Secure Joint Communication and Sensing

Onur Günlü[1], Matthieu Bloch[2], Rafael F. Schaefer[1], and Aylin Yener[3]
[1]Chair of Communications Engineering and Security, University of Siegen, {onur.guenlue, rafael.schaefer}@uni-siegen.de
[2]School of Electrical and Computer Engineering, Georgia Institute of Technology, matthieu.bloch@ece.gatech.edu
[3]Department of Electrical and Computer Engineering, The Ohio State University, yener@ece.osu.edu

***Abstract*—This work considers mitigation of information leakage between communication and sensing operations in joint communication and sensing systems. Specifically, a discrete memoryless state-dependent broadcast channel model is studied in which (i) the presence of feedback enables a transmitter to simultaneously achieve reliable communication and channel state estimation; (ii) one of the receivers is treated as an eavesdropper whose state should be estimated but which should remain oblivious to a 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 characteristic of the receiver, e.g., its location. For independent identically distributed (i.i.d.) 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 characterization is also extended to the situation in which the entire transmitted message should be kept secret. The benefits of a joint approach compared to separation-based secure communication and state-sensing methods are illustrated with a binary joint communication and sensing model.**

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 harmonization of communication and sensing [1]. For instance, a 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 [2]. Joint communication and sensing (JCAS) techniques are envisioned more broadly as key enablers for a wide range of applications, including connected vehicles and drones.

Several information-theoretic studies of JCAS have been initiated, drawing on existing results for joint communication and state estimation [3]–[6]. Motivated by the integration of communication and radar for mmWave vehicular applications, [7] 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 JCAS channels and 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 [8] and broadcast channels [9].

The nature of JCAS 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 sensitive information can occur. For example, a target illuminated for sensing its range has the ability to gather potentially sensitive information about the transmitted message [10]. As the sensing performance and secrecy performance are both measured with respect to the signal received at the sensed target, there exists a trade-off between the two [2]. To capture and characterize this trade-off, we extend the JCAS model in [7] 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 (strongly) secret (this is called partial secrecy in [11]). We develop inner and outer bounds for the secrecy-distortion region of this partial-secrecy scenario under a strong secrecy constraint when i.i.d. channel states are causally available at the corresponding receivers. The bounds match when the JCAS channel is physically- or reversely-physically-degraded and the outer bound also applies to the case of noisy generalized feedback. We also extend these characterizations to the case in which the entire transmitted message should be kept secret. The proposed secure JCAS models can be viewed as extensions of the wiretap channel with feedback models [12]–[19]. Our achievability proof leverages the output statistics of random binning (OSRB) method [20]–[22] to obtain strong secrecy. A binary JCAS channel example with multiplicative Bernoulli states illustrates how secure JCAS methods may outperform separation-based secure communication and state-sensing methods.

II. Problem Definition

We consider the secure JCAS 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 JCAS channel with known statistics $P_{Y_1Y_2Z|S_1S_2X}$ and i.i.d. state sequence $(S_1^n, S_2^n) \in \mathcal{S}_1^n \times \mathcal{S}_2^n$

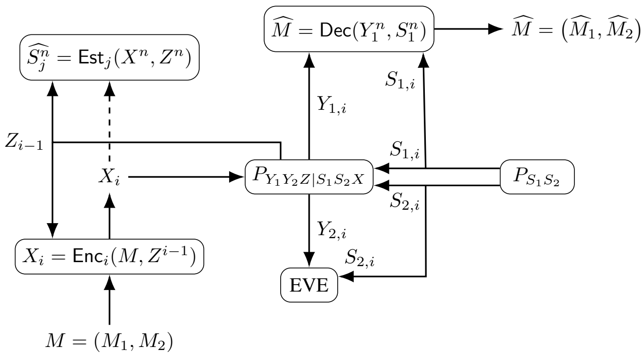

Fig. 1. JCAS model with partial secrecy, where only M_2 should be kept secret from Eve, for $j = 1, 2$ and $i = [1 : n]$. We mainly consider JCAS with perfect output feedback, where $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$.

generated according to a known joint probability distribution $P_{S_1S_2}$. The transmitter calculates the channel inputs X^n as $X_i = \mathsf{Enc}_i(M, Z^{i-1}) \in \mathcal{X}$ for all $i = [1 : n]$, where $\mathsf{Enc}_i(\cdot)$ 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 $S_{1,i}$ for all channel uses $i = [1 : n]$ should reliably decode both M_1 and M_2 by forming the estimate $\widehat{M} = \mathsf{Dec}(Y_1^n, S_1^n)$, where $\mathsf{Dec}(\cdot)$ is a decoding function. The eavesdropper that observes $Y_{2,i} \in \mathcal{Y}_2$ and $S_{2,i}$ should be kept ignorant of M_2. Finally, the transmitter estimates the state sequence (S_1^n, S_2^n) as $\widehat{S_j^n} = \mathsf{Est}_j(X^n, Z^n) \in \widehat{\mathcal{S}_j}^n$ for $j = 1, 2$, where $\mathsf{Est}_j(\cdot,\cdot)$ is an estimation function. Unless specified otherwise, 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.

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

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

Although this is explicitly used in our achievability proofs, some of our converse results hold for generalized feedback. 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* if, for any $\delta > 0$, there exist $n \geq 1$, one encoder, one decoder, and two estimators $\mathsf{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$ such that

$$\frac{1}{n}\log|\mathcal{M}_j| \geq R_j - \delta \qquad \text{for } j=1,2 \quad \text{(rates)} \tag{2}$$
$$\Pr\left[M \neq \widehat{M}\right] \leq \delta \qquad \text{(reliability)} \tag{3}$$
$$I(M_2; Y_2^n|S_2^n) \leq \delta \qquad \text{(strong secrecy)} \tag{4}$$
$$\mathbb{E}\left[d_j(S_j^n, \widehat{S_j^n})\right] \leq D_j + \delta \qquad \text{for } j=1,2 \quad \text{(distortions)} \tag{5}$$

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 with partial secrecy and perfect output feedback.

The use of per-letter distortion metrics $d_j(\cdot,\cdot)$ in conjunction with i.i.d. states simplifies the problem to a rate distortion region characterization [7]–[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 JCAS models with memory leads to conceptually different results, see, e.g., [23].

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.

III. Bounds for JCAS with Partial-Secrecy

We next provide inner and outer bounds for the secrecy-distortion region $\mathcal{R}_{\text{PS,POF}}$; see Section VI for a proof sketch.

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

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

$$R_1 \leq I(U; Y_1|S_1) \tag{6}$$
$$R_2 \leq \min\{R_2', \ (I(V; Y_1|S_1) - R_1)\} \tag{7}$$
$$D_j \geq \mathbb{E}[d_j(S_j, \widehat{S}_j))] \qquad \text{for } j = 1, 2 \tag{8}$$

where

$$P_{UVXY_1Y_2S_1S_2} = P_{U|V} P_{V|X} P_X P_{S_1S_2} P_{Y_1Y_2|S_1S_2X}, \tag{9}$$

$$R_2' = [I(V; Y_1|S_1, U) - I(V; Y_2|S_2, U)]^+ + H(Y_1|Y_2, S_2, S_1, V) \tag{10}$$

and $\mathsf{Est}_j^*(x, y_1, y_2) = \hat{s}_j$ for $j = 1, 2$ are per-letter state estimators such that $d_j(x, y_1, y_2)$ is equal to

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

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

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

and $|\mathcal{V}|$ to

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

Proposition 2 (Outer Bound)**.** *$\mathcal{R}_{\text{PS,POF}}$ is included in the union over all joint distributions P_{VX} of the rate tuples in (8) and*

$$R_1 \leq I(V; Y_1|S_1) \tag{14}$$
$$R_2 \leq \min\Big\{\big(H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_2, S_2, V)\big), \big(I(V; Y_1|S_1) - R_1\big)\Big\} \tag{15}$$

where (9) with constant U follows and we can apply the deterministic per-letter estimators $\mathsf{Est}_j^*(x, y_1, y_2) = \hat{s}_j$ for $j = 1, 2$ by using (11). One can limit the cardinality to

$$|\mathcal{V}| \leq (\min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}+1). \tag{16}$$

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

We next characterize the exact strong secrecy-distortion regions for physically-degraded and reversely-physically-degraded JCAS channels with partial secrecy and perfect output feedback, defined below; see also [9, Definition 2].

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

$$P_{Y_1Y_2|S_1S_2X} = P_{S_1}P_{Y_1|S_1X}P_{Y_2S_2|S_1Y_1}. \tag{17}$$

The channel is *reversely-physically-degraded* if the degradation order is changed and

$$P_{Y_1Y_2|S_1S_2X} = P_{S_2}P_{Y_2|S_2X}P_{Y_1S_1|S_2Y_2}. \tag{18}$$

The physically-degraded corresponds to a situation in which the observations (Y_2^n, S_2^n) of the eavesdropper are degraded versions of observations (Y_1^n, S_1^n) of the legitimate receiver with respect to the channel input X^n.

Theorem 1. *$\mathcal{R}_{\text{PS,POF}}$ for a physically-degraded JCAS problem with partial secrecy and perfect output feedback is the region defined in Proposition 2.*

Proof Sketch: Since the outer bound given in Proposition 2 does not assume any degradedness, the converse proof for Theorem 1 follows from the outer bound. Furthermore, the achievability proof for Theorem 1 follows by modifying the proof of the inner bound in Proposition 1. We next provide a sketch of the modifications for a physically-degraded JCAS.

First, U^n is not used, i.e., U^n is eliminated from the achievability proof. Second, to each $v^n(k)$ we assign four random bin indices $(F_{\text{v}}(k), W_{\text{v}_1}(k), W_{\text{v}_2}(k), L_{\text{v}}(k))$ such that $F_{\text{v}}(k) \in [1 : 2^{n\widetilde{R}_{\text{v}}}]$, $W_{\text{v}_1}(k) \in [1 : 2^{nR_{\text{v}_1}}]$, $W_{\text{v}_2}(k) \in [1 : 2^{nR_{\text{v}_2}}]$, and $L_{\text{v}}(k) \in [1 : 2^{n\overline{R}_{\text{v}}}]$ for all $k = [1 : b]$ independently such that $M_1(k) = W_{\text{v}_1}(k)$ and $M_2(k) = (W_{\text{v}_2}(k), L_{\text{v}}(k))$. As in (53), we impose the reliability constraint

$$\widetilde{R}_{\text{v}} > H(V|Y_1, S_1) \tag{19}$$

as in (55) and (56) we impose the strong secrecy constraints

$$R_{\text{v}_2} + \widetilde{R}_{\text{v}} < H(V|Y_2, S_2) \tag{20}$$

$$\overline{R}_{\text{v}} < H(Y_1|Y_2, S_2, S_1, V) \tag{21}$$

and as in (57) we impose the mutual independence and uniformity constraint

$$R_{\text{v}_1} + R_{\text{v}_2} + \widetilde{R}_{\text{v}} + \overline{R}_{\text{v}} < H(V). \tag{22}$$

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

$$[I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ \overset{(a)}{=} H(V|Y_2, S_2) - H(V|Y_1, S_1) \tag{23}$$

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

$$V - X - (Y_1, S_1) - (Y_2, S_2) \tag{24}$$

form a Markov chain for these JCAS scenarios. Define

$$\begin{aligned} R'_{2,\text{deg}} &= [I(V; Y_1|S_1) - I(V; Y_2|S_2)]^+ + H(Y_1|Y_2, S_2, S_1, V) \\ &\overset{(a)}{=} H(V|Y_2, S_2) - H(V|Y_1, S_1) + H(Y_1|Y_2, S_2, S_1, V) \\ &= H(Y_1, V|Y_2, S_2, S_1) - H(V|Y_1, S_1) + H(S_1|Y_2, S_2) \\ &\quad - H(S_1|Y_2, S_2, V) \\ &= H(V|Y_2, S_2, S_1, Y_1) - H(V|Y_1, S_1) + H(Y_1|Y_2, S_2, S_1) \\ &\quad + H(S_1|Y_2, S_2) - H(S_1|Y_2, S_2, V) \\ &\overset{(b)}{=} H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_2, S_2, V) \end{aligned} \tag{25}$$

where (a) follows by (23) and (b) follows from the Markov chain in (24).

Applying the Fourier-Motzkin elimination [24] to (19)-(22), for any $\epsilon > 0$ one can achieve

$$R_1 = R_{\text{v}_1} = I(V; Y_1, S_1) - 2\epsilon = I(V; Y_1|S_1) - 2\epsilon \tag{26}$$

and for any R_1 that is less than or equal to (26), one can achieve

$$R_2 = R_{\text{v}_2} + \overline{R}_{\text{v}} = \min\{R'_{2,\text{deg}}, (I(V; Y_1|S_1) - R_1)\} - 3\epsilon. \tag{27}$$

Furthermore, the proofs for achievable distortions, sufficiency of given deterministic estimators, inversion of the problem in the source model into the problem in the channel model, and elimination of the public indices follow similarly as in Section VI-A, so we omit them. ■

Lemma 1. *$\mathcal{R}_{\text{PS,POF}}$ for a reversely-physically-degraded JCAS problem with partial secrecy and perfect output feedback is the union over all joint distributions P_{VX} of the rate tuples satisfying (8), (14), and*

$$R_2 \leq \min\big\{H(Y_1|Y_2, S_2, S_1),\ \big(I(V; Y_1|S_1) - R_1\big)\big\} \tag{28}$$

for joint distributions as in (9) but with constant U, and we can apply the deterministic per-letter estimators $\mathsf{Est}_j^*(x, y_1, y_2) = \hat{s}_j$ for $j = 1, 2$ by using (11). One can limit the cardinality to

$$|\mathcal{V}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}. \tag{29}$$

Proof Sketch: The proof follows by showing that the inner and outer bounds in Propositions 1 and 2, respectively, match after elimination of U^n from the proof of achievability, as in the proof for Theorem 1 above. After removal of U, i.e., U is constant, by (7) we have

$$\begin{aligned} R_2 &\overset{(a)}{\leq} \min\big\{H(Y_1|Y_2, S_2, S_1, V),\ \big(I(V; Y_1|S_1) - R_1\big)\big\} \\ &\overset{(b)}{=} \min\big\{H(Y_1|Y_2, S_2, S_1),\ \big(I(V; Y_1|S_1) - R_1\big)\big\} \end{aligned} \tag{30}$$

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

$$V - X - (Y_2, S_2) - (Y_1, S_1) \tag{31}$$

and (b) follows because of the Markov chain

$$V - X - (Y_2, S_2, S_1) - Y_1. \tag{32}$$

Furthermore, by (15) we obtain

$$R_2 \overset{(a)}{\leq} \min\Big\{\big(H(Y_1,S_1|Y_2,S_2,V)-H(S_1|Y_2,S_2,V)\big),\ \big(I(V;Y_1|S_1)-R_1\big)\Big\}$$
$$\overset{(b)}{=} \min\big\{H(Y_1|Y_2,S_2,S_1),\ \big(I(V;Y_1|S_1)-R_1\big)\big\} \qquad (33)$$

where (a) follows from the Markov chain in (31) and (b) follows from the Markov chain in (32). ■

IV. Bounds for JCAS with Single Secure Message

We next give inner and outer bounds for the JCAS problem with perfect output feedback, in which there is a single message $M=M_2$ that should be kept secret from an eavesdropper, i.e., $M_1=\varnothing$ in Fig. 1. For this problem, the definitions of an achievable secrecy-distortion tuple (R,D_1,D_2) and corresponding strong secrecy-distortion region $\mathcal{R}_{\text{POF}}$ follow similarly as in Definition 1 by eliminating (M_1,R_1) and by replacing $(M_2,R_2,\mathcal{R}_{\text{PS,POF}})$ with $(M,R,\mathcal{R}_{\text{POF}})$, respectively.

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

$$R \leq \min\{R_2'',\ I(V;Y_1|S_1)\} \qquad (34)$$

where

$$P_{VXY_1Y_2S_1S_2} = P_{V|X}P_XP_{S_1S_2}P_{Y_1Y_2|S_1S_2X}, \qquad (35)$$

$$R_2'' = [I(V;Y_1|S_1)-I(V;Y_2|S_2)]^+ + H(Y_1|Y_2,S_2,S_1,V) \quad (36)$$

and apply the deterministic per-letter estimators $\mathsf{Est}_j^*(x,y_1,y_2)=\hat{s}_j$ for $j=1,2$ by using (11). One can limit the cardinality as in (16).

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

$$R \leq \min\Big\{\big(H(Y_1,S_1|Y_2,S_2)-H(S_1|Y_2,S_2,X)\big),\ I(X;Y_1|S_1)\Big\} \qquad (37)$$

where we can apply the deterministic per-letter estimators $\mathsf{Est}_j^*(x,y_1,y_2)=\hat{s}_j$ for $j=1,2$ by using (11).

Proof Sketch: The proof of the inner bound in Proposition 3 follows by eliminating U^n in the proof of the inner bound for Proposition 1 such that $R_1=R_{\text{v}_1}=0$ and by imposing (19)-(22) after replacing R_{v_2} with R_{v} since for this case we have $M(k)=(W_{\text{v}}(k),L_{\text{v}}(k))$ for all $k=[1:b]$.

We next prove the outer bound. Assume that for some $\delta_n>0$ and $n\geq 1$, there exist an encoder, decoder, and estimators such that all constraints imposed on the JCAS problem with perfect output feedback are satisfied for some tuple (R,D_1,D_2). We then obtain

$$\begin{aligned}
nR &\overset{(a)}{\leq} I(M;Y_1^n|S_1^n)+n\epsilon_n\\
&\overset{(b)}{\leq} \sum_{i=1}^n H(Y_{1,i}|S_{1,i}) - H(Y_1^n|S_1^n,X^n)+n\epsilon_n\\
&\overset{(c)}{=} \sum_{i=1}^n \big(H(Y_{1,i}|S_{1,i})-H(Y_{1,i}|S_{1,i},X_i)+\epsilon_n\big)\\
&= \sum_{i=1}^n (I(X_i;Y_{1,i}|S_{1,i})+\epsilon_n)
\end{aligned} \qquad (38)$$

where (a) follows because M and S_1^n are independent, and from Fano's inequality and (3) for an $\epsilon_n>0$ such that $\epsilon_n\to 0$ if $\delta_n\to 0$, which is similar to (60) below, (b) follows since $M-(X^n,S_1^n)-Y_1^n$ form a Markov chain, and (c) follows because the JCAS channel is memoryless and state sequence is i.i.d. Furthermore, we also have

$$\begin{aligned}
nR &\overset{(a)}{\leq} I(M;Y_1^n,Y_2^n,S_1^n,S_2^n)+n\epsilon_n\\
&= H(Y_1^n,S_1^n|Y_2^n,S_2^n)+I(Y_2^n,S_2^n;M)\\
&\qquad - H(Y_1^n,S_1^n|Y_2^n,S_2^n,M)+n\epsilon_n\\
&\overset{(b)}{\leq} \sum_{i=1}^n H(Y_{1,i},S_{1,i}|Y_{2,i},S_{2,i})+\delta_n\\
&\qquad - H(S_1^n|Y_2^n,S_2^n,X^n)+n\epsilon_n\\
&\overset{(c)}{=} \sum_{i=1}^n H(Y_{1,i},S_{1,i}|Y_{2,i},S_{2,i})+\delta_n\\
&\qquad - \sum_{i=1}^n H(S_{1,i}|Y_{2,i},S_{2,i},X_i)+n\epsilon_n
\end{aligned} \qquad (39)$$

where (a) follows from Fano's inequality and (3) for an $\epsilon_n>0$ such that $\epsilon_n\to 0$ if $\delta_n\to 0$, (b) follows by (4) and from Remark 1 after replacing M_2 with M for the JCAS problem with perfect output feedback, and because $M-(Y_2^n,S_2^n,X^n)-S_1^n$ form a Markov chain, and (c) follows because the JCAS channel is memoryless and state sequence is i.i.d. Thus, by applying (66) given below and introducing a uniformly-distributed time-sharing random variable, as being applied in the proof of outer bound for Proposition 2, we prove the outer bound for the JCAS problem with perfect output feedback by letting $\delta_n\to 0$. ■

Similar to Section III, we characterize the exact strong secrecy-distortion regions for the JCAS problem with perfect output feedback when the JCAS channel $P_{Y_1Y_2|S_1S_2X}$ is physically-degraded, as in (17), or reversely-physically-degraded, as in (18).

Theorem 2. *$\mathcal{R}_{POF}$ for a physically-degraded JCAS problem with perfect output feedback is the region defined in Proposition 4.*

Proof: Since the outer bound given in Proposition 4 is valid for any JCAS channel, the converse proof for Theorem 2 follows from Proposition 4. Furthermore, the achievability proof for Theorem 2 follows by modifying the proof of the inner bound for 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 $V^n(k)$. ∎

Lemma 2. *$\mathcal{R}_{POF}$ for a reversely-physically-degraded JCAS problem with perfect output feedback is the union over all P_X of the rate tuples in (8) and*

$$R \leq \min\left\{H(Y_1|Y_2, S_2, S_1),\ I(X; Y_1|S_1)\right\} \tag{40}$$

where we can apply the deterministic per-letter estimators $\mathsf{Est}_j^*(x, y_1, y_2) = \hat{s}_j$ for $j = 1, 2$ by using (11).

Proof Sketch: We show that the inner and outer bounds in Propositions 3 and 4, respectively, match after assigning $V^n = X^n$ in the proof of achievability, i.e., we choose $V = X$ that is allowed by (35), such that by (34) we obtain

$$\begin{aligned} R &\overset{(a)}{\leq} \min\left\{H(Y_1|Y_2, S_2, S_1, X),\ I(X; Y_1|S_1)\right\} \\ &\overset{(b)}{=} \min\left\{H(Y_1|Y_2, S_2, S_1),\ I(X; Y_1|S_1)\right\} \end{aligned} \tag{41}$$

where (a) follows since X is independent of (S_1, S_2) and since $H(X|Y_1, S_1) \geq H(X|Y_2, S_2)$ for all reversely-physically-degraded JCAS channels because of the Markov chain in (31) and (b) follows because of the Markov chain in (32). Furthermore, by (37) we have

$$\begin{aligned} R &\overset{(a)}{\leq} \min\Big\{\big(H(Y_1, S_1|Y_2, S_2, X) - H(S_1|Y_2, S_2, X)\big), \\ &\qquad\qquad I(X; Y_1|S_1)\Big\} \\ &\overset{(b)}{=} \min\left\{H(Y_1|Y_2, S_2, S_1),\ I(V; Y_1|S_1)\right\} \end{aligned} \tag{42}$$

where (a) follows from the Markov chain in (31) and (b) follows from the Markov chain in (32). ∎

V. Binary JCAS Channel with Multiplicative Bernoulli States Example

We next consider a JCAS with perfect output feedback example, in which JCAS channel input and output alphabets are binary with multiplicative Bernoulli states, i.e., we have

$$Y_1 = S_1 \cdot X, \qquad\qquad Y_2 = S_2 \cdot X \tag{43}$$

where $P_{S_1S_2}(0,0) = (1-q)$, $P_{S_1S_2}(1,1) = q\alpha$, and $P_{S_1S_2}(1,0) = q(1-\alpha)$ for fixed $q, \alpha \in [0,1]$, so the JCAS channel satisfies (17) [9, Section IV-A].

Define the binary entropy function, for any $c \in [0,1]$, as

$$H_b(c) = -c\log c - (1-c)\log(1-c). \tag{44}$$

Lemma 3. *The strong secrecy-distortion region $\mathcal{R}_{POF}$ for a binary JCAS channel with multiplicative Bernoulli states characterized by parameters (q, α), and with Hamming distortion metrics is the union over all $p = \Pr[X = 1]$ of the rate tuples*

$$R \leq q(1-\alpha)H_b(p) \tag{45}$$

$$D_1 \geq (1-p) \cdot \min\{q, (1-q)\} \tag{46}$$

$$D_2 \geq (1-p) \cdot \min\{q\alpha, (1-q\alpha)\}. \tag{47}$$

Proof Sketch: The proof follows by evaluating the strong secrecy-distortion region $\mathcal{R}_{\text{POF}}$ defined in Theorem 2 since the JCAS channel considered is physically-degraded. Proofs for (46) and (47) follow by choosing $\mathsf{Est}_j^*(1, y_1, y_2) = y_j$ and $\mathsf{Est}_j^*(0, y_1, y_2) = \mathbb{1}\{\Pr[S_j = 1] > 0.5\}$ for $j = 1, 2$ that result from (11), which are equivalent to the proofs for [9, Eqs. (27c) and (27d)]. We next have $I(X; Y_1|S_1) = qH_b(p)$, which is equivalent to the proof for [9, Eq. (27a)] with $r = 1$. Furthermore, we obtain

$$\begin{aligned} &H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_2, S_2, X) \\ &\overset{(a)}{=} H(S_1|S_2) + H(Y_1|S_1, Y_2, S_2) - H(S_1|S_2) \\ &\overset{(b)}{=} P_{S_1S_2}(1,0)H(Y_1|S_1 = 1, S_2 = 0) \\ &\overset{(c)}{=} P_{S_1S_2}(1,0)H(X) = q(1-\alpha)H_b(p) \end{aligned} \tag{48}$$

where (a) follows since $S_1 - S_2 - (Y_2, X)$ form a Markov chain for the considered JCAS channel, (b) follows since if $S_1 = 0$, then $Y_1 = 0$, and if $(S_1, S_2) = (1, 1)$, then $Y_1 = Y_2$, and (c) follows since $Y_1 = X$ that is because of $S_1 = 1$ and since X is independent of (S_1, S_2). Therefore, we have

$$\begin{aligned} R &\leq \min\Big\{\big(H(Y_1, S_1|Y_2, S_2) - H(S_1|Y_2, S_2, X)\big), \\ &\qquad\qquad I(X; Y_1|S_1)\Big\} \\ &= q(1-\alpha)H_b(p) \end{aligned} \tag{49}$$

which follows since $\alpha \leq 1$. ∎

We remark that for the considered example, the rate of the securely transmitted message is upper bounded by $\big(H(Y_1, S_1|Y_2, S_2) – H(S_1|Y_2, S_2, X)\big)$ rather than $I(X; Y_1|S_1)$, the latter of which is the upper bound for the rate for the same example when there is no secrecy constraint [9, Corollary 4]. Thus, the amount of rate loss due to the strong secrecy constraint is $q\alpha H_b(p)$ for this JCAS example. Furthermore, one can show that JCAS methods achieve significantly better performance than separation-based secure communication and state-sensing methods. First, one can show that the maximum secure communication rate in (45) is achieved with $p = 0.5$, whereas the minimum distortions in (46) and (47) are achieved with $p = 1$ that results in zero communication rate. Then, applying time sharing between the tuples achieved by the separation based methods to convexify and enlarge the region, we observe that the secrecy-distortion region that can be achieved by applying the JCAS methods is strictly larger than the region being achieved by the separation based methods. 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 [25]–[27].

VI. Proofs for Propositions 1 and 2

A. Inner Bound

Proof Sketch: We use the OSRB method [21], [22] for the achievability proofs, applying the steps in [28, Section 1.6], see also [29].

Since in the JCAS problem with partial secrecy and perfect output feedback an encoder maps messages into length-n codewords in the channel model, we first define an operationally dual problem to this problem in the source model, as defined in [21] and which is called *Protocol A*. Reliability and secrecy analysis for a proposed random code construction is conducted for Protocol A. We next define a problem in the channel model, called *Protocol B*, that is equivalent to the JCAS problem considered with the addition of a public index. The joint probability distributions in Protocols A and B are shown to be almost equal under given constraints, which allows to invert the random source code proposed for Protocol A to construct a random channel code for Protocol B. The achievability proof by using the OSRB method follows by proving that the public index in Protocols A and B can be fixed ahead of transmissions.

Protocol A (dual problem in the source model): Similar to the dual problem defined in [29] for a wiretap channel, the dual of the JCAS problem with partial secrecy and perfect output feedback is a secret key agreement model, where a source encoder observes $X^n \in \mathcal{X}^n$ and independently and uniformly randomly assigns two random bin indices $M \in \mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ and $F \in \mathcal{F}$ to it. In the dual source model, $M = (M_1, M_2)$ represents a secret key that should be reliably reconstructed at a source decoder that observes $(Y_1^n, S_1^n) \in \mathcal{Y}_1^n \times \mathcal{S}_1^n$ and F to satisfy (3), whereas the eavesdropper observes $(Y_2^n, S_2^n) \in \mathcal{Y}_2^n \times \mathcal{S}_2^n$ and F, which determines the conditions to satisfy the strong secrecy constraint (4). Furthermore, the state sequence estimation at the source encoder by using perfect output feedback should satisfy the distortion constraints (5).

While the strictly causal observation of the i.i.d. state through feedback does not provide opportunities to improve reliability, feedback offers significant opportunities to improve secrecy. Hence, we apply a block Markov coding scheme that consists of $b \geq 2$ transmission blocks, each with n channel uses, to transmit $(b-1)$ independent messages $M(k) = (M_1(k), M_2(k))$. In every block, secret keys are distilled from the states and used to protect messages in the subsequent block. In the following, all n-letter random variables are i.i.d. according to (9) for all $k = [1:b]$, obtained by fixing $P_{U|V}$, $P_{V|X}$, and P_X so that there exist associated per-letter estimators $\mathsf{Est}_j(x, y_1, y_2) = \widehat{S_j}$ for $j = 1, 2$ that satisfy

$$\mathbb{E}[d_j(S_j^n, \mathsf{Est}_j^n(X^n, Y_1^n, Y_2^n))] \leq D_j + \epsilon_n \tag{50}$$

where $\epsilon_n > 0$ such that $\epsilon_n \to 0$ when $n \to \infty$. The block k under consideration is indicated by adding the argument (k) to the variables, e.g., $M(k)$ refers to the message in block k, etc.

For all blocks $k = [1:b]$ we construct codes as follows. To each $u^n(k)$ independently and uniformly assign two random bin indices $(F_{\mathrm{u}}(k), W_{\mathrm{u}}(k))$ such that $F_{\mathrm{u}}(k) \in [1 : 2^{n\widetilde{R}_{\mathrm{u}}}]$ and $W_{\mathrm{u}}(k) \in [1 : 2^{nR_{\mathrm{u}}}]$ for all $k = [1:b]$. Furthermore, to each $v^n(k)$ independently and uniformly assign three random indices $(F_{\mathrm{v}}(k), W_{\mathrm{v}}(k), L_{\mathrm{v}}(k))$ such that $F_{\mathrm{v}}(k) \in [1 : 2^{n\widetilde{R}_{\mathrm{v}}}]$, $W_{\mathrm{v}}(k) \in [1 : 2^{nR_{\mathrm{v}}}]$, and $L_{\mathrm{v}}(k) \in [1 : 2^{n\overline{R}_{\mathrm{v}}}]$ for all $k = [1:b]$. Finally, to each $y_1^n(k-1)$, independently and uniformly assign a random index $L_{\mathrm{y}_1}(k-1) \in [1 : 2^{n\overline{R}_{\mathrm{y}_1}}] = [1 : 2^{n\overline{R}_{\mathrm{v}}}]$. Conceptually, the indices $F(k) = (F_{\mathrm{u}}(k), F_{\mathrm{v}}(k))$ represent the public choice of an independent encoder-decoder pair in block $k \in [1:b]$, while the indices $W(k) = (W_{\mathrm{u}}(k), W_{\mathrm{v}}(k), L_v(k))$ represent the messages that should be reliably reconstructed at the decoder. Only $W_{\mathrm{v}}(k)$ should be directly kept secret from the eavesdropper. $L_{\mathrm{v}}(k)$ represents a non-secure additional message that should be reliably reconstructed at the decoder and can be kept secret by applying a one-time pad as used in the chosen-secret model [30]–[32]. The role of the index $L_{\mathrm{y}_1}(k-1)$, which is known at all legitimate parties thanks to the perfect output feedback, is to provide the required key for the one-time pad in block k. Secure reconstruction of $L_{\mathrm{v}}(k)$ follows by summing it in modulo-$2^{n\overline{R}_{\mathrm{v}}}$ with $L_{\mathrm{y}_1}(k-1)$. Thus, rather than reconstructing $L_{\mathrm{v}}(k)$ directly, the decoder reconstructs the modulo sum $(L_{\mathrm{v}}(k)+L_{\mathrm{y}_1}(k-1))$ by estimating $V^n(k)$ since it then can use its observation $Y_1^n(k-1)$ from the previous transmission block to obtain $L_{\mathrm{v}}(k)$ by applying modulo-$2^{n\overline{R}_{\mathrm{v}}}$ subtraction. If $L_{\mathrm{y}_1}(k-1)$ is uniformly distributed and independent of all random variables in the source model except $Y_1^n(k-1)$, then the modulo sum is also uniformly distributed and independent of $L_{\mathrm{v}}(k)$, which allows to keep $L_{\mathrm{v}}(k)$ secret from the eavesdropper. Furthermore, we assign for all $k = [2:b]$ that

$$M_1(k) = W_{\mathrm{u}}(k), \qquad M_2(k) = (W_{\mathrm{v}}(k), L_{\mathrm{v}}(k)). \tag{51}$$

We next impose conditions on the bin sizes to satisfy all constraints given in Definition 1.

Using a Slepian-Wolf [33] decoder, one can reliably reconstruct $U^n(k)$ from $(Y_1^n(k), S_1^n(k), F_{\mathrm{u}}(k))$ for all $k = [1:b]$ such that the expected value of the error probability taken over the random bin assignments vanishes when $n \to \infty$, if we have [21, Lemma 1]

$$\widetilde{R}_{\mathrm{u}} > H(U|Y_1, S_1). \tag{52}$$

Similarly, one can next reliably reconstruct $V^n(k)$ from $(Y_1^n(k), S_1^n(k), F_{\mathrm{v}}(k), U^n(k))$ for all $k = [1:b]$ if we have

$$\widetilde{R}_{\mathrm{v}} > H(V|Y_1, S_1, U). \tag{53}$$

Thus, (3) is satisfied if (52) and (53) are satisfied and the *backward decoding* is applied, which is a method proposed in [34] that requires to wait until all b block transmissions are complete to decode the blocks in the backward order as $k = b, b-1, \ldots, 2$ such that reliable reconstruction of $L_{\mathrm{v}}(k)$ is possible by using $Y_1^n(k-1)$. Furthermore, the large delay of nb channel uses to apply backward decoding can be reduced by applying a binning step in the channel model or using the *sliding window decoding* [35], as mentioned in [36, pp. 393].

The public index $F_{\mathrm{u}}(k)$ and secret key $W_{\mathrm{u}}(k)$ are almost independent and uniformly distributed for all $k = [1:b]$ if we have [21, Theorem 1]

$$R_{\mathrm{u}} + \widetilde{R}_{\mathrm{u}} < H(U) \tag{54}$$

since then the expected value, which is taken over the random bin assignments, of the variational distance between the joint probability distributions $\text{Unif}[1:2^{nR_{\text{u}}}]\cdot\text{Unif}[1:2^{n\widetilde{R}_{\text{u}}}]$ and $P_{W_{\text{u}}F_{\text{u}}}$ vanishes when $n\rightarrow\infty$. Furthermore, the public index $F_{\text{v}}(k)$ and secret key $W_{\text{v}}(k)$ are almost independent of $(Y_2^n(k),S_2^n(k),U^n(k))$ and uniformly distributed for all $k=[1:b]$ if we have

$$R_{\text{v}}+\widetilde{R}_{\text{v}}<H(V|Y_2,S_2,U). \tag{55}$$

Similarly, the random bin index $L_{\text{y}_1}(k-1)$ is almost independent of $(Y_2^n(k-1),S_2^n(k-1),S_1^n(k-1),V^n(k-1),U^n(k-1))$ and uniformly distributed for all $k=[2:b]$ if we have

$$\overline{R}_{\text{y}_1}=\overline{R}_{\text{v}}$$
$$<H(Y_1|Y_2,S_2,S_1,V,U)\overset{(a)}{=}H(Y_1|Y_2,S_2,S_1,V) \tag{56}$$

where (a) follows because $U-V-(Y_1,Y_2,S_1,S_2)$ form a Markov chain. Thus, (4) is satisfied by applying the one-time padding step above if (55) and (56) are satisfied. Consider next the joint condition that $(F_{\text{u}}(k),W_{\text{u}}(k),F_{\text{v}}(k),W_{\text{v}}(k),L_{\text{v}}(k))$ are almost mutually independent and uniformly distributed for all $k=[1:b]$ if we have

$$R_{\text{u}}+\widetilde{R}_{\text{u}}+R_{\text{v}}+\widetilde{R}_{\text{v}}+\overline{R}_{\text{v}}<H(V,U). \tag{57}$$

Applying the Fourier-Motzkin elimination to (52)-(57), for any $\epsilon>0$ we can achieve

$$R_1=R_{\text{u}}=I(U;Y_1,S_1)-2\epsilon\overset{(a)}{=}I(U;Y_1|S_1)-2\epsilon \tag{58}$$

$$R_2=R_{\text{v}}+\overline{R}_{\text{v}}\overset{(b)}{=}\min\{R_2',(I(V;Y_1|S_1)-R_1)\}-3\epsilon \tag{59}$$

where (a) follows since U and S_1 are independent and (b) follows because (U,V) are mutually independent of (S_1,S_2) and if $H(V|Y_2,S_2,U)\leq H(V|Y_1,S_1,U)$, then W_{v} cannot be securely reconstructed, i.e., we then have $R_{\text{v}}=0$.

We next consider the distortion constraints (5) on channel-state estimations. Since we assume per-letter estimators given in (50), (3) is satisfied by imposing the conditions above on the bin sizes, and all $(u^n(k),v^n(k),x^n(k),y_1^n(k),y_2^n(k),s_1^n(k),s_2^n(k))$ tuples are in the jointly typical set with high probability, by applying the law of total expectation to bounded distortion metrics and from the typical average lemma [36, pp. 26], distortion constraints (5) are satisfied; see also [37]. Furthermore, without loss of generality one can use the deterministic per-letter estimators that result from (11) and the proof follows from the proof of [7, Lemma 2] by replacing $(S,Z,\hat{S},d)$ with $(S_j,(Y_1,Y_2),\widehat{S}_j,d_j)$, respectively, since $\widehat{S_j}(k)-(X(k),Y_1(k),Y_2(k))-S_j(k)$ form a Markov chain for all $j=1,2$ and $k=[1:b]$.

Protocol B (main problem in the channel model with common randomness assistance): In Protocol B, we consider the JCAS problem with partial secrecy and perfect output feedback, and assist the problem with the public index $F(k)$ for all $k=[1:b]$ such that (3)-(5) are satisfied also for Protocol B by choosing R_1 and R_2 as in (58) and (59), respectively. The proof of this result follows mainly by proving that the joint probability distribution obtained in Protocol A is almost preserved in Protocol B, i.e., we prove for $n\rightarrow\infty$ that 1) the limit of the expectation, defined over the random binning operations, of the variational distance between the joint probability distributions obtained in Protocol B and required for the reliability constraint is 0; 2) the limit of the random probability, defined over the random binning operations, that Kullback-Leibler divergence between the joint probability distributions obtained in Protocol B and required for the secrecy constraint is greater than 0 is 0. Since the proof steps are standard and mainly repeat the steps in [21], we omit them; see [29, Section IV] for an extensive proof for a wiretap channel.

Now suppose the public indices $F(k)$ are generated uniformly at random for all $k=[1:b]$ independently. The encoder generates $(U^n(k),V^n(k))$ according to $P_{U^n(k)V^n(k)|X^n(k)F_{\text{u}}(k)F_{\text{v}}(k)}$ obtained from the binning scheme above to compute the bins $W_{\text{u}}(k)$ from $U^n(k)$ and $(W_{\text{v}}(k),L_{\text{v}}(k))$ from $V^n(k)$, respectively, for all $k=[1:b]$. This procedure induces a joint probability distribution that is almost equal to $P_{UVXY_1Y_2S_1S_2}$ fixed above [28, Section 1.6]. We remark that the reliability and secrecy metrics considered above are expectations over all possible realizations $F=f$. Thus, applying the selection lemma [38, Lemma 2.2], these results prove the inner bound in Proposition 1 by choosing an $\epsilon>0$ such that $\epsilon\rightarrow0$ when $n\rightarrow\infty$ and imposing $b\rightarrow\infty$. ■

B. Outer Bound

Proof Sketch: Assume that for some $\delta_n>0$ and $n\geq1$, there exist an encoder, decoder, and estimators such that (3)-(5) are satisfied for some tuple (R_1,R_2,D_1,D_2). Using Fano's inequality and (3), we have

$$H(M|Y_1^n,S_1^n)\overset{(a)}{\leq}H(M|\widehat{M})\leq n\epsilon_n \tag{60}$$

where (a) allows randomized decoding and $\epsilon_n=\delta_n(R_1+R_2)+H_b(\delta_n)/n$ such that $\epsilon_n\rightarrow0$ if $\delta_n\rightarrow0$.

Let $V_i\triangleq(M_1,M_2,Y_1^{i-1},S_1^{i-1})$ 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 $\mathbf{R_1}$: We have

$$nR_1\overset{(a)}{\leq}I(M_1;Y_1^n|S_1^n)+n\epsilon_n$$
$$\leq\sum_{i=1}^n\big(H(Y_{1,i}|S_{1,i})-H(Y_{1,i}|M_1,M_2,Y_1^{i-1},S_1^n)+\epsilon_n\big)$$
$$\overset{(b)}{=}\sum_{i=1}^n\big(H(Y_{1,i}|S_{1,i})-H(Y_{1,i}|M_1,M_2,Y_1^{i-1},S_1^i)+\epsilon_n\big)$$
$$\overset{(c)}{=}\sum_{i=1}^n\big(I(V_i;Y_{1,i}|S_{1,i})+\epsilon_n\big) \tag{61}$$

where (a) follows by (60) and because M_1 and S_1^n are independent, (b) follows since

$$S_{1,i+1}^n-(M_1,M_2,Y_1^{i-1},S_1^i)-Y_{1,i} \tag{62}$$

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

Bound on $(\mathbf{R_1}+\mathbf{R_2})$: Similar to (61), we obtain

$$\begin{aligned} n(R_1+R_2) &\overset{(a)}{\leq} I(M_1,M_2;Y_1^n|S_1^n)+n\epsilon_n \\ &\overset{(b)}{\leq} \sum_{i=1}^{n}\big(H(Y_{1,i}|S_{1,i})-H(Y_{1,i}|M_1,M_2,Y_1^{i-1},S_1^{i})+\epsilon_n\big) \\ &\overset{(c)}{=} \sum_{i=1}^{n}\big(I(V_i;Y_{1,i}|S_{1,i})+\epsilon_n\big) \end{aligned} \tag{63}$$

where (a) follows because (M_1,M_2,S_1^n) are mutually independent and by (60), (b) follows since (62) form a Markov chain, and (c) follows from the definition of V_i.

Bound on $\mathbf{R_2}$: We obtain

$$\begin{aligned} nR_2 &\overset{(a)}{\leq} I(M_2;Y_1^n,Y_2^n,S_1^n,S_2^n)+n\epsilon_n \\ &\leq H(Y_1^n,S_1^n|Y_2^n,S_2^n)+H(Y_2^n,S_2^n) \\ &\quad -H(Y_2^n,S_2^n|M_2)-H(Y_1^n,S_1^n|Y_2^n,S_2^n,M_1,M_2)+n\epsilon_n \\ &= H(Y_1^n,S_1^n|Y_2^n,S_2^n)+I(Y_2^n,S_2^n;M_2) \\ &\quad -H(Y_1^n,S_1^n|Y_2^n,S_2^n,M_1,M_2)+n\epsilon_n \\ &\overset{(b)}{\leq} \sum_{i=1}^{n}H(Y_{1,i},S_{1,i}|Y_{2,i},S_{2,i})+\delta_n+n\epsilon_n \\ &\quad -\sum_{i=1}^{n}H(S_{1,i}|Y_{2,i},S_{2,i},M_1,M_2,Y_1^{i-1},S_1^{i-1}) \\ &\overset{(c)}{\leq} \sum_{i=1}^{n}H(Y_{1,i},S_{1,i}|Y_{2,i},S_{2,i})+\delta_n+n\epsilon_n \\ &\quad -\sum_{i=1}^{n}H(S_{1,i}|Y_{2,i},S_{2,i},V_i) \end{aligned} \tag{64}$$

where (a) follows by (60), (b) follows by (4) and from Remark 1, and because

$$(Y_2^{n\setminus i},S_2^{n\setminus i})-(Y_{2,i},S_{2,i},M_1,M_2,Y_1^{i-1},S_1^{i-1})-S_{1,i} \tag{65}$$

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

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

$$(D_j+\delta_n) \overset{(a)}{\geq} \mathbb{E}\big[d_j(S_j^n,\widehat{S_j^n})\big]=\frac{1}{n}\mathbb{E}\big[d_j(S_{j,i},\widehat{S_{j,i}})\big] \tag{66}$$

where (a) follows by (5), which is achieved by using the deterministic per-letter estimators that result from (11).

Introduce a uniformly distributed time-sharing random variable $Q\sim\text{Unif}[1:n]$ that is independent of other random variables, and define $Y_1=Y_{1,Q}$, $S_1=S_{1,Q}$, $Y_2=Y_{2,Q}$, $S_2=S_{2,Q}$, 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 $\delta_n\to 0$.

Cardinality Bounds: We use the support lemma [39, Lemma 15.4] to prove the cardinality bound, which is a standard procedure, so we omit the proof. ■

Acknowledgment

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 Grant CCF 1955401.

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] 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.

[3] 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.

[4] H. W. et al., "Integration of communication and sensing in 6G: A joint industrial and academic perspective," in *IEEE Annu. Int. Symp. Pers., Indoor Mobile Radio Commun.*, Helsinki, Finland, Sep. 2021, pp. 1–7.

[5] S. Buzzi, C. D'Andrea, and M. Lops, "Using Massive MIMO arrays for joint communication and sensing," in *Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, Nov. 2019, pp. 5–9.

[6] G. Fettweis *et al.*, "Joint communications & sensing - Common radio-communications and sensor technology," *VDE Positionspapier*, July 2021.

[7] M. Kobayashi, G. Caire, and G. Kramer, "Joint state sensing and communication: Optimal tradeoff for a memoryless case," in *IEEE Int. Symp. Inf. Theory*, Vail, CO, June 2018, pp. 111–115.

[8] M. Kobayashi, H. Hamad, G. Kramer, and G. Caire, "Joint state sensing and communication over memoryless multiple access channels," in *IEEE Int. Symp. Inf. Theory*, Paris, France, July 2019, pp. 270–274.

[9] M. Ahmadipour, M. Wigger, and M. Kobayashi, "Joint sensing and communication over memoryless broadcast channels," in *IEEE Inf. Theory Workshop*, Riva del Garda, Italy, Apr. 2021, pp. 1–5.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] A. Gohari and G. Kramer, "An upper bound for wiretap multi-way channels," Sep. 2020, [Online]. Available: arxiv.org/abs/2009.14814.

[20] 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.

[21] 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.

[22] 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.

[23] M.-C. Chang, T. Erdogan, S.-Y. Wang, and M. Bloch, "Rate and detection error-exponent tradeoffs of joint communication and sensing," in *IEEE Int. Hybrid Symp. Joint Commun. & Sensing*, Seefeld, Austria, Mar. 2022, to appear.

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

[25] 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.

[26] 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.

[27] O. Günlü, P. Trifonov, M. Kim, R. F. Schaefer, and V. Sidorenko, "Randomized nested polar subcode constructions for privacy, secrecy, and storage," in *IEEE Int. Symp. Inf. Theory Appl.*, Kapolei, HI, Oct. 2020, pp. 475–479.

[28] M. Bloch, *Lecture Notes in Information-Theoretic Security*. Atlanta, GA: Georgia Inst. Technol., July 2018.

[29] 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.

[30] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, "Reliable secret-key binding for physical unclonable functions with transform coding," in *IEEE Global Conf. Sign. Inf. Process.*, Washington, DC, Dec. 2016, pp. 986–991.

[31] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[32] O. Günlü, "Key agreement with physical unclonable functions and biometric identifiers," Ph.D. dissertation, TU Munich, Germany, Nov. 2018, published by Dr.-Hut Verlag in Feb. 2019.

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

[34] F. Willems and E. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 313–327, May 1985.

[35] A. Carleial, "Multiple-access channels with different generalized feedback signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 841–850, Nov. 1982.

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

[37] 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.

[38] M. Bloch and J. Barros, *Physical-layer Security*. Cambridge, U.K.: Cambridge University Press, 2011.

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