound, which is a standard procedure, so we omit the proof. ■

We next characterize the exact secrecy-distortion regions for physically-degraded and reversely-physically-degraded ISAC channels, which are defined below.

**Definition 2.** An ISAC channel  $P_{Y_1Y_2|S_1S_2X}$  is *physically-degraded* if we have

$$P_{Y_1Y_2S_1S_2|X} = P_{Y_1Y_2|S_1S_2X}P_{S_1S_2} = P_{S_1}P_{Y_1|S_1X}P_{Y_2S_2|S_1Y_1} \quad (47)$$

and is *reversely-physically-degraded* if the degradation order is changed such that

$$P_{Y_1Y_2S_1S_2|X} = P_{Y_1Y_2|S_1S_2X}P_{S_1S_2} = P_{S_2}P_{Y_2|S_2X}P_{Y_1S_1|S_2Y_2}. \quad (48)$$

◇

A physically-degraded ISAC channel corresponds to a situation in which the observation  $Y_2$  of the eavesdropper given its state  $S_2$  is a degraded version of the observation  $Y_1$  of the legitimate receiver given its state  $S_1$  with respect to the channel input  $X$ .

**Theorem 1.** (Physically-degraded Channels): *For a physically-degraded ISAC channel,  $\mathcal{R}_{\text{PS,POF}}$  is the union over all joint distributions  $P_{VX}$  of the rate tuples  $(R_1, R_2, D_1, D_2)$  satisfying (8), (37), and (38), where we have (9) with constant  $U$  and (11). One can limit  $|\mathcal{V}|$  to (39).*

*Proof of Theorem 1:* Since the outer bound given in Proposition 2 does not assume any degradedness, the outer bound terms for  $R_1$ ,  $R_2$ , and  $D_j$  for  $j = 1, 2$  follow from Proposition 2.

The achievability proof for Theorem 1 follows by modifying the construction and analysis of Protocol A in the proof of Proposition 1. We next provide a sketch of the modifications for a physically-degraded ISAC channel. First,  $U^n$  is not used, i.e.,  $U^n$  is eliminated from the achievability proof. Second, to each  $v^n$  we assign four random bin indices  $(F_v, W_{v_1}, W_{v_2}, L_v)$  such that  $F_v \in [1 : 2^{n\tilde{R}_v}]$ ,  $W_{v_1} \in [1 : 2^{nR_{v_1}}]$ ,  $W_{v_2} \in [1 : 2^{nR_{v_2}}]$ , and  $L_v \in [1 : 2^{n\bar{R}_v}]$  independently such that  $M_1 = W_{v_1}$  and  $M_2 = (W_{v_2}, L_v)$ . As in (17), we impose the reliability constraint

$$\tilde{R}_v > H(V|Y_1, S_1) \quad (49)$$

as in (19) and (20) we impose the strong secrecy constraints

$$R_{v_2} + \tilde{R}_v < H(V|Y_2, S_2) \quad (50)$$

$$\bar{R}_v < H(Y_1|Y_2, S_2, V) \quad (51)$$

and as in (21) we impose the mutual independence and uniformity constraint

$$R_{v_1} + R_{v_2} + \tilde{R}_v + \bar{R}_v < H(V). \quad (52)$$

We remark that we have  $H(V|Y_2, S_2) \geq H(V|Y_1, S_1)$  for all physically-degraded ISAC channels, i.e., we obtain

$$[I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ \stackrel{(a)}{=} H(V|Y_2, S_2) - H(V|Y_1, S_1) \quad (53)$$

where (a) follows because  $V$  is independent of  $(S_1, S_2)$  and since

$$V - X - (Y_1, S_1) - (Y_2, S_2) \quad (54)$$

form a Markov chain for such ISAC channels. Define

$$\begin{aligned} R'_{2,\text{deg}} &= [I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ + H(Y_1|Y_2, S_2, V) \\ &\stackrel{(a)}{=} H(V|Y_2, S_2) - H(V|Y_1, S_1) + H(Y_1|Y_2, S_2, V) \\ &\stackrel{(b)}{=} H(Y_1, V|Y_2, S_2) - H(V|Y_1, S_1, Y_2, S_2) \\ &= H(Y_1|Y_2, S_2) + I(V; S_1|Y_1, Y_2, S_2) \\ &= H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, V) \end{aligned} \quad (55)$$

where (a) follows by (53) and (b) follows from the Markov chain in (54).

Applying the Fourier-Motzkin elimination [37] to (49)-(52), for any  $\epsilon > 0$  one can achieve

$$R_1 = R_{v_1} = I(V; Y_1, S_1) - 2\epsilon = I(V; Y_1|S_1) - 2\epsilon \quad (56)$$

and for any  $R_1$  that is less than or equal to (56), one can simultaneously achieve

$$R_2 = R_{v_2} + \bar{R}_v = \min\{R'_{2,\text{deg}}, (I(V; Y_1|S_1) - R_1)\} - 3\epsilon. \quad (57)$$

The construction of Protocol B, the analysis of achievable distortions and sufficiency of deterministic estimators, as well as the de-randomization and chaining analysis, follow as in the proof of Proposition 1 and are omitted for brevity. ■

**Theorem 2.** (Reversely-physically-degraded Channels): *For a reversely-physically-degraded ISAC channel,  $\mathcal{R}_{\text{PS,POF}}$  is the union over all joint distributions  $P_{VX}$  of the rate tuples  $(R_1, R_2, D_1, D_2)$  satisfying (8), (37), and*

$$R_2 \leq \min \{H(Y_1|Y_2, S_2), (I(V; Y_1|S_1) - R_1)\} \quad (58)$$

where we have (9) with constant  $U$  and (11). One can limit  $|\mathcal{V}|$  to

$$\min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{S}_1|, |\mathcal{Y}_2| \cdot |\mathcal{S}_2|\}. \quad (59)$$

*Proof of Theorem 2:* The achievability proof follows from Proposition 1 after elimination of  $U$  from its proof, as in the proof for Theorem 1. After removal of  $U$ , by (7) we have the inner bound

$$\begin{aligned} R_2 &\stackrel{(a)}{\leq} \min \{H(Y_1|Y_2, S_2, V), (I(V; Y_1|S_1) - R_1)\} \\ &\stackrel{(b)}{=} \min \{H(Y_1|Y_2, S_2), (I(V; Y_1|S_1) - R_1)\} \end{aligned} \quad (60)$$

where (a) follows since  $V$  is independent of  $(S_1, S_2)$  and because  $H(V|Y_1, S_1) \geq H(V|Y_2, S_2)$  for all reversely-physically-degraded ISAC channels because of the Markov chain

$$V - X - (Y_2, S_2) - (Y_1, S_1) \quad (61)$$

and (b) follows also because of the Markov chain in (61).

Since the outer bound in Proposition 2 does not assume any degradedness, the outer bound terms for  $R_1$  and  $D_j$  for  $j = 1, 2$  follow from Proposition 2. Furthermore, by (38) we obtain the outer bound

$$\begin{aligned} R_2 &\stackrel{(a)}{\leq} \min \{(H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2)), (I(V; Y_1|S_1) - R_1)\} \\ &= \min \{H(Y_1|Y_2, S_2), (I(V; Y_1|S_1) - R_1)\} \end{aligned} \quad (62)$$

where (a) follows from the Markov chain in (61). ■

#### IV. ISAC UNDER FULL SECRECY

We next give inner and outer bounds for the situation, in which  $M = M_2$  should be kept secret from the eavesdropper and  $M_1 = \emptyset$ . For this situation, the definitions of an achievable secrecy-distortion tuple  $(R, D_1, D_2)$  and corresponding strong secrecy-distortion region  $\mathcal{R}_{\text{POF}}$  follow from Definition 1 by eliminating  $(M_1, R_1)$  and replacing  $(M_2, R_2, \mathcal{R}_{\text{PS,POF}})$  with  $(M, R, \mathcal{R}_{\text{POF}})$ , respectively.

**Proposition 3.** (Inner Bound): *The region  $\mathcal{R}_{\text{POF}}$  includes the union over all joint distributions  $P_{VX}$  of the rate tuples  $(R, D_1, D_2)$  satisfying (8) and*

$$R \leq \min\{R'', I(V; Y_1|S_1)\} \quad (63)$$

where

$$P_{VXY_1Y_2S_1S_2} = P_{V|X}P_XP_{S_1S_2}P_{Y_1Y_2|S_1S_2X}, \quad (64)$$

$$R'' = [I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ + H(Y_1|Y_2, S_2, V) \quad (65)$$

and one can apply the deterministic per-letter estimators in (11). One can limit  $|\mathcal{V}|$  to (39).

*Proof of Proposition 3:* The proof follows by eliminating  $U$  in the proof of Proposition 1, so  $R_1 = R_{v_1} = 0$  and by imposing (49)-(52) after replacing  $R_{v_2}$  with  $R_v$ , since for this case we have  $M = (W_v, L_v)$ . ■

**Proposition 4.** (Outer Bound): *The region  $\mathcal{R}_{\text{POF}}$  is included in the union over all  $P_X$  of the rate tuples  $(R, D_1, D_2)$  satisfying (8) and*

$$R \leq \min \left\{ \left( H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X) \right), I(X; Y_1|S_1) \right\} \quad (66)$$

where one can apply the deterministic per-letter estimators in (11).

*Proof of Proposition 4:* Assume that for some  $\delta_n > 0$  and  $n \geq 1$ , there exist an encoder, a decoder, and estimators such that all constraints imposed on the ISAC problem with perfect

output feedback are satisfied for some tuple  $(R, D_1, D_2)$ . We then obtain

$$\begin{aligned}
nR &\stackrel{(a)}{\leq} I(M; Y_1^n | S_1^n) + n\epsilon_n \\
&\leq \sum_{i=1}^n (H(Y_{1,i} | S_{1,i}) - H(Y_{1,i} | Y_1^{i-1}, S_1^n, M, X_i) + \epsilon_n) \\
&\stackrel{(b)}{=} \sum_{i=1}^n (H(Y_{1,i} | S_{1,i}) - H(Y_{1,i} | S_{1,i}, X_i) + \epsilon_n) \\
&= \sum_{i=1}^n (I(X_i; Y_{1,i} | S_{1,i}) + \epsilon_n)
\end{aligned} \tag{67}$$

where (a) follows because  $M$  and  $S_1^n$  are independent, and from Fano's inequality for an  $\epsilon_n > 0$  such that  $\epsilon_n \rightarrow 0$  if  $\delta_n \rightarrow 0$ , which is entirely similar to (40), and (b) follows because

$$Y_{1,i} - (S_{1,i}, X_i) - (Y_1^{i-1}, S_1^{n \setminus i}, M) \tag{68}$$

form a Markov chain. Furthermore, we also have

$$\begin{aligned}
nR &\stackrel{(a)}{\leq} I(M; Y_1^n, Y_2^n, S_1^n, S_2^n) + n\epsilon_n \\
&= H(Y_1^n, S_1^n | Y_2^n, S_2^n) + I(Y_2^n, S_2^n; M) - H(Y_1^n, S_1^n | Y_2^n, S_2^n, M) + n\epsilon_n \\
&\stackrel{(b)}{\leq} \sum_{i=1}^n H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) + \delta_n - \sum_{i=1}^n H(S_{1,i} | Y_1^n, Y_2^n, S_2^n, M, S_1^{i-1}, X_i) + n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{i=1}^n (H(Y_{1,i}, S_{1,i} | Y_{2,i}, S_{2,i}) - H(S_{1,i} | Y_{1,i}, Y_{2,i}, S_{2,i}, X_i) + \epsilon_n) + \delta_n
\end{aligned} \tag{69}$$

where (a) follows from Fano's inequality, which is similar to (40), (b) follows by (4) and from Remark 1 after replacing  $M_2$  with  $M$  for the ISAC problem with a single secure message, and (c) follows because

$$S_{1,i} - (Y_{1,i}, Y_{2,i}, S_{2,i}, X_i) - (Y_1^{n \setminus i}, Y_2^{n \setminus i}, S_2^{n \setminus i}, M, S_1^{i-1}) \tag{70}$$

form a Markov chain. Thus, by applying the distortion bound in (46) and introducing a uniformly-distributed time-sharing random variable, as being applied in the proof of Proposition 2, we prove the outer bound for the ISAC problem with a single secure message and perfect output feedback by letting  $\delta_n \rightarrow 0$ . ■

We next present the exact strong secrecy-distortion regions for the ISAC problem with a single secure message when the ISAC channel  $P_{Y_1Y_2|S_1S_2X}$  is physically-degraded, as in (47), or reversely-physically-degraded, as in (48).

**Theorem 3.** (Physically-degraded Channels): *For a physically-degraded ISAC channel,  $\mathcal{R}_{\text{POF}}$  is the union over all probability distributions  $P_X$  of the rate tuples  $(R, D_1, D_2)$  satisfying (8) and (66), where we have (11).*

*Proof of Theorem 3:* Since the bound given in Proposition 4 is valid for any ISAC channel, the proof for the outer bound follows from Proposition 4. Furthermore, the achievability proof follows by modifying the proof of Theorem 1 such that we assign  $V^n(k) = X^n(k)$  for all  $k = [1 : b]$  and then apply the same OSRB steps for  $X^n(k)$  rather than  $V^n(k)$ , i.e., replace  $V$  with  $X$  in the inner bound terms given in Proposition 3. Define

$$\begin{aligned} R''_{\text{deg}} &= [I(X; Y_1|S_1) - I(X; Y_2|S_2)]^+ + H(Y_1|Y_2, S_2, X) \\ &\stackrel{(a)}{=} I(X; Y_1, S_1|Y_2, S_2) + H(Y_1|Y_2, S_2, X) \\ &= H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X) \end{aligned} \quad (71)$$

where (a) follows because the ISAC channel is physically-degraded, and since  $X$  is independent of  $(S_1, S_2)$ . Thus, by (63) we have

$$R \leq \min\{R''_{\text{deg}}, I(X; Y_1|S_1)\} \quad (72)$$

which proves the achievability bound. ■

**Theorem 4.** (Reversely-physically-degraded Channels): *For a reversely-physically-degraded ISAC channel,  $\mathcal{R}_{\text{POF}}$  is the union over all probability distributions  $P_X$  of the rate tuples  $(R, D_1, D_2)$  satisfying (8) and*

$$R \leq \min\{H(Y_1|Y_2, S_2), I(X; Y_1|S_1)\} \quad (73)$$

where one can apply the deterministic per-letter estimators in (11).

*Proof of Theorem 4:* We assign  $V^n = X^n$  in the achievability proof, i.e., we choose  $V = X$  that is allowed by (64), such that by (63) we obtain the inner bound

$$\begin{aligned} R &\stackrel{(a)}{\leq} \min \{H(Y_1|Y_2, S_2, X), I(X; Y_1|S_1)\} \\ &\stackrel{(b)}{=} \min \{H(Y_1|Y_2, S_2), I(X; Y_1|S_1)\} \end{aligned} \quad (74)$$

where (a) follows since  $X$  is independent of  $(S_1, S_2)$  and because  $H(X|Y_1, S_1) \geq H(X|Y_2, S_2)$  for all reversely-physically-degraded ISAC channels due to the Markov chain in (61), and (b) follows also because of the Markov chain in (61).

Since the outer bound in Proposition 4 does not assume any degradedness, the outer bound terms for  $D_j$  for  $j = 1, 2$  follow from Proposition 4. Furthermore, by (66) we have the outer bound

$$\begin{aligned} R &\stackrel{(a)}{\leq} \min \left\{ \left( H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2) \right), I(X; Y_1|S_1) \right\} \\ &= \min \{H(Y_1|Y_2, S_2), I(X; Y_1|S_1)\} \end{aligned} \quad (75)$$

where (a) follows from the Markov chain in (61). ■

## V. ISAC CHANNELS WITH BERNOULLI STATES

### A. Binary Noiseless ISAC Channels with Bernoulli States

We next consider a scenario with perfect output feedback and single secure message, in which channel input and output alphabets are binary with multiplicative Bernoulli states, which serves as a coarse model of fading channels with high signal-to-noise ratio. Specifically, we have

$$Y_1 = S_1 \cdot X, \quad Y_2 = S_2 \cdot X \quad (76)$$

and

$$P_{S_1 S_2}(0, 0) = (1 - q), \quad P_{S_1 S_2}(1, 1) = q\alpha, \quad P_{S_1 S_2}(0, 1) = 0, \quad P_{S_1 S_2}(1, 0) = q(1 - \alpha) \quad (77)$$

for fixed  $q, \alpha \in [0, 1]$ , so the ISAC channel is stochastically-degraded, i.e., there exists a marginal probability distribution such that the ISAC channel can be represented as in (47). The constraints



(2)-(5) in Definition 1 only depend on the marginal probability distributions of  $(X, Y_1, S_1)$  and  $(X, Y_2, S_2)$  when per-letter estimators of the form  $\text{Est}_j(x, y_j)$  are imposed for  $j = 1, 2$ , so the secrecy-distortion region given in Theorem 3 is also valid for stochastically-degraded ISAC channels.

**Lemma 1.** *The strong secrecy-distortion region  $\mathcal{R}_{\text{POF}}$  for a binary ISAC channel with multiplicative Bernoulli states characterized by parameters  $(q, \alpha)$  and with Hamming distortion metrics is the union over all  $p \in [0, 1]$ , where  $X \sim \text{Bern}(p)$ , of the rate tuples  $(R, D_1, D_2)$  satisfying*

$$R \leq \min \left\{ \left( q(1 - \alpha)H_b(p) + p(1 - q\alpha)H_b\left(\frac{q(1 - \alpha)}{(1 - q\alpha)}\right) \right), qH_b(p) \right\} \quad (78)$$

$$D_1 \geq (1 - p) \cdot \min\{q, (1 - q)\} \quad (79)$$

$$D_2 \geq (1 - p) \cdot \min\{q\alpha, (1 - q\alpha)\}. \quad (80)$$

*Proof of Lemma 1:* The proof follows by evaluating the strong secrecy-distortion region  $\mathcal{R}_{\text{POF}}$  defined in Theorem 3. Proofs for (79) and (80) follow by choosing  $\text{Est}_j(1, y_j) = y_j$  and  $\text{Est}_j(0, y_j) = \mathbb{1}\{\Pr[S_j = 1] > 0.5\}$  for  $j = 1, 2$  that can be obtained as in (11), which are equivalent to the proofs for [38, Eqs. (27c) and (27d)]. We next have  $I(X; Y_1|S_1) = qH_b(p)$ , which is equivalent to the proof for [38, Eq. (27a)] with  $r = 1$ . Furthermore, we obtain

$$\begin{aligned} & H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_1, Y_2, S_2, X) \\ & \stackrel{(a)}{=} H(S_1|S_2) + H(Y_1|S_1, Y_2, S_2) - H(S_1|S_2) + I(S_1; Y_1, X|S_2) \\ & \stackrel{(b)}{=} P_{S_1 S_2}(1, 0)H(Y_1|S_1 = 1, S_2 = 0) + H(X) + H(Y_1|X, S_2) - H(Y_1, X|S_2, S_1) \\ & \stackrel{(c)}{=} P_{S_1 S_2}(1, 0)H(X) + H(X) + P_X(1)P_{S_2}(0)H(Y_1|X = 1, S_2 = 0) \\ & \quad + P_X(1)P_{S_2}(1)H(Y_1|X = 1, S_2 = 1) - H(X) \\ & \stackrel{(d)}{=} q(1 - \alpha)H_b(p) + p(1 - q\alpha)H_b\left(\frac{q(1 - \alpha)}{(1 - q\alpha)}\right) \end{aligned} \quad (81)$$

where (a) follows since  $S_1 - S_2 - Y_2$  and  $S_1 - (Y_1, S_2, X) - Y_2$  form Markov chains for the considered ISAC channel, (b) follows since if  $S_1 = 0$ , then  $Y_1 = 0$ ; if  $(S_1, S_2) = (1, 1)$ , then

$Y_1 = Y_2 = X$ ; and if  $S_2 = 0$ , then  $Y_2 = 0$ , and because  $X$  is independent of  $S_2$ , (c) follows since  $Y_1 = X$  if  $S_1 = 1$ , because  $X$  is independent of  $(S_1, S_2)$ , since  $Y_1 = 0$  if  $X = 0$ , and because  $(S_1, X)$  determine  $Y_1$ , and (d) follows since  $S_1 = 1$  if  $S_2 = 1$  due to (77) and because  $(S_1, X)$  determine  $Y_1$ . Therefore, we have

$$\begin{aligned} R &\leq \min \left\{ \left( H(Y_1, S_1 | Y_2, S_2) - H(S_1 | Y_1, Y_2, S_2, X) \right), I(X; Y_1 | S_1) \right\} \\ &= \min \left\{ \left( q(1 - \alpha)H_b(p) + p(1 - q\alpha)H_b\left(\frac{q(1 - \alpha)}{1 - q\alpha}\right) \right), qH_b(p) \right\} \end{aligned} \quad (82)$$

■

The securely-transmitted message rate for ISAC scenarios under full secrecy is upper bounded both by  $(H(Y_1, S_1 | Y_2, S_2) - H(S_1 | Y_1, Y_2, S_2, X))$  and  $I(X; Y_1 | S_1)$ , the latter of which is the upper bound for the rate when there is no secrecy constraint [38, Corollary 4]. Thus, secrecy might incur a rate penalty for this example. Nevertheless, ISAC methods achieve significantly better performance than separation-based secure communication and state-sensing methods. One can illustrate this by showing that time sharing between the operation point with the maximum secrecy rate and the point with the minimum distortions results in a region that is strictly smaller than the one identified in Lemma 1; see Figure 2 for the boundary of the secrecy-distortion region  $\mathcal{R}_{\text{POF}}$  for a binary ISAC channel with multiplicative Bernoulli states characterized by parameters  $(q = 0.65, \alpha = 0.21)$ . These analyses are analogous to the comparisons between joint and separation-based secrecy and reliability methods for the secret key agreement problem, as discussed in [39]–[41].

### B. BEC-BSC ISAC Channels with State-Dependent Inputs

We next illustrate an achievable rate region for a noisy ISAC channel. Consider a binary-input ISAC channel with binary channel states such that

$$X \sim \text{Bern}(p), \quad (83)$$

$$\bar{X}_1 = S_1 \cdot X, \quad \bar{X}_2 = S_2 \cdot X, \quad (84)$$

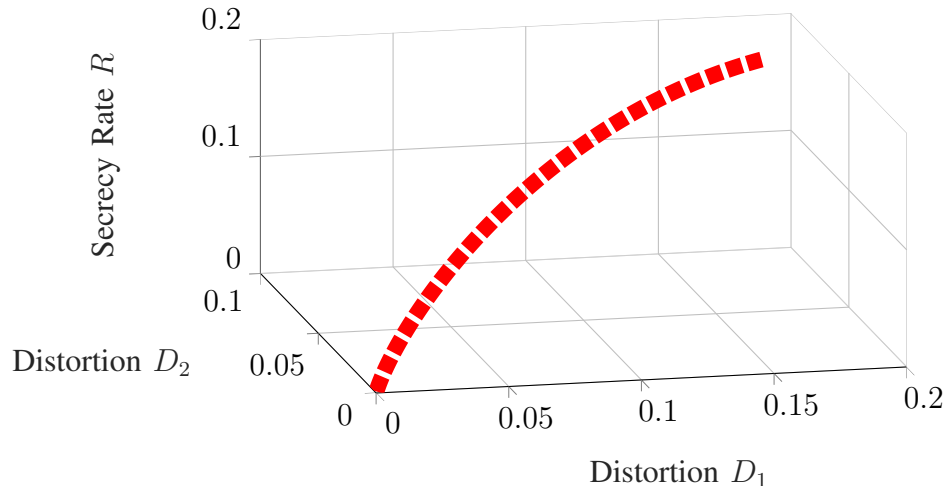


Fig. 2. Boundary of the secrecy-distortion region  $\mathcal{R}_{\text{POF}}$  for a binary ISAC channel with multiplicative Bernoulli states characterized by parameters ( $q = 0.65, \alpha = 0.21$ ) and with Hamming distortion metrics.

$$P_{Y_1|S_1X} = P_{Y_1|\bar{X}_1} \sim \text{BEC}(\gamma), \quad (85)$$

$$P_{Y_2|S_2X} = P_{Y_2|\bar{X}_2} \sim \text{BSC}(\beta) \quad (86)$$

for  $\gamma, \beta \in (0, 1)$ ,  $p \in [0, 1]$ , and the binary states  $(S_1, S_2)$  are again distributed according to the joint probability distribution in (77). We remark that (85) and (86) impose the following Markov chains

$$Y_1 - (S_1, X) - (Y_2, S_2), \quad (87)$$

$$Y_2 - (S_2, X) - (Y_1, S_1). \quad (88)$$

We next establish the set of  $(\gamma, \beta)$  parameters such that the BEC-BSC ISAC channel is more-capable, as defined below.

**Definition 3.** An ISAC channel  $P_{Y_1Y_2|S_1S_2X}$  is *more-capable* if we have for all  $P_X$

$$I(X; Y_1, S_1) \geq I(X; Y_2, S_2). \quad (89)$$

◇

The set of more-capable channels is strictly larger than the set of degraded channels. Furthermore, (89) is equivalent to  $I(X; Y_1|S_1) \geq I(X; Y_2|S_2)$  since  $X$  is independent of  $(S_1, S_2)$  for ISAC models.

**Lemma 2.** *BEC-BSC ISAC channels with state-dependent inputs, as defined in (83)-(86), are more-capable if we have*

$$\gamma \leq 1 - \alpha(1 - H_b(\beta)). \quad (90)$$

We present the proof of Lemma 2 in Appendix.

We next evaluate an inner bound for the strong secrecy-distortion region of more-capable BEC-BSC ISAC channels. For simplicity in the bound below for  $D_2$ , suppose  $\beta \in (0, 0.5]$ . The results for  $\beta \in (0.5, 1)$  follow by symmetry.

**Lemma 3.** *For more-capable BEC-BSC ISAC channels with state-dependent inputs, defined in (83)-(86) for  $\gamma \in (0, 1)$  and  $\beta \in (0, 0.5]$ , satisfying (90), and with Hamming distortion metrics,  $\mathcal{R}_{\text{POF}}$  includes the union over all  $p \in [0, 1]$  of the rate tuples  $(R, D_1, D_2)$  satisfying*

$$R \leq q(H_b(p)(1 - \gamma) + \alpha(H_b(\beta) - H_b(p * \beta))) \quad (91)$$

$$D_1 \geq (1 - p + p\gamma) \cdot \min\{q, (1 - q)\} \quad (92)$$

$$D_2 \geq (1 - p) \cdot \min\{q\alpha, (1 - q\alpha)\} + p \cdot \begin{cases} q\alpha & \text{if } q\alpha \leq \beta \\ (q\alpha * \beta * q\alpha) & \text{if } \beta < q\alpha \leq (1 - \beta) \\ (1 - q\alpha) & \text{if } q\alpha > (1 - \beta). \end{cases} \quad (93)$$

*Proof of Lemma 3:* Consider the inner bound given in Proposition 3 that is valid for all ISAC channels with single secure message and perfect output feedback. Choose  $V = X$  in (63), which is allowed by (64), so we obtain

$$\begin{aligned} R &\leq \min\{([I(X; Y_1|S_1) - I(X; Y_2|S_2)]^+ + H(Y_1|Y_2, S_2, X)), I(X; Y_1|S_1)\} \\ &\stackrel{(a)}{=} \min\{(I(X; Y_1|S_1) - I(X; Y_2|S_2) + H(Y_1|S_2, X)), I(X; Y_1|S_1)\} \end{aligned} \quad (94)$$

where (a) follows by (89) since the BEC-BSC ISAC channel is more-capable and from the Markov chain in (88). Using (109), we obtain

$$I(X; Y_1|S_1) - I(X; Y_2|S_2) = q(H_b(p)(1 - \gamma) + \alpha(H_b(\beta) - H_b(p * \beta))). \quad (95)$$

We remark that the calculation of the term  $H(Y_1|S_2, X)$  in (94) is cumbersome, so we omit it for simplicity since the rate region given in Lemma 3 is an inner bound. We next calculate the achievable distortions.

Choose the first estimator as

$$\text{Est}_1(x, y_1) = \begin{cases} \mathbb{1}\{\Pr[S_1 = 1] > 0.5\} & \text{if } (x, y_1) = (0, 0) \text{ or } (\cdot, \mathbf{e}) \\ y_1 & \text{if } (x, y_1) = (1, 1) \text{ or } (1, 0) \end{cases} \quad (96)$$

which minimizes the probability of error given  $(x, y_1)$ . Thus, by using (8) we obtain

$$\begin{aligned} D_1 &\geq \mathbb{E}[d(S_1, \text{Est}_1(X, Y_1))] \\ &\stackrel{(a)}{=} (P_X(0) + P_{XY_1}(1, \mathbf{e})) \cdot \mathbb{E}[d(S_1, \mathbb{1}\{\Pr[S_1 = 1] > 0.5\})] \\ &\stackrel{(b)}{=} (1 - p + p\gamma) \cdot \left( P_{S_1}(1) \cdot (1 \oplus \mathbb{1}\{\Pr[S_1 = 1] > 0.5\}) + P_{S_1}(0) \cdot (0 \oplus \mathbb{1}\{\Pr[S_1 = 1] > 0.5\}) \right) \\ &= (1 - p + p\gamma) \cdot \min\{q, (1 - q)\} \end{aligned} \quad (97)$$

where (a) follows since  $P_{XY_1}(0, 1) = 0$  and because there is no estimation error in other cases, and (b) follows because we consider a Hamming distortion metric.

Choose the second estimator as

$$\text{Est}_2(x, y_2) = \begin{cases} \mathbb{1}\{\Pr[S_2 = 1] > 0.5\} & \text{if } x = 0 \\ \mathbb{1}\{\Pr[S_2 = 1|Y_2 = y_2, X = x] > 0.5\} & \text{if } x = 1 \end{cases} \quad (98)$$

which minimizes the probability of error given  $(x, y_2)$ . One can show that

$$\mathbb{1}\{\Pr[S_2 = 1|Y_2 = 1, X = 1] > 0.5\} = \mathbb{1}\{q\alpha > \beta\}, \quad (99)$$

$$\mathbb{1}\{\Pr[S_2 = 1|Y_2 = 0, X = 1] > 0.5\} = \mathbb{1}\{q\alpha > (1 - \beta)\}. \quad (100)$$

Thus, by using (8), (99), and (100), we obtain

$$\begin{aligned}
D_2 &\geq \mathbb{E}[d(S_2, \text{Est}_2(X, Y_2))] \\
&= P_X(0) \cdot \mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > 0.5\})] + P_{XY_2}(1, 1) \cdot \mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > \beta\})] \\
&\quad + P_{XY_2}(1, 0) \cdot \mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > (1 - \beta)\})] \\
&\stackrel{(a)}{=} (1 - p) \cdot \min\{q\alpha, (1 - q\alpha)\} + p(q\alpha * \beta) \cdot \mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > \beta\})] \\
&\quad + p(1 - q\alpha * \beta) \cdot \mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > (1 - \beta)\})] \tag{101}
\end{aligned}$$

where (a) follows by applying a similar step to (97)(b). Furthermore, we have

$$\mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > \beta\})] = \begin{cases} q\alpha & \text{if } q\alpha \leq \beta \\ (1 - q\alpha) & \text{if } q\alpha > \beta, \end{cases} \tag{102}$$

$$\mathbb{E}[d(S_2, \mathbf{1}\{q\alpha > (1 - \beta)\})] = \begin{cases} q\alpha & \text{if } q\alpha \leq (1 - \beta) \\ (1 - q\alpha) & \text{if } q\alpha > (1 - \beta). \end{cases} \tag{103}$$

Therefore, since we assume that  $\beta \in (0, 0.5]$ , i.e., we have  $\beta \leq (1 - \beta)$ , using (101)-(103) we have

$$\begin{aligned}
D_2 &\geq (1 - p) \cdot \min\{q\alpha, (1 - q\alpha)\} \\
&\quad + p \cdot \begin{cases} (q\alpha * \beta)q\alpha + (1 - q\alpha * \beta)q\alpha & \text{if } q\alpha \leq \beta \\ (q\alpha * \beta)(1 - q\alpha) + (1 - q\alpha * \beta)q\alpha & \text{if } \beta < q\alpha \leq (1 - \beta) \\ (q\alpha * \beta)(1 - q\alpha) + (1 - q\alpha * \beta)(1 - q\alpha) & \text{if } q\alpha > (1 - \beta) \end{cases} \\
&\tag{104}
\end{aligned}$$

which is equal to (93). ■

## REFERENCES

- [1] O. Günlü, M. R. Bloch, R. F. Schaefer, and A. Yener, "Secure joint communication and sensing," in *Proc. of IEEE Int. Symp. Inf. Theory*, Espoo, Finland, June-July 2022, pp. 844–849.

- [2] 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.
- [3] Z. Wei, F. Liu, C. Masouros, N. Su, and A. P. Petropulu, "Towards multi-functional 6G wireless networks: Integrating sensing, communication and security," July 2021, [Online]. Available: [arxiv.org/abs/2107.07735](https://arxiv.org/abs/2107.07735).
- [4] G. Fettweis *et al.*, "Joint communications & sensing - Common radio-communications and sensor technology," *VDE Positionspapier*, July 2021.
- [5] W. Zhang, S. Vedantam, and U. Mitra, "Joint transmission and state estimation: A constrained channel coding approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7084–7095, Oct. 2011.
- [6] H. Wymeersch *et al.*, "Integration of communication and sensing in 6G: A joint industrial and academic perspective," in *Proc. of IEEE Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Helsinki, Finland, Sep. 2021, pp. 1–7.
- [7] S. Buzzi, C. D'Andrea, and M. Lops, "Using Massive MIMO arrays for joint communication and sensing," in *Proc. of Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, Nov. 2019, pp. 5–9.
- [8] M. Ahmadipour, M. Kobayashi, M. Wigger, and G. Caire, "An information-theoretic approach to joint sensing and communication," *IEEE Trans. Inf. Theory*, May 2022, early access.
- [9] M. Kobayashi, H. Hamad, G. Kramer, and G. Caire, "Joint state sensing and communication over memoryless multiple access channels," in *Proc. of IEEE Int. Symp. Inf. Theory*, Paris, France, July 2019, pp. 270–274.
- [10] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 83–95, Jan. 2021.
- [11] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, "Robust transmit beamforming for secure integrated sensing and communication," July 2022, [Online]. Available: [arxiv.org/abs/2207.13863](https://arxiv.org/abs/2207.13863).
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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, Mar. 2021.
- [16] 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.
- [17] 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.
- [18] 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.

- [19] 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.
- [20] A. Gohari and G. Kramer, "An upper bound for wiretap multi-way channels," Sep. 2020, [Online]. Available: [arxiv.org/abs/2009.14814](https://arxiv.org/abs/2009.14814).
- [21] 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.
- [22] 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.
- [23] 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.
- [24] 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.
- [25] M.-C. Chang, T. Erdogan, S.-Y. Wang, and M. Bloch, "Rate and detection error-exponent tradeoffs of joint communication and sensing," in *Proc. of IEEE Int. Hybrid Symp. Joint Commun. & Sensing*, Seefeld, Austria, Mar. 2022.
- [26] H. Joudeh and F. M. Willems, "Joint communication and binary state detection," *IEEE J. Sel. Areas Inf. Theory*, vol. 3, no. 1, pp. 113–124, Mar. 2022.
- [27] H. Wu and H. Joudeh, "On joint communication and channel discrimination," Feb. 2022.
- [28] Y. Liu, M. Li, A. Liu, J. Lu, R. Du, and T. X. Han, "Generalized modeling and fundamental limits for multiple-access integrated sensing and communication systems," May 2022, [Online]. Available: [arxiv.org/abs/2205.05328](https://arxiv.org/abs/2205.05328).
- [29] M. Bloch, *Lecture Notes in Information-Theoretic Security*. Atlanta, GA: Georgia Inst. Technol., July 2018.
- [30] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 2077–2092, Mar. 2018.
- [31] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.
- [32] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge University Press, 2011.
- [33] O. Günlü, R. F. Schaefer, and H. V. Poor, "Biometric and physical identifiers with correlated noise for controllable private authentication," July 2020, [Online]. Available: [arxiv.org/abs/2001.00847](https://arxiv.org/abs/2001.00847).
- [34] E. Sasoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, July 2013, pp. 1117–1121.
- [35] 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.
- [36] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge University Press, 2011.
- [37] A. Schrijver, *Theory of Linear and Integer Programming*. Chichester, England: John Wiley & Sons, June 1998.



- [38] M. Ahmadipour, M. Wigger, and M. Kobayashi, “Joint sensing and communication over memoryless broadcast channels,” in *Proc. of IEEE Inf. Theory Workshop*, Riva del Garda, Italy, Apr. 2021, pp. 1–5.
- [39] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, “Code constructions for physical unclonable functions and biometric secrecy systems,” *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.
- [40] R. A. Chou and M. R. Bloch, “Separation of reliability and secrecy in rate-limited secret-key generation,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.
- [41] O. Günlü, P. Trifonov, M. Kim, R. F. Schaefer, and V. Sidorenko, “Randomized nested polar subcode constructions for privacy, secrecy, and storage,” in *Proc. of IEEE Int. Symp. Inf. Theory Appl.*, Kapolei, HI, Oct. 2020, pp. 475–479.
- [42] C. Nair, “Capacity regions of two new classes of two-receiver broadcast channels,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4207–4214, Sep. 2010.

## APPENDIX

*Proof of Lemma 2:* We follow steps similar to the proofs of [42, Claims 3 and 4]. Define

$$\begin{aligned} D(p) &= I(X; Y_1 | S_1) - I(X; Y_2 | S_2) \\ &\stackrel{(a)}{=} H_b(p) - H(X|Y_1, S_1) - H(Y_2|S_2) + H(Y_2|S_2, X) \end{aligned} \quad (105)$$

where (a) follows since  $X \sim \text{Bern}(p)$  is independent of  $S_1$ .

First, we have

$$\begin{aligned} H(X|Y_1, S_1) &\stackrel{(a)}{=} H_b(p)(P_{Y_1 S_1}(0, 0) + P_{Y_1}(e)) \\ &= H_b(p)((1 - q)(1 - \gamma) + \gamma) = H_b(p)(1 - q + q\gamma) \end{aligned} \quad (106)$$

where (a) follows since  $H(X|Y_1 = 0, S_1 = 1) = H(X|Y_1 = 1, S_1 = 1) = 0$  and  $P_{Y_1 S_1}(1, 0) = 0$ .

Second, we have

$$\begin{aligned} H(Y_2|S_2) &= P_{S_2}(0)H(Y_2|S_2 = 0) + P_{S_2}(1)H(Y_2|S_2 = 1) \\ &\stackrel{(a)}{=} (1 - q\alpha)H_b(\beta) + q\alpha H_b(p * \beta) \end{aligned} \quad (107)$$

where (a) follows since we obtain

$$P_{Y_2|S_2}(0|1) = P_X(0)P_{Y_2|\bar{X}_2}(0|0) + P_X(1)P_{Y_2|\bar{X}_2}(0|1) = p * (1 - \beta)$$

and because the binary entropy function is symmetric around 0.5.

Third, we have

$$H(Y_2|S_2, X) = H_b(\beta). \quad (108)$$

Therefore, by combining (105)-(108), have

$$D(p) = q(H_b(p)(1 - \gamma) + \alpha(H_b(\beta) - H_b(p * \beta))). \quad (109)$$

We next establish the set of  $(\gamma, \beta)$  parameters such that the BEC-BSC ISAC channel is more-capable by finding the set of parameters such that  $D(p) \geq 0$  for all  $p \in [0, 1]$ .

Since  $D(p)$  given in (109) is symmetric around 0.5, which follows from the symmetry of the binary entropy function around 0.5, we can consider the range  $p \in [0, 0.5]$  rather than  $p \in [0, 1]$ . Similarly, we can consider the range  $\beta \in (0, 0.5]$  due to symmetry. One can show that  $D(0) = 0$ , and  $D(0.5) \geq 0$  if

$$\gamma \leq 1 - \alpha(1 - H_b(\beta)). \quad (110)$$

Moreover, we have

$$\frac{d}{dp}D(p) = q\left(\log\left(\frac{1-p}{p}\right)(1-\gamma) - \alpha\log\left(\frac{1-p*\beta}{p*\beta}\right)(1-2\beta)\right) \quad (111)$$

that is non-negative for all  $p \in [0, 0.5]$  if

$$\gamma \leq 1 - \alpha(1 - 2\beta) \quad (112)$$

which follows because  $\log((1-p)/p)$  is non-negative and  $p * \beta \geq p$  for all  $p \in [0, 0.5]$  and any  $\beta \in (0, 0.5]$ . Thus, if the parameters satisfy (112),  $D(p)$  is non-decreasing and is non-negative for  $p \in [0, 0.5]$  since  $D(0) = 0$ , which proves that the BEC-BSC ISAC channel is more-capable for the parameters that satisfy (112).

Next, we consider the case

$$\gamma > 1 - \alpha(1 - 2\beta). \quad (113)$$

Define

$$c = \frac{1 - \gamma}{\alpha(1 - 2\beta)} \quad (114)$$

such that using (111) we obtain

$$\frac{d}{dp}D(p) \geq 0 \iff \left(\frac{1-p}{p}\right)^c \geq \left(\frac{1-p*\beta}{p*\beta}\right) \iff p*\beta \geq \left(\left(\frac{1-p}{p}\right)^c + 1\right)^{-1} \quad (115)$$

with equality if  $p = 0.5$ . We remark that  $0 < c < 1$  when we consider (113), which does not allow  $\alpha = 0$  or  $\beta = 0.5$  since  $\gamma \in (0, 1)$ . Furthermore, the function

$$\left(\left(\frac{1-p}{p}\right)^c + 1\right)^{-1} \quad (116)$$

is proved in [42, pp. 10] to be concave in  $p$  in the range  $[0, 0.5]$  if  $0 < c < 1$ , which indicates that there can be at most two values of  $p$  that achieves equality in (115). Since equality is achieved when  $p = 0.5$ , the other possible value of  $p$  that achieves equality in (115) must be in the range  $(0, 0.5)$ . Note that we have

$$\lim_{p \rightarrow 0^+} \frac{d}{dp}D(p) = \infty \quad (117)$$

so we can conclude that  $D(p)$  first increases and then decreases in  $p$  in the range  $p \in [0, 0.5]$  for the parameters that satisfy (113). Thus, combining the conditions in (110) and (113), as well as the results for the condition in (112), the proof follows. ■