Abstract—We study the information-theoretic limits of joint communication and sensing when the sensing task is modeled as the estimation of a discrete channel state fixed during the transmission of an entire codeword. This setting captures scenarios in which the time scale over which sensing happens is significantly slower than the time scale over which symbol transmission occurs. The tradeoff between communication and sensing then takes the form of a tradeoff region between the rate of reliable communication and the state detection-error exponent. We investigate such tradeoffs for both mono-static and bi-static scenarios, in which the sensing task is performed at the transmitter or receiver, respectively. In the mono-static case, we develop an exact characterization of the tradeoff in open-loop, when the sensing is not used to assist the communication. We also show the strict improvement brought by a closed-loop operation, in which the sensing informs the communication. In the bi-static case, we develop an achievable tradeoff region that highlights the fundamentally different nature of the bi-static scenario. Specifically, the rate of communication plays a key role in the characterization of the tradeoff and we show how joint strategies, which simultaneously estimate message and state, outperform successive strategies, which only estimate the state after decoding the transmitted message.

Index Terms—Joint communication and sensing, integrated sensing and communication, multiple hypothesis testing, error exponent, state estimation.

I. INTRODUCTION

A common feature envisioned for the next generation of mobile networks is the convergence of communication and sensing [2], [3] (also known as integrated communication and sensing), motivated in part by the need to offer detection and localization capabilities to inter-connected devices interacting with the real world (robots, UAVs, etc.). This convergence is also enabled by the shift of communication frequencies towards the mmWave part of the spectrum, which allows a single Radio-Frequency (RF) hardware to perform both communication and sensing. While joint communication and sensing has already attracted interest in the context of joint communication and radar [4], [5], [6], theoretical, algorithmic, and hardware-related challenges remain and must be addressed to assess the true potential of joint communication and sensing [3], [7].

The objective of the present work is to further the theoretical understanding of the information-theoretic limits of joint communication and sensing, and specifically to better understand the tradeoffs incurred by a joint operation. While information-theoretic models often abstract fine channel modeling aspects, they provide valuable insights to identify the regimes in which tradeoffs exist and to quantify their severity. In particular, information-theoretic limits of joint communication and sensing are naturally approached from the perspective of joint channel transmission and channel state estimation, where the state simultaneously represents the quantity of interest for sensing and affects the communication. Early works [8], [9], [10] have considered state-dependent channel models with independent and identically distributed (i.i.d.) channel states, in which the encoder attempts to simultaneously communicate and facilitate the estimation of the state at the receiver, and have leveraged rate-distortion theory to characterize the optimal tradeoff between communication rate and state reconstruction accuracy. Recently, [11], [12] have revisited the model of [10] by shifting the task of estimating the state from the receiver to the transmitter using generalized feedback, a situation more in line with the scenarios envisioned in the context of joint communication and sensing, and characterized again the optimal tradeoff between rate and average state distortion. Extensions to multiple-access channels [13] and broadcast channels [12], [14] have been investigated, as well, although exact characterizations of the tradeoff remain elusive. Recent works have also considered secure joint communication and sensing to quantify and investigate the intrinsic information leakage associated to a joint operation [15], [16], [17].

A common feature of [10], [11], [12], [13], [14], [17] is that the i.i.d. nature of the channel state precludes any prediction. Consequently, state detection and estimation strategies are open-loop and the tradeoff between communication and sensing reduces to a resource allocation problem, in which the

Manuscript received 10 October 2022; revised 15 February 2023; accepted 20 April 2023. Date of publication 12 May 2023; date of current version 9 August 2023. This work was supported by the National Science Foundation (NSF) under Grant 1955401 and Grant 2148400 as part of the Resilient and Intelligent NextG Systems (RINGS) Program. Parts of the results have been presented at the 2022 IEEE International Symposium on Joint Communications and Sensing [DOI: 10.1109/JCSS4837.2022.9743498].

The authors are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: mchang301@gatech.edu; shiyuan.wang@gatech.edu; etuna3@gatech.edu; matthieu.bloch@ece.gatech.edu).

Digital Object Identifier 10.1109/JSAIT.2023.3275877
choice of a channel input distribution dictates the tradeoff.\footnote{The situation is more nuanced when introducing secrecy constraints as in \cite{kumar2015}; since feedback is known to improve secrecy.} Furthermore, the i.i.d. model is not well-suited to applications in which the physical phenomena sensed, such as the presence or absence of an obstacle that would disrupt line-of-sight communication, evolve on a time scale that is much slower than the time scale at which communication symbols are transmitted. To address such applications, one may instead adopt a model in which the channel state remains constant over the block-length used for communication. Except in rare cases, estimating the channel state is then always possible so that the tradeoff between communication and sensing appears between the rate of communication and the accuracy of the state estimation. For the case of uncountably infinite channel states parameterized by continuous variables, accuracy can be captured by the Cramer-Rao bound \cite{cramer1946}. For the case of finitely many channel states, accuracy may be captured by the asymptotic state detection error exponent, as studied thereafter and already reported in our preliminary results \cite{wu2021} concurrently with \cite{wu2020, wolniansky1988}.

Two kinds of joint communication and sensing models are considered in this paper, namely, mono-static and bi-static models, where we borrow these terminologies from mono-static and bi-static radars. In both models, there is a transmitter-receiver pair attempting to convey messages without exact knowledge of the channel state. The difference between these two models is that sensing is performed at the transmitter in the mono-static model and at the receiver in the bi-static model. Since the transmitter always knows the transmitter-receiver pair attempting to convey messages with fixed channel states. Accordingly, our approach draws on the rate/detection-error exponent for both mono-static and bi-static models \cite{wu2021}.

In contrast, the receiver in the bi-static model needs to determine the state follows the decoding of the channel code. We further illustrate the results with two kinds of joint communication and sensing models \cite{wu2022, wolniansky1988}.

The remaining of the paper is organized as follows. We introduce the mono-static and bi-static models for joint communication and sensing in Section III. We present our main results in Section IV, along with numerical examples illustrating the joint communication and sensing tradeoffs. We relegate all proofs to Section V to streamline the presentation.

II. NOTATION

For any set $\Omega$, the indicator function is defined as $1(\omega \in \Omega) = 1$ if $\omega \in \Omega$ and 0 otherwise. For any discrete set $X$, $\mathcal{P}_X$ is the set of all probability distributions on $X$. For any $n \in \mathbb{N}$, a sequence of length $n$ is implicitly denoted $x = (x_1, \ldots, x_n) \in X^n$, while $x_i = (x_1, \ldots, x_i) \in X^i$ denotes a sequence of length $i$, and $x_i^j = (x_i, \ldots, x_j)$ is a subsequence of $x$. For $x \in X^n$, $\hat{x}$ denotes the type of $x$, i.e., $\hat{x}(a) = \frac{1}{n} \sum_{i=1}^n 1[x_i = a]$. For any type $\mathcal{T}_n$, $\mathcal{T}_n^a$ is the corresponding type class, i.e., the set of all sequences $x \in X^n$ such that $\hat{x}(a) > 0$ and $a \in \mathcal{T}_n$. Let $\mathcal{P}_X^n$ be the set of all conditional types for length $n$ sequences $x \in X^n$. Let $\mathcal{P}_{X|Y}$ be the set of all conditional probability distributions of $Y$ given $X \in X$. Given a sequence $x \in X^n$ and $y \in Y^n$, we define $\hat{P}_{X|Y}$ as the empirical conditional type, i.e., $\hat{P}_{X|Y}(b|a) = \sum_{i=1}^n 1[x_i = a, y_i = b]/\sum_{j=1}^n 1[x_i = a]$ for all $a \in X$ such that $\hat{x}(a) > 0$ and $b \in Y$. Let $\mathcal{P}_{X|Y}^n$ be the set of all conditional types for length $n$ sequences $x \in X^n$ and $y \in Y^n$. For any conditional type $P_{X|Y}$, we define $\mathcal{T}_{X}(P_{Y|X})$ as the conditional type class of $P_{Y|X}$, i.e., the set of sequences $y \in Y^n$ such that $P_{X|Y}(a|y) = P_{X|Y}(a|b)$. Let $\mathcal{P}_{X|Y}$ be the entropy of $X \sim P_X$. If $W_{Y|X}$ is a conditional distribution on $Y \sim P_Y$ given $X \sim P_X$, we let $\mathbb{E}(P_{X|Y}) \triangleq \sum_{a \in X} P_X(x) \log P_X(x)$ be the entropy of $X \sim P_X$. If $W_{Y|X}$ is a conditional distribution on $Y \sim P_Y$ given $X \sim P_X$, we let $\mathbb{E}(P_{Y|X}) \triangleq \sum_{a \in X} P_X(x) \log P_X(x)$ be the conditional entropy of $W_{Y|X}$ given an input distribution $P_X$ and $\mathbb{E}(P_X, W_{Y|X}) \triangleq \mathbb{E}(W_{Y|X} \circ P_X) - \mathbb{E}(W_{Y|X}P_X)$ is the mutual information between $X$ and $Y$, where $X \sim P_X$ and $Y \sim P_Y \circ W_{Y|X} \triangleq \sum_X P_X(x) W_{Y|X}(x|x)$. The relative entropy between $P_{X|Y}$ and $P_{Y|X}$ given an input distribution $P_X$ is $\mathbb{D}(P_{Y|X} \parallel P_{X|Y}) \triangleq \mathbb{E}_{P_X}(P_{Y|X} P_{X|Y}) \triangleq \mathbb{E}_{P_X}(P_{Y|X} P_{X|Y})$. Throughout this paper, $\log$ is with respect to (w.r.t.) base $e$, and therefore all the information quantities should be understood in nats. Moreover, for $a, b \in \mathbb{R}$ such that $|a| \leq |b|$, we define $[a; b] \triangleq [a; a + 1, \ldots, |b| - 1, |b|];$ otherwise $[a; b] \triangleq 0$. In addition, for any $x \in \mathbb{R}$, we let $|x|^+ = \max(x, 0)$.

III. JOINT COMMUNICATION AND SENSING MODELS

A. Mono-Static Model

The mono-static joint communication and sensing model is illustrated in Fig. 1, in which a transmitter attempts to communicate with a receiver over a state-dependent Discrete Memoryless Channel (DMC), also known as a compound channel, while simultaneously probing the channel state in a strictly causal manner through a sensing channel. Specifically, the transmitter encodes a uniformly distributed message $W \in [1; M]$ into a length $n$ codeword $X^n$, of which symbols are transmitted over a DMC with transition probability $W_{Y|X}$. The concurrent works \cite{wu2020, wolniansky1988} developed characterizations similar to ours in more restricted settings; the results therein are subsumed by Theorem 1 of the present document and \cite[Th. 1]{wu2021}.
The transmission and takes value in a finite set \( W \). Channels assume in this paper that the Chernoff information between past observations obtained from the output \( Z \) of the DMC, allowing it to adapt its transmission in an online fashion. We assume in this paper that the Chernoff information between channels \( W_{Z|X,s} \) and \( W_{Z|X,s'} \) is non-zero for all \( s \neq s' \), i.e.,

\[
\max_{P_X} \max_{\ell \in [0,1]} \sum_x P_X(x) \times \log \left( \sum_z W_{Z|X,s}(z|x)^{\ell} W_{Z|X,s'}(z|x)^{1-\ell} \right) > 0.
\]

Formally, the encoder consists of a set of functions

\[
f_i^{(m)} : [1; M] \times Z^{i-1} \rightarrow X' : (w, z^{i-1}) \mapsto x_i \triangleq f_i^{(m)}(w, z^{i-1})
\]

defined for every \( i \in [1; n] \), while the state estimator is a function

\[
g^{(m)} : X^n \times Z^n \rightarrow S : (x^n, z^n) \mapsto \hat{s}.
\]

The message decoder is a function

\[
h^{(m)} : Y^n \rightarrow [1; M] : y^n \mapsto \hat{w}.
\]

A code \( C^{(m)} \) then consists of the tuple \( (f_i^{(m)})_{i \in [1; n]}, g^{(m)}, h^{(m)} \), as well as the implicitly defined associated message set \( [1; M] \).

### B. Bi-Static Model

As illustrated in Fig. 2, the bi-static joint communication and sensing model differs from the mono-static one in that the receiver should simultaneously sense the state and decode the message. Specifically, the transmitter encodes a uniformly distributed message \( W \in [1; M] \) into a length \( n \) codeword \( X^n \), of which symbols are transmitted over a DMC with transition probability \( W_{Y|X} \). We again assume that the a priori unknown state \( S \) is fixed during the whole duration of the transmission and takes value in a finite set \( S \). The encoder is then defined as

\[
f^{(b)} : [1; M] \rightarrow X^n : w \mapsto x_w,
\]

while the decoder and the state estimator are the functions

\[
g^{(b)} : Y^n \rightarrow S : y^n \mapsto \hat{s},
\]

and

\[
h^{(b)} : Y^n \rightarrow \{1; M\} : y^n \mapsto \hat{w}.
\]

The code \( C^{(b)} \) in the bi-static model then consists of the tuple \( (f^{(b)}, g^{(b)}, h^{(b)}) \), as well as the message set \( [1; M] \).

**Remark 1:** A key difference between the mono-static model and the bi-static model is that the former reduces the coupling of performance between communication and sensing to the type of the transmitted codewords. Specifically, the mono-static model endows the state estimator with full knowledge of the transmitted codeword, so that correct decoding is irrelevant to the state detection performance. In contrast, the bi-static model requires the receiver to perform a joint estimation of the codeword and of the state.

**Remark 2:** The model of Fig. 1 differs from the ones in [10], [12], in which the state is i.i.d. and changing from symbol to symbol. Our model captures a scenario in which the coherence time of the state is much longer than the duration of a transmission. Since the state does not change during the transmission, the transmitter can gradually obtain an accurate estimation about the state and is able to adapt the transmission scheme according to the estimated channel state. As a result our model also captures the ability to adapt to the channel state in an online fashion, while the models in [10], [12] only allow for an offline adaptation based on a target rate/distortion pair. Neither model supersedes the other and both capture scenarios that could be relevant to next generation communication networks.

### C. Performance Evaluation Metrics

The performance of the system is measured in terms of the asymptotic rate of reliable communication and asymptotic detection-error exponent. Formally, we define the communication-error probability and the detection-error probability for both mono-static and bi-static cases as follows

- **Mono-static case:**

  \[
P_c^{(n)} \triangleq \max_{s \in S} \max_{w \in [1; M]} \mathbb{P}(h^{(m)}(Y^n) \neq w \mid W = w, S = s),
\]

  \[
P_d^{(n)} \triangleq \max_{s \in S} \max_{w \in [1; M]} \mathbb{P}(g^{(m)}(X^n, Z^n) \neq s \mid W = w, S = s).
\]

- **Bi-static case:**

  \[
P_c^{(n)} \triangleq \max_{s \in S} \max_{w \in [1; M]} \mathbb{P}(h^{(b)}(Y^n) \neq w \mid W = w, S = s),
\]

  \[
P_d^{(n)} \triangleq \max_{s \in S} \max_{w \in [1; M]} \mathbb{P}(g^{(b)}(Y^n) \neq s \mid W = w, S = s).
\]

The rate and the detection-error exponent for both mono-static and bi-static models are

\[
R^{(n)} \triangleq \frac{1}{n} \log M \quad \text{and} \quad E_d^{(n)} \triangleq -\frac{1}{n} \log P_d^{(n)},
\]

respectively.

**Definition 1 (Achievability):** A rate/detection-error exponent \( (R, E) \) is achievable in the mono-static (bi-static) joint communication model if for any \( s \in S \) and any \( \epsilon > 0 \), there
exist a sufficiently large \( n \) and a code \( C^{(m)} (C^{(b)}) \) of length \( n \) such that

\[
P^{(n)}_c \leq \epsilon, \tag{1}
E^{(n)}_d \geq E - \epsilon, \tag{2}
R^{(n)} \geq R - \epsilon. \tag{3}
\]

When the encoder does not perform any online adaptation so that \( f^{(m)} : [1; M] \mapsto \mathcal{X} \) is independent of the observation \( Z^{n-1} \), the scheme is called open-loop. On the other hand, if the encoder utilizes feedback information, the scheme is called closed-loop. Our objective is to characterize the set of all achievable rate/detection-error exponent pairs by open-loop strategies in both mono-static and bi-static models as well as the set of all achievable rate/detection-error exponent pairs by closed-loop strategies in the mono-static model.

**Definition 2:** We define \( C^{(m)}_{\text{open}} \) and \( C^{(b)} \) as the closure of all achievable rate/detection-error exponent pairs by open strategies in the mono-static and bi-static model, respectively. Similarly, we define \( C^{(m)}_{\text{close}} \) as the closure of all achievable rate/detection-error exponent pairs by closed-loop strategies in the mono-static model.

**IV. MAIN RESULTS**

**A. Mono-Static Model**

We first restrict ourselves to open-loop schemes, which provide a baseline for assessing the usefulness of adaptation. For simplicity, we denote in this case the encoder that maps a message \( w \) to a codeword of \( n \) symbols by \( f^{(m)} : [1; M] \mapsto \mathcal{X}^n \).

The following theorem provides an exact characterization of \( C^{(m)}_{\text{open}} \).

**Theorem 1:** The closure of all achievable joint communication and sensing rate/detection-error exponent pairs for mono-static open-loop schemes is

\[
C^{(m)}_{\text{open}} = \bigcup_{P_X \in \mathcal{X}} \left\{ \left( R, E \right) \in \mathbb{R}^2_+ : R \leq \min_{s \in \mathbb{S}} \mathbb{I}(P_X, W_{Y|X,s}) \right\}
\]

where

\[
\phi(P_X) = \min_{s \neq s'} \max_{s} \sum_{x} P_X(x) \times \log \left( \sum_{x} W_{Z|X,s}(z|x)^{1/2} W_{Z|X,s'}(z|x)^{1/2} \right).
\]

**Proof:** See Sections V-A and V-B.

A couple of comments are in order. First, since open-loop schemes do not exploit the information about the state contained in past noisy observations of the state, achievable rates are necessarily upper bounded by the compound channel capacity \( \max_{P_X} \min_{s \in \mathbb{S}} \mathbb{I}(P_X, W_{Y|X,s}) \). This is a weakness of all open-loop schemes. Second, because of the open-loop nature of the coding schemes, the interplay between communication and sensing is captured by the choice of a distribution \( P_X \) that governs the empirical statistics of the codewords and is set offline. This is similar to what is obtained in other information-theoretic approaches based on rate-distortion [10], [12].

The results in [19] are also special cases of Theorem 1. In [19], the authors consider a mono-static joint communication and sensing model in which \( W_{YZ|X,s} = W_{Y|X} W_{Z|X,s} \), i.e., the communication channel is irrelevant to the state. One of the channel models in [19] is a binary setting in which \( X = Z = S = \{0, 1\} \) and \( W_{YZ|X,s} = W_{Z|X,s} \), i.e., at each time \( t \) the state-estimator obtains \( Z_t = X_t \cdot S_t \oplus N_t \), where \( \oplus \) denotes the modulo-2 sum and \( N_t \sim \text{Ber}(q) \) for some \( 0 < q < 1 \). By specializing Theorem 1, one recovers [19, Th. 1] as follows.

**Corollary 1:** Let \( X = Y = Z = S = \{0, 1\} \). When the mono-static joint communication model satisfies \( W_{YZ|X,s} = W_{Y|X} W_{Z|X,s} \), where \( W_{Y|X} \) and \( W_{Z|X,s} \) are binary symmetric channels with cross over probability \( p \) and \( q \), respectively, then

\[
C^{(m)}_{\text{open}} = \bigcup_{a \in \{0, 1\}} \left\{ \left( R, E \right) \in \mathbb{R}^2_+ : R \leq \mathbb{H}(\text{Ber}(a * p)) - \mathbb{H}(\text{Ber}(p)) \right\}
\]

where \( a * p = \alpha(1 - p) + (1 - \alpha) * p \).

**Proof:** Since, \( W_{YZ|X,s} = W_{Y|X} W_{Z|X,s} \), the achievable rate is irrelevant to the state, and for each \( P_X \sim \text{Ber}(\alpha) \) we have

\[
\min_{s \in \mathbb{S}} \mathbb{I}(P_X, W_{Y|X,s}) = \mathbb{H}(P_X \circ W_{Y|X}) - \mathbb{H}(W_{Y|X}|P_X)
\]

\[
= \mathbb{H}(\text{Ber}(\alpha * p)) - \mathbb{H}(\text{Ber}(p)).
\]

Moreover, for such \( P_X, \phi(P_X) \) can be calculated as follows.

\[
\phi(P_X) = \min_{s \neq s'} \max_{s} \sum_{x} P_X(x) \times \log \left( \sum_{z} W_{Z|X,s}(z|x)^{1/2} W_{Z|X,s'}(z|x)^{1/2} \right)
\]

\[
= \max_{\ell \in \{0, 1\}} -P_X(1) \log\left(q^{1/2}(1 - q)^{1/2} + (1 - q)^{1/2}q^{1/2}\right)
\]

\[
= a \mathbb{D}(\text{Ber}(0.5)||\text{Ber}(q)),
\]

where (7) follows from the fact that \( \ell = 1/2 \) maximizes (6). The corollary follows by taking the union over all \( P_X \).

**Remark 3:** Note that in the setting considered in Corollary 1, transmitting \( X = 0 \) does not help the performance of the state-estimation, and the detection-error exponent is a monotonically increasing function of the weight of the codeword.

We also observe that there is no tradeoff between maximizing the communication capacity and the detection-error exponent in some cases.

**Corollary 2:** If there exists \( x_0 \in \mathcal{X} \) such that for all \( x \in \mathcal{X} \), there exists a permutation \( x_0 \in \mathcal{X} \) such that for every \( s \in S \)

\[
W_{Z|X,s}(z|x) = W_{Z|X,s}(\sigma_x(z)|x_0),
\]

then

\[
C^{(m)}_{\text{open}} = \bigcup_{(R, E) \in \mathbb{R}^2_+} \left\{ (R, E) \in \mathbb{R}^2_+ : R \leq \min_{s \in \mathbb{S}} \mathbb{I}(P_X, W_{Y|X,s}) \right\}
\]

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
where $\phi(\cdot)$ is defined in (5).

Proof: For every $x \in \mathcal{X} \setminus \{x_0\}$,

$$\sum_{z \in \mathcal{Z}} W_{Z|X,s}(z|x)^\ell W_{Z|X,s'}(z|x)^{1-\ell}$$

$$= \sum_{z \in \mathcal{Z}} W_{Z|X,s}(\pi_s(z)|x_0)^\ell W_{Z|X,s'}(\pi_s(z)|x_0)^{1-\ell}\quad (10)$$

$$= \sum_{z \in \mathcal{Z}} W_{Z|X,s}(z'|x_0)^\ell W_{Z|X,s'}(z'|x_0)^{1-\ell}\quad (11)$$

$$= \sum_{z \in \mathcal{Z}} W_{Z|X,s}(z|x)^\ell W_{Z|X,s'}(z|x)^{1-\ell} \quad (12)$$

Thus, we know that the detection-error exponent is invariant to the input type under this scenario.

In other words, when the channel satisfies certain symmetry conditions, there is no tradeoff between rate and detection-error exponent and one simultaneously achieves the optimal communication rate and the optimal detection performance. One of the compound channel families that falls into such a category is the set of Binary Symmetric Channels (BSCs). The maximal detection-error exponent and the compound capacity are then simultaneously achieved with a uniform input distribution.

We now turn our attention back to the characterization of closed-loop schemes, which exploit the feedback to adapt to the state. The next theorem characterizes an inner bound of the set $C^{(m)}_{closed}$.

Theorem 2: The closure of all achievable joint communication and sensing rate/detection error exponent pairs for mono-static closed-loop schemes satisfies

$$C^{(m)}_{closed} \supseteq \bigcup_{P_{X,X'} \in (P_X)^{|S|}} \left\{ (R, E) \in \mathbb{R}^2_+ : \begin{array}{l} R \leq \min_{s \in S} I(P_X, W_{Y|X,s}) \\ E \leq \min_{s \in S} \phi(P_X) \end{array} \right\}$$

where the notation $\bigcup_{P_{X,X'} \in (P_X)^{|S|}}$ means that we are taking the union over all possible $|S|$-tuples of probability distributions in $P_X$ and $(P_X)^{|S|}$ is the set of tuples of $|S|$ elements in $P_X$.

Theorem 2 is obtained by considering a simple strategy in which the transmitter learns the state, informs the receiver, and uses a code adapted to the learned channel state. The exact characterization of the optimal tradeoffs for closed-loop schemes remains elusive and presents non-trivial challenges, chief among them the absence of a known optimal detection error-exponent for multi-hypothesis controlled sensing [21]. One can conclude that the maximal achievable detection-error exponent characterized by Theorem 2 is identical to that of the open-loop strategy by observing the following equality

$$\max_{P_{X,X'} \in (P_X)^{|S|}} \min_{s \in S} \phi(P_X, s) = \max_{P_X \in P_X} \phi(P_X).$$

Therefore, the region characterized in Theorem 2 is sub-optimal because it is already shown in [21] that there exists a closed-loop method that achieves a better detection-error exponent than an open-loop scheme. However, the benefit of Theorem 2 is in improving the communication rate from the compound channel capacity, i.e.,

$$\max_{P_X \in P_X} \min_{s \in S} I(P_X, W_{Y|X,s})$$

to the worst-case capacity, i.e.,

$$\min_{s \in S} \max_{P_X \in P_X} I(P_X, W_{Y|X,s}).$$

Note that the worst-case capacity is exactly the maximal achievable rate described in Theorem 2 because

$$\max_{P_{X,X'} \in (P_X)^{|S|}} \min_{s \in S} I(P_X, W_{Y|X,s}) = \min_{s \in S} \max_{P_X \in P_X} I(P_X, W_{Y|X,s}).$$

A similar technique exploiting the feedback to improve the capacity in a compound channel can be found in [26].

Remark 4: The regions characterized in Theorem 2 and Theorem 3 are identical when the condition in Corollary 2 is satisfied and the worst-case capacity is equal to the compound channel capacity.

B. Bi-Static Model

In joint communication and sensing, codewords convey information and induce a codeword-dependent distribution from which observations are generated and are used to estimate the state. In the mono-static model, state estimation is performed at the transmitter, which has the access to the transmitted codeword, so that a likelihood-based state estimation can be performed with exact knowledge of the transmitted codeword. In the bi-static model, however, the transmitted codeword is unknown to the state estimator $g^{(b)}$.

A natural method to estimate the state is to use a successive approach, by which one first estimates the codeword and then performs a maximum likelihood estimation given the decoded codeword. Denoting by $C^{(b)}$ the closure of all achievable regions in the bi-static model, our next theorem provides an inner bound of $C^{(b)}$ based on successive schemes.

Theorem 3: The closure region of all achievable joint communication and sensing rate/detection error exponent pairs for the bi-static joint communication and sensing model satisfies

$$C^{(b)} \supseteq \mathcal{D}_{succ} = \bigcup_{P_X \in P_X} \left\{ (R, E) \in \mathbb{R}^2_+ : \begin{array}{l} (R, E) \in \mathbb{R}^2_+ \\ R \leq \min_{s \in S} I(P_X, W_{Y|X,s}) \\ E \leq \min_{s \in S} \rho_{succ}(P_X, s, \phi(P_X)) \end{array} \right\},$$

where

$$\rho_{succ}(P_X, s, \phi(P_X)) = \min_{P_X \in P_X} \left( \mathbb{D}(P||W_{Y|X,s}|P_X) + |\mathbb{E}(P_X; \bar{P}) - R|^+ \right).$$

Proof: Theorem 3 is a direct result of the following inequality

$$P_d^{(n)} = \max_{s \in S} \max_{w \in [1:M]} \mathbb{P}\left( g^{(b)}(Y^n) \neq s | W = w, S = s \right)$$

$$= \max_{s \in S} \max_{w \in [1:M]} \mathbb{P}\left( g^{(b)}(Y^n) \neq s | h^{(b)} = w, W = w, S = s \right)$$

$$\times \mathbb{P}\left( h^{(b)} = w | W = w, S = s \right).$$
The calculation of $\rho_{\text{joint}}(P_X, R)$ in (13) involves a minimization over $\hat{P} \in \mathcal{P}_{\gamma}|X$ and $P' \in \mathcal{P}_{s,s'}(\hat{P}, P_X, R)$. In Corollary 3, we provide a lower bound on $\rho_{\text{joint}}(P_X, R)$ to simplify the expression and show that it is greater than or equal to the compound channel communication-error exponent $\rho_{\text{suc}}(P_X, R)$.

Corollary 3: For all $P_X$, it holds that $\rho_{\text{joint}}(P_X, R) \geq \rho_{\text{suc}}(P_X, R)$, and hence, $\mathcal{D}_{\text{joint}} \supseteq \mathcal{D}_{\text{suc}}$. Moreover, $\rho_{\text{joint}}(P_X, R)$ is lower bounded by

$$\rho_{\text{joint}}(P_X, R) \geq \min_s \left( \min_{\tilde{P} \in \mathcal{P}_{\gamma}|X}(\tilde{P}, R, s) \right),$$

where for all $\tilde{P}$ and $s$,

$$\gamma_1(\tilde{P}, R, s) \triangleq \mathcal{D}(\tilde{P} || W_{Y|X,s}|P_X) + \mathcal{H}(\tilde{P} | P_X) - R - R^+, \quad \text{and}$$

$$\gamma_2(\tilde{P}, R, s) \triangleq \mathcal{D}(\tilde{P} || W_{Y|X,s}|P_X) + \mathcal{H}(\tilde{P} | P_X),$$

and

$$\mathcal{P}_{\gamma|X}(P_X, R, s) \triangleq \left\{ \tilde{P} \in \mathcal{P}_{\gamma|X} : \max_{s' \in s} \min_{P' \in \mathcal{P}_{s,s'}(\tilde{P}, P_X, R)} \mathcal{D}(\tilde{P} || W_{Y|X,s}|P_X) + \mathcal{H}(\tilde{P} | P_X) \right\} \subseteq \mathcal{D}_{\text{joint}} \supseteq \mathcal{D}_{\text{suc}}.$$
TABLE I
Table for \( W_{Z|X,S}(0) = W_{Y|X,S}(0) \) for all \( X \in \{0, 1\} \) and \( S \in \{0, 1, 2\} \)

| S | X | 0      | 1      |
|---|---|--------|--------|
| 0 | 0.95 | 0.45   |
| 1 | 0.6  | 0.2    |
| 2 | 0.5  | 0.03   |

transmitting the symbol \( X = 1 \) is most useful to identify the channel state because this is the situation in which the output distributions corresponding to different states are most distinguishable. However, if the transmitter only transmits \( X = 1 \), the communication rate would become zero as seen in Fig. 3(a). Therefore, the tradeoff between maximizing the detection-error exponent and maximizing the communication rate can be clearly seen in Fig. 3(a). On the other hand, the difference between \( C_{\text{open}}^{(m)} \) and the inner bound of \( C_{\text{closed}}^{(m)} \) given in Theorem 2 is shown in Fig. 3(b), illustrating how the communication rate is increased. Indeed, the inner bound region for \( C_{\text{closed}}^{(m)} \) is larger than \( C_{\text{open}}^{(m)} \) because the compound capacity is here strictly less than the worst-case capacity.

In contrast to the channel given in Table I, for which the tradeoff between sensing and communication exists, the channel given in Table II is a BSC for which, according to Corollary 2, the best error exponent of detection is always achieved regardless of the type of codewords. The result of Theorem 1 for this channel is illustrated in Fig. 4.

Fig. 3. Closure region \( C_{\text{open}}^{(m)} \) and inner bounds for \( C_{\text{closed}}^{(m)} \) corresponding to the channel of Table I.

Fig. 4. Closure region \( C_{\text{open}}^{(m)} \) corresponding to the channel of Table II.

2) Bi-Static Model: For the bi-static model, we present a numerical example as defined in Table III. Here, \( Y = Z = X = \{0, 1\} \) and \( S = \{0, 1\} \). When \( S = 0 \), the channel \( W_{Y|X,0} \) is a BSC with cross-over probability 0.3, and \( W_{Y|X,1} \) is a BSC with cross-over probability 0.6. From Fig. 5, one observes that \( D_{\text{joint}}^{(m)} \) is strictly larger than \( D_{\text{succ}}^{(m)} \) especially when the code rate is high. When the rate is low, the exponent \( \rho_{\text{joint}}^{(m)} \) is dominated by the Chernoff information \( \phi(P_X) \), which is approximately 0.048 in this example. When the rate is high, the exponent is dominated by a rate-dependent term, capturing the fact the receiver’s inability to easily decode the transmitted sequence is what drives performance. By the definition of \( \rho_{\text{succ}}^{(m)} \), the value of \( \rho_{\text{succ}}^{(m)} \) is zero when the code rate is at the compound channel capacity. However, the joint detection scheme reaches a positive exponent even when transmitting at the compound capacity, highlighting the benefits of joint detection over successive decoding.

V. DETAILED PROOFS
A. Achievability Proof of Theorem 1

We show that all \((R, E)\) pairs within the region \( C_{\text{open}}^{(m)} \) are achievable. Since we restrict ourselves to open-loop schemes, we may fix \( P_X \) as the type of all codewords. Fix any \( \epsilon > 0 \). By [27, Th. 10.2], there exists a code with encoder \( f^{(m)} \) and

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
decoder $h^{(m)}$ such that $f^{(m)}(w) \in \mathcal{T}^n_w$ for all $w$, the rate is at least $\min_{s \in S} \mathbb{P}(P_X, W|X, s) - \epsilon$, and $\max_w \mathbb{P}(h(Y^n) \neq w|S = s) < \epsilon$ for all $s \in S$. Then, the detection-error exponent $\phi(P_X)$ is given by Lemma 1 adapted from [21, Th. 1].

**Lemma 1:** Suppose that the codeword corresponding to the message $w \in [1; M]$ has type $P_X \in \mathcal{P}_X$, the conditional detection-error exponent $E_d, w, s \triangleq \frac{1}{n} \log \max_{x \in S} \mathbb{P}(g(Z^n) \neq s|S = s, W = w)$ in an open-loop scheme is asymptotically upper bounded by

$$\phi(P_X) \triangleq \min_{s \neq s'} \min_{\epsilon \in [0, 1]} - \sum_{x} P_X(x) \times \log \left( \sum_{z} W_{Z|X,s}(z|x)^{\ell} W_{Z|X,s'}(z|x)^{1-\ell} \right).$$

Moreover, it is also asymptotically achievable by a maximum likelihood estimator $g_{ML}$. Specifically,

$$\max_{s \in S} \mathbb{P}(g_{ML}(Z^n) \neq s|S = s, W = w) \leq \Theta_n(1) e^{-\phi(P_X)}$$

for all $w \in [1; M]$, and for all $s \in S$

$$\mathbb{P}(g_{ML}(Z^n) \neq s|S = s, W = w) \leq \Theta_n(1) e^{-\psi(s)(P_X)}.$$

for all $w \in [1; M]$, where

$$\psi_s(P_X) \triangleq \min_{x} - \sum_{x} P_X(x) \times \log \left( \sum_{z} W_{Z|X,s}(z|x)^{\ell} W_{Z|X,s'}(z|x)^{1-\ell} \right).$$

Taking the union over all possible $P_X$ leads to the region in (4).

**B. Converse Proof of Theorem 1**

Assume that the rate/detection-error exponent pair $(R, E)$ is achievable. Then, for all $\epsilon > 0$, there exists $n$ sufficiently large and a codebook $C^{(n)}$ such that

$$\frac{\log |C^{(n)}|}{n} \geq R - \epsilon$$

and

$$\max_{s \in S} \max_{w \in [1; M]} \mathbb{P}(h(Y^n) \neq w|W = w, S = s) \leq \epsilon$$

for all $s \neq s' \in S$, $w \in [1; M]$, and

$$\frac{1}{n} \log \mathbb{P}(g(Z^n) \neq s|W = w, S = s) \geq E - \epsilon.$$ 

Since there is at most a polynomial number of types, there exists a set of types $\mathcal{T}$ such that, for all $P_X \in \mathcal{T}$, the subcode $C_{P_X} \triangleq \{ f(w) : P_{f(w)} = P_X \} \subset C^{(n)}$ satisfies

$$\max_{s \in S} \mathbb{P}(h(Y^n) \neq w|W = w, S = s) \leq \epsilon$$

and

$$\frac{\log |C_{P_X}|}{n} > \frac{\log |C^{(n)}|}{n} - \delta \geq R - \epsilon - \delta$$

for some $\delta$ vanishing with $\epsilon$. Fix any $P_X \in \mathcal{T}$. Let

$$\tilde{P}_X(x) \triangleq \frac{1}{|C_{P_X}|} \sum_{s \in C_{P_X}} 1[x = \tilde{x}].$$

Observe that

$$\tilde{P}_X(x) \triangleq \frac{1}{n} \sum_{i=1}^{n} \tilde{P}_X(x) = P_X(x),$$

where $\tilde{P}_X$ is the $i$-th marginal distribution of $\tilde{P}_X$. Then, for any state $s$,

$$(1 - \epsilon) \log |C_{P_X}| - h_b(\epsilon)$$

where $h_b(\epsilon)$ is the binary entropy function, (a) follows from Fano’s inequality and standard techniques, (b) follows by identifying $Y^n \sim P_{\tilde{X}} 0^{\epsilon(i)}, |X|$, and the definition of mutual information, and (c) follows from the concavity of mutual information in the input distribution. Then, we obtain

$$\frac{\log |C_{P_X}|}{n} \leq \frac{\mathbb{P}(P_X, W|X, s) + \frac{\epsilon}{2}}{1 - \epsilon},$$

where we have used (17).

Since (19) is valid for any $\epsilon$ and state $s$, the size of sub-codebook $C_{P_X}$ is upper bounded by the mutual information in a compound channel, i.e.,

$$\frac{\log |C_{P_X}|}{n} < \min_{s \in S} \mathbb{P}(P_X, W|X, s) + \tau$$

for some $\tau > 0$ vanishing with $\epsilon$. On the other hand, for this $P_X \in \mathcal{T}$,

$$E - \epsilon$$

$$\leq \frac{1}{n} \log \max_{s \in S} \mathbb{P}(g(Z^n) \neq s|W = w, S = s)$$

and

$$\leq \frac{1}{n} \log \max_{s \in S} \mathbb{P}(g(Z^n) \neq s|W = w, S = s) \leq \phi(P_X) + \delta,$$

where (a) follows by restricting the set to only the terms corresponding to messages in $C_{P_X}$; (b) follows since the detection error is upper bounded by $\phi(P_X)$ for any message with type $P_X$ by Lemma 1. Combining (20) and (21) and choosing $P^*_X \triangleq \arg \min_{s \in \text{supp}} \phi(P_X)$, we conclude that for all $\epsilon > 0$, there exist $\tau, \delta > 0$ vanishing with $\epsilon$ such that

$$R \leq \min_{s} \mathbb{I}(P^*_s, W|X, s) + \tau + \epsilon + \delta$$

and

$$E \leq \phi(P^*_X) + \delta + \epsilon.$$
Since \( \epsilon, \tau, \delta \) can be chosen arbitrarily small as the block length \( n \) goes to infinity, \( E \) is upper bounded by \( \phi(P_X) \) for some \( P_X \in \mathcal{P}_X \) and the rate \( R \) is achieved by this \( P_X \). Taking the union over all possible \( P_X \) completes the result of converse of Theorem 1.

C. Proof of Theorem 2

1) Definition of the Code: Before the protocol starts, we fix \( n \in \mathbb{N}^*, \Delta_1, \Delta_2 \in (0,1) \) such that \( \Delta_1 + \Delta_2 < 1 \), and we also fix some \( |S| \)-tuple \( (P_{X,s}^n, \gamma^n, h_{\gamma^n}) \), where \( \{ P_{X,(1-\Delta_1-\Delta_2)n}^{(1-\Delta_1-\Delta_2)n} | \tilde{S} \} \) is the set of tuples of types in \( \mathcal{P}_X^{(1-\Delta_1-\Delta_2)n} \), as well as the number of messages \( M \) as

\[
M = n(1 - \Delta_1 - \Delta_2) \times \left( \min_{s \in \mathcal{S}} \mathbb{I}(P_{X,s,\epsilon}, W_Y^{X,s,\epsilon}) - \delta \right)
\]

for some \( \delta > 0 \).

We first define \( g_{\text{ML},1} \) as the maximum likelihood estimator at each time \( i \in \mathbb{N}^* \), i.e.,

\[
g_{\text{ML},1}(z_i, \epsilon) = \arg \max_{s \in \mathcal{S}} \prod_{\ell=1}^{i} W_X(z_i | x_{\ell})
\]

Then, the code \( C^{(m)} = ([S]_{1:n}, g^{(m)}, h^{(m)}) \) is defined through the following steps.

a) Initial estimation: We define \( P_X^{(1-\Delta_1)n} \phi(P_X) \) and pick any length \( n \Delta_1 \) sequence \( v = (v_1, \ldots, v_{n \Delta_1}) \) from the type class \( \mathcal{P}_X^{(1-\Delta_1)n} \). Then, for \( 1 \leq i \leq \Delta_1 n \), the encoder is defined as

\[
f_i(w, z^{i-1}) = v_i
\]

for all \( w \in [1: M] \) and \( z^{i-1} \in \mathbb{Z}^{i-1} \). At time \( \Delta_1 n + 1 \), the transmitter estimates the state by using the maximum likelihood estimator \( \tilde{s} = g_{\text{ML},\Delta_1 n}(X_{\Delta_1 n}, z_{\Delta_1 n}) \).

b) State information transmission: The transmitter then conveys the information of the estimated state to the receiver by encoding the estimated state \( \tilde{s} \) into a codeword. Since \( |S| \) does not grow with \( n \), there exists a channel length \( \Delta_2 n \) channel code \( f : \tilde{s} \mapsto X_{\Delta_2 n} \) with arbitrarily small error probability, where \( f : \tilde{s} \mapsto X_{\Delta_2 n} \) is the encoder and \( \tilde{s} : Y_{\Delta_2 n} \mapsto \tilde{s} \) is the decoder. Denoting \( \tilde{x}_s(\tilde{s}) = (\tilde{x}_1(\tilde{s}), \ldots, \tilde{x}_{\Delta_2 n}(\tilde{s})) = f(\tilde{s}) \) the codeword corresponding to \( \tilde{s} \). Then, for \( \Delta_1 n < i \leq (\Delta_1 + \Delta_2) n \), the encoder is defined as

\[
f_i(w, z^{i-1}) = \tilde{x}_{i-\Delta_1 n}(g_{\text{ML},\Delta_1 n}(X_{\Delta_1 n}, z_{\Delta_1 n}))
\]

for all \( w \in [1: M] \) and \( z^{i-1} \in \mathbb{Z}^{i-1} \).

c) Message transmission: It is known that for every \( P_X \in \mathcal{P}_X \), there exists a channel code with arbitrarily small error probability \( \epsilon > 0 \) such that the rate is at least \( \mathbb{I}(P_X, W_Y^{X,s,\epsilon}) - 2 \tau \) for any \( \tau > 0 \) when the channel state is \( s \in \mathcal{S} \) and the number of channel uses is large enough. Therefore, for any \( s \in \mathcal{S} \), there exist an \( (1 - \Delta_1 - \Delta_2) n, \epsilon \) constant composition code with the type \( P_{X,s} \) for the state \( s \) channel with rate \( \min_{s \in \mathcal{S}} \mathbb{I}(P_{X,s}, W_Y^{X,s,\epsilon}) - \delta \) for any \( \delta > 0 \), where the set of types \( \{ P_{X,s}^{(1-\Delta_1-\Delta_2)n} | \tilde{S} \} \) is fixed at the beginning of the protocol. Let the channel code for the channel with state \( s \) be characterized by \( (f_s, h_s) \), where \( f_s : [1: M] \mapsto X^{(1-\Delta_1-\Delta_2)n} \) is the encoder and \( h_s : f_s([1: M]) \mapsto \mathcal{Y}^{(1-\Delta_1-\Delta_2)n} \) is the decoder.
Note that \( \text{argmax}_{s \in S} \prod_{t = (\Delta_1 + \Delta_2)n + 1}^{n} W_{Z|X}(z_{\ell}|x_{\ell}) \neq s \) is the error event of applying the ML estimator when the type of the input sequence is \( \hat{P}_{X|S}^{n}(\Delta_1 + \Delta_2) = 1 \). For all \( t \in [n(\Delta_1 + \Delta_2) + 1; n] \), the channel input \( X_{t} \) is chosen without using the feedback \( Z_{\Delta_1(\Delta_1 + \Delta_2) + 1}^{n} \). Moreover, for any \( w \in [1; M] \), the sequence \( X_{t}^{n}(\Delta_1 + \Delta_2) = 1 \) has a constant type which depends on \( \hat{s} \). Therefore, we can apply Lemma 1 and the law of total probability to upper bound the error probability of (30) as

\[
P_{d}^{(n)} \leq \max_{s \in S} \max_{w \in [1; M]} \sum_{s' \in S} \mathbb{P} \left( \hat{s} = s'|W = w, S = s \right)
\]

where in (31) we lower bound the exponent \( \psi_{S}(P_{X|S}) \) by the minimum one and \( \Theta_{n}(1) \) is some constant, and in (32) we swap the order of \( \min_{s \in S} \) and \( \min_{s' \in S} \) and apply the definition of \( \Phi \). Then, we have shown that

\[
P_{d}^{(n)} \geq \left( 1 - \Delta_1 - \Delta_2 \right) \min_{s \in S} \Phi(P_{X,s}).
\] (33)

By taking the union over all possible choices of \( \{P_{X,s'} \}_{s' \in S} \in (P_{X}^{(\Delta_1(\Delta_1 + \Delta_2)n + 1)} | S) \) and making \( \Delta_1, \Delta_2 \) arbitrarily small, we conclude that the following region is achievable.

\[
\bigcup_{s \in S} \left\{ (R, E) \in \mathbb{R}^{2}; \begin{array}{l}
R \leq \min_{s \in S} \mathbb{E}(P_{X,s}, W_{Y|X,s}) \\
E \leq \min_{s \in S} \Phi(P_{X,s})
\end{array} \right\}
\] (34)

To recover the result of Theorem 2, note that for any \( P_{X} \in P_{X} \), there exists some type \( \hat{P}_{X} \in P_{X}^{(\Delta_1(\Delta_1 + \Delta_2)n + 1)} \) such that \( |P_{X}(X) - \hat{P}_{X}(X)| \leq \eta \) for any \( x \in \mathcal{X} \) and \( \eta > 0 \) for some \( n \) large enough. A similar continuity argument can be used to guarantee that the rate and exponent derived by \( \hat{P}_{X} \) would be \( \xi(n) \)-close to the result obtained by \( P_{X} \), where the difference \( \xi(n) \) vanishes with \( n \). By taking the union of all \( \{P_{X,s} \}_{s \in S} \), we conclude that the closure of all achievable regions is at least

\[
\bigcup_{s \in S} \left\{ (R, E) \in \mathbb{R}^{2}; \begin{array}{l}
R \leq \min_{s \in S} \mathbb{E}(P_{X,s}, W_{Y|X,s}) \\
E \leq \min_{s \in S} \Phi(P_{X,s})
\end{array} \right\}
\] (35)

which completes the proof.

D. Proof of Theorem 4

We first construct the code by the following steps. Fix a specific type \( P_{X} \). The length \( n \) codeword corresponds to the message \( w \in [1; M] \) is \( x_{w} \), and is uniformly drawn from the type class \( \mathcal{T}_{P}(n) \). The message decoder and the state estimator are jointly defined as

\[
(\hat{w}, \hat{s}) = \text{argmax}_{w \in [1; M], s \in S} \mathbb{P}(y|S = s, X^{n} = x_{w}).
\] (36)

The message decoder \( h^{(b)} \) and the state estimator \( g^{(b)} \) are then well-defined by (34). Note that the codewords \( \{x_{w} \}_{w \in [1; M]} \) are random and so is the code \( C^{(b)} \). Since we have fixed the definition of \( h^{(b)} \) and \( g^{(b)} \), with a slight abuse of notation, we denote \( C^{(b)} = \{x_{w} \}_{w \in [1; M]} \) as the set of codewords in the derivation below. We next derive the detection-error exponent when averaging over \( C^{(b)} \), which codewords are drawn uniformly from \( \mathcal{T}_{P_{X}}(n) \).

1) Detection-Error Analysis: Without loss of generality we assume that the message \( w = 1 \) is transmitted and the state \( S = s \) for some \( s \in S \). The error event is the set of all received \( y \) that would result in detection errors and is defined as

\[
\mathcal{E} = \left\{ y \in \mathcal{Y}^{n}; \max_{i \in [1; M]} \mathbb{P}(y|S = s, X^{n} = x_{i}) < \min_{i \in [1; M]} \mathbb{P}(y|S = s', X^{n} = x_{i}) \right\}
\] (37)

For any \( \hat{P}_{Y|X} \in P_{Y|X} \), it is known from [28] that the probability of receiving \( y \in \mathcal{T}_{X}(\hat{P}_{Y|X}) \) is upper bounded by

\[
\mathbb{P}(y \in \mathcal{T}_{X}(\hat{P}_{Y|X}) | X^{n} = x_{1}, S = s) \leq e^{-\Delta_{1}(\hat{P}_{Y|X}||W_{Y|X,s}P_{X})},
\] (38)

For all \( y \in \mathcal{Y}^{n} \) and for any \( k \neq 1 \), we define the random variable

\[
I_{k}(y) \triangleq \mathbb{1} \left( \max_{i \neq k} \mathbb{P}(y|S = s, X^{n} = x_{i}) \right) \leq \mathbb{P}(y|S = s', X^{n} = x_{1})
\] for some \( s' \neq s \)

\[
= 1(\exists s' \neq s \text{ s.t. } e^{\Delta_{1} \sum_{i \neq k} P_{X}(x)\tilde{P}_{Y|X,i} g_{Y|X,i} g_{Y|X,s}}) \geq \max_{i \neq k} e^{\Delta_{1} \sum_{i \neq k} P_{X}(x)\tilde{P}_{Y|X,i} g_{Y|X,i} g_{Y|X,s}}.
\] (39)

The randomness of the variables \( I_{k}(y) \) and \( J_{1}(y) \) comes from the random coding, i.e., the type \( \tilde{P}_{Y|X} \) is random. \( I_{k}(y) \) is equal to one when there exists some state \( s' \neq s \) such that the likelihood calculated according to the state \( s' \) and the codeword \( k \) is greater than the maximal possible likelihood according to the state \( s \). Then, the average detection error probability can be upper bounded by the following

\[
\frac{E_{C_{\text{ub}}}^{(n)}}{\mathbb{P}(y \neq s|X^{n} = x_{1}, S = s)} \leq \frac{1}{|T_{P_{X}}(n)|} \sum_{s \in T_{P_{X}}(n)} \sum_{x_{1} \in T_{P_{X}}(n)} \sum_{y \in T_{X}} \mathbb{P}(y|X^{n} = x_{1}, S = s)
\]

\[
\times \mathbb{P} \left( \text{error}|X^{n} = x_{1}, S = s, Y^{n} = y \right) \quad \text{(37)}
\]

\[
\leq \frac{1}{|T_{P_{X}}(n)|} \sum_{s \in T_{P_{X}}(n)} \sum_{x_{1} \in T_{P_{X}}(n)} \sum_{y \in T_{X}} \mathbb{P}(y|X^{n} = x_{1}, S = s)
\]

\[
\times \sum_{k \neq 1} \mathbb{E}_{C^{(b)}}(I_{k}(y)|X^{n} = x_{1}, S = s) \quad \text{(38)}
\]
where the expectation is taken over all possibilities of codewords \( \{x_\ell\}_{\ell \neq 1} \). Note that \( I_k(y) \) is random because the codewords \( \{x_\ell\}_{\ell \neq 1} \) are drawn from \( T_{p_k} \) uniformly, and hence, \( \{\hat{p}_{Y|X_k}\}_{\ell \neq 1} \) are random as well.

The difficulty of analyzing \( I_k(y) \) comes from the term \( \max_{\ell \neq k} e^n \sum_{x \in T_{p_k}} P_x(x) \hat{p}_{Y|X_k}(y|x) \log W_{Y|X_k}(y|x) \), which involves a maximization over exponentially many indices \( \ell \). Observe that

\[
\max_{\ell \neq k} e^n \sum_{x \in T_{p_k}} P_x(x) \hat{p}_{Y|X_k}(y|x) \log W_{Y|X_k}(y|x) = \max_{\ell \neq k} e^{-nD(\hat{p}_{Y|X_k}||W_{Y|X_k}) + \mathbb{H}(\hat{p}_{Y|X_k}|P_X)}.
\]

(39)

Note that the type \( \hat{Y|X_k} \) is fixed when \( y \in T_{|X_k}(\hat{p}_{Y|X_k}) \) for some \( \hat{p}_{Y|X_k} \in \mathcal{P}_{Y|X_k} \). Therefore, in the following we define a set \( A_k \) of conditional types \( \{\hat{p}_{Y|X_k}(\cdot|x_{\ell}, 1, k) \in \mathcal{P}_{Y|X_k}\}^{2n-2} \) such that when \( x_\ell \in T_{|X_k}(\hat{p}_{Y|X_k}) \) for all \( \ell \neq [1, k] \), we can control the right-hand side of (39). Moreover, \( A_k \) needs to have the property that \( \{\hat{Y|X_k}(\cdot|x_{\ell}, 1, k) \in A_k \) with high probability. Specifically, we define

\[
A_k \left( \hat{p}_{Y|X_k}(\cdot|x_{\ell}, 1, k), P_X, R \right) \triangleq \left\{ \hat{p}_{Y|X_k}(\cdot|x_{\ell}, 1, k) \in \mathcal{P}_{Y|X_k}^{2n-2} : \right. \\
\forall \hat{p}_{Y|X}(\cdot|x_{\ell}, 1, k) \in \mathcal{P}_{Y|X_k}, \exists j \notin [1, k] \ s.t. \ P_X \circ \hat{p}_{Y|X} = \hat{p}_{Y|X_k} \circ P_X \}
\]

Then, by using the law of total probability, we have

\[
\mathbb{E}_{C^{(0)}_{X_k}} \left[ I_k(y) | X^n = x_1, S = s \right] = \sum_{\hat{p}_{Y|X_k}(\cdot|x_{\ell}, 1, k) \in A_k} \prod_{\ell \notin [1, k]} \mathbb{P} \left( x_\ell \in T_{|X_k}(\hat{p}_{Y|X_k}) \right) \\
\times \mathbb{E}_{x_\ell} \left[ I_k(y) | x_\ell = x \right],
\]

(40)

where (a) follows since for every \( \hat{p}_{Y|X} \in \mathcal{P}_{Y|X_k}^{2n-2} \) satisfying \( \mathbb{I}(P_X, \hat{p}_{Y|X}) < R \), there is some \( \hat{p}_{Y|X_k} \) such that \( \hat{p}_{Y|X_k} = \hat{p}_{Y|X} \) by definition of \( A_k \). Then, for \( y \in T_{|X_k}(\hat{p}_{Y|X_k}) \), the indicator function \( I_k \) can be upper bounded by

\[
I_k(y) \leq \sum_{s \neq s'} 1 \left( x_k \in T_{|X_k}(P_{Y|X}^{(1)}) \right)
\]

for some \( P_{Y|X} \in \mathcal{P}_{Y|X}^{n, s} \).
and $|P^n_{x,s}|(\hat{P}^{(1)}_{Y|X}, P_X, R)| \leq \text{poly}(n)$. Moreover, for all $P'' \in P^n_{Y|X}$ such that $\mathbb{I}(P_X, P'') < R$ and for all $\ell \notin \{1, k\}$, it holds that
\[
P \left( x^\ell \notin \mathcal{T}_Y(P') \right) \leq 1 - e^{-n(\mathbb{I}(P_X, P'') + o(n))} \leq e^{-n(\mathbb{I}(P_X, P') + o(n))},
\]
for some $\xi < R$, where in (42) we lower bound $P(\mathcal{T}_Y(P'))$ by $e^{-n(\mathbb{I}(P_X, P'') + o(n))}$ [29, eq. (14)] and in (43) we use the fact that $1 - x \leq e^{-x}$ for all $x \in \mathbb{R}$. Then,
\[
\sum_{P' \in P^n_{Y|X}; \mathbb{I}(P_X, P'') < R, \ell \notin \{1, k\}} \prod_{\ell \notin \{1, k\}} P \left( x^\ell \notin \mathcal{T}_Y(P') \right) \leq e^{-n\mathbb{I}(P_X, P'') + o(n)}
\]
which has the double exponential form and decays much faster than the right-hand side of (41), and (44) follows since $\mathbb{I}(\hat{P}^{(1)}_{Y|X} | \ell \notin \{1, k\}, A_k(\hat{P}^{(1)}_{Y|X}, P_X, R)) = 0$. Therefore, for $\mathcal{T}_Y(P'^*)$, it holds that
\[
\mathbb{E}_{C(\xi)}[l(y)|X^n = y, S = s] \leq e^{-n\min_{\nu, \nu' \geq 0} \mathbb{I}(\hat{P}^{(1)}_{Y|X} | \ell \notin \{1, k\}, A_k(\hat{P}^{(1)}_{Y|X}, P_X, R)) - o(n)}.
\]
By applying inequality (47) to the first term on the right-hand side of (38) and using (35), we obtain
\[
\frac{1}{|P^n_{Y|X}|} \sum_{x^1 \in T^n_{P_X}} \sum_{y \in \mathcal{T}_Y(\hat{P}^{(1)}_{Y|X})} \sum_{y_1 \in \mathcal{T}_Y(\hat{P}^{(1)}_{Y|X})} \mathbb{P}(y|X^n = x_1, S = s) \times \mathbb{E}_{C(\xi)}[l(y)|X^n = x_1, S = s] \leq \text{poly}(n) \times \exp \left( -n \min_{\nu, \nu' \geq 0} \mathbb{I}(\hat{P}^{(1)}_{Y|X} | X^n, S = s) \right)
\]
which is the detection-error probability by using the ML detector when the codeword is known. From Lemma 1, we have
\[
\frac{1}{|P^n_{Y|X}|} \sum_{x^1 \in T^n_{P_X}} \sum_{y \in \mathcal{T}_Y(\hat{P}^{(1)}_{Y|X})} \sum_{y_1 \in \mathcal{T}_Y(\hat{P}^{(1)}_{Y|X})} \mathbb{P}(y|X^n = x_1, S = s)J_1(y) \leq e^{-n\phi(P_X)}
\]
Combining (38), (48), (49), we have
\[
\mathbb{E}_{C(\delta)}[\mathbb{P}(\hat{s} \neq s|X^n = x_w, S = s)] \leq e^{-n\min(\phi(P_X), \rho_{\text{joint}}(P_X, R) - \epsilon(\delta))},
\]
for all $s \in \mathcal{S}$ by the linearity of expectation.

2) Communication-Error Analysis: By [27, Lemma 10.1 and Th. 10.2], we have that
\[
\mathbb{E}_{C(\delta)}[\max_{s} \mathbb{P}(\hat{w} \neq w|X^n = x_w, S = s)] \leq e^{-n\rho_{\text{acc}}(P_X, R) - \epsilon(\delta)},
\]
where $\kappa$ vanishes with $n$.

3) Derandomization and Expurgation: By the Markov’s inequality, we have for any $\zeta > 0$
\[
\mathbb{P}_{C(\delta)} \left( \exists s \in S \text{ s.t. } \frac{1}{M} \sum_{w} \mathbb{P}(\hat{s} \neq s|X^n = x_w, S = s) > e^{-n(\min(\phi(P_X), \rho_{\text{joint}}(P_X, R) - \epsilon(\delta)) - \zeta)} \right) \leq \frac{1}{M} \mathbb{E}_{C(\delta)}[\sum_{s} \mathbb{P}(\hat{s} \neq s|X^n = x_w, S = s)]
\]
which goes to zero when $n \to \infty$. Therefore, there exists some code $C(\delta')$ such that
\[
\max_{s} \frac{1}{M} \sum_{w=1}^{M} \mathbb{P}(\hat{s} \neq s|X^n = x_w, S = s) < e^{-n(\min(\phi(P_X), \rho_{\text{joint}}(P_X, R) - \epsilon(\delta)) - \zeta)},
\]
\[
\max_{w} \mathbb{P}(\hat{w} \neq w|X^n = x_w, S = s) < e^{-n(\rho_{\text{acc}}(P_X, R) - \zeta)}
\]
when \( n \) is sufficiently large. By the codebook expurgation argument, there exists a code \( \tilde{C}^{(b)} \triangleq \{ \tilde{x}_n \} \subset C^{(b)} \) with size \( |\tilde{C}^{(b)}| = |C^{(b)}|/2 \) such that
\[
\max_s \max_w \mathbb{P}(\hat{s} \neq s | X^n = \tilde{x}_n, S = s) < 2 e^{-n(\min(\phi(P_x), \rho_{\text{joint}}(P_x, R)) - \epsilon(s) - \zeta_1)}, \quad (56)
\]
\[
\max_s \max_w \mathbb{P}(\hat{w} \neq w | X^n = x_n, S = s) < 2 e^{-n(\rho_{\text{succ}}(P_x, R) - \zeta_2)}. \quad (57)
\]
For every \( R < \min_{\lambda} \mathbb{I}(P(x, W_{Y,X|s})) \), there exists some \( \zeta_2 > 0 \). Therefore, for every \( R < \min_{\lambda} \mathbb{I}(P(x, W_{Y,X|s})) \) there exists a code \( \tilde{C}^{(b)} \) with rate \( R - o_n(1) \) that
\[
-\frac{1}{n} \log \max_s \max_w \mathbb{P}(\hat{s} \neq s | X^n = \tilde{x}_n, S = s) \
\geq \min_{\beta} \left( \phi(P_x), \rho_{\text{joint}}(P_x, R) \right) - \epsilon, \quad (58)
\]
\[
\max_s \max_w \mathbb{P}(\hat{w} \neq w | X^n = \tilde{x}_n, S = s) < \epsilon \quad (59)
\]
for any \( \epsilon > 0 \) whenever \( n \) is sufficiently large. The theorem is proved by taking the union over all possible \( P_x \).

### E. Proof of Corollary 3

Recall that the definition of \( \rho_{\text{joint}}(P_x, R) \) is
\[
\rho_{\text{joint}}(P_x, R) \triangleq \min_{s \in S} \min_{P} \left( \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) + \mathbb{H}(P' | P_X) \right)^+ + \min_{s' \neq s} \min_{P' \in \mathcal{P}_{s',s}(P_x, R)} \| (P_x, P') - R \|^+. \quad (60)
\]
We first analyze the term \( \min_{s} \min_{P \in \mathcal{P}_{s'}(P_x, R)} \tilde{P}(P_{Y,X|s}, s, \tilde{P}) \). Let the arguments of the minimization of the term \( \min_{s} \mathbb{I}(P_{Y,X|s}) \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \)
\[
+ \min_{s' \neq s} \min_{P' \in \mathcal{P}_{s',s}(P_x, R)} \| (P_x, P') - R \|^+. \quad (59)
\]
be achieved by the tuple \((\tilde{P}, s', P')\), where \( \tilde{P}, s' \) and \( P' \) are the minimizer corresponding to \( \min_{s} \mathbb{I}(P_{Y,X|s}) \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \) and \( \min_{s' \neq s} \mathbb{I}(P_{Y,X|s}) \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \), respectively. Given the tuple \((\tilde{P}, s', P')\), if \( \mathbb{I}(P_{Y,X|s}) \geq \mathbb{I}(\tilde{P}, \tilde{P}) \), then
\[
\min_{P \in \mathcal{P}_{s'}(P_x, R)} \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \quad + \min_{s' \neq s} \min_{P' \in \mathcal{P}_{s',s}(P_x, R)} \| (P_x, P') - R \|^+. \quad (60)
\]
On the other hand, if the minimizer \( P' \) satisfies \( \mathbb{I}(P_{Y,X|s}) < \mathbb{I}(\tilde{P}, \tilde{P}) \), then by definition of \( \mathcal{P}_{s',s}(P_x, R) \) and the fact that \( \tilde{P} \in \mathcal{P}_{s'}(P_{Y,X|s}) \), it holds that
\[
\mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \geq \mathbb{D}(P' \| W_{Y|X,s}|P_X) \quad (61)
\]
Moreover, since \( P' \in \mathcal{P}_{s',s}(P_x, R) \), it holds that
\[
\mathbb{D}(P' \| W_{Y|X,s}|P_X) \leq \min_{s' \neq s} \mathbb{I}(P_{Y,X|s'}) \quad (62)
\]
where in \( (62) \) we use the fact that \( P_X \circ P' = P_X \circ \tilde{P} \). Therefore, by definition of \( \mathcal{P}_{s',s}(P_x, R) \) it holds that \( P' \in \mathcal{P}_{s'}(P_{Y,X|s'}) \). Then,
\[
\min_{P' \in \mathcal{P}_{s'}(P_{Y,X|s'})} \mathbb{D}(P_{Y,X|s'}|P_X) \quad (64)
\]
\[
\mathbb{D}(P_{Y,X|s'}|P_X) \leq \min_{s' \neq s} \mathbb{I}(P_{Y,X|s}) \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \quad (65)
\]
where in \( (65) \) we use the fact that \( P_X \circ P' = P_X \circ \tilde{P} \). Therefore, by definition of \( \mathcal{P}_{s',s}(P_x, R) \) it holds that \( P' \in \mathcal{P}_{s'}(P_{Y,X|s'}) \). Then,
\[
\min_{P' \in \mathcal{P}_{s'}(P_{Y,X|s'})} \mathbb{D}(P_{Y,X|s'}|P_X) \quad (66)
\]
\[
\mathbb{D}(P_{Y,X|s'}|P_X) \leq \min_{s' \neq s} \mathbb{I}(P_{Y,X|s}) \mathbb{D}(\tilde{P} \| W_{Y|X,s}|P_X) \quad (67)
\]
Taking the minimum over both cases of $\|(P_X, P') \geq \|(P_X, \bar{P})$ and $\|(P_X, P') < \|(P_X, \bar{P})$ and all possible $s \in S$, we obtain that
\[
\rho(P_X, R, s) = \rho(P_X, R, s, \bar{P}) \geq \min_{s} \min_{P \in P'_r}(P_X, P, R, s, \bar{P}) + \|P_X - \bar{P}\| + \|R - P\|
\]
Finally, by taking the minimum over all $s$ and applying the fact that $\rho_{\text{joint}}(P_X, R)$ is the minimum of the right-hand sides of (64) and (68), we conclude that
\[
\rho_{\text{joint}}(P_X, R) \geq \min_{s} \min_{\bar{P}} \left( \gamma_1(P_X, R, s) \right),
\]
where for all $\bar{P}$ and $\gamma_1(P_X, R, s) \triangleq \|P_X - \bar{P}\| - \|P_X - P\| - \|P - R\| + \|P - R\|
\]

References

[1] M.-C. Chang, T. Erdoğan, S.-Y. Wang, and M. R. Bloch, “Rate and detection error-exponent tradeoffs of joint communication and sensing,” in Proc. IEEE Int. Symp. Joint Commun. Sens., Vienna, Austria, Mar. 2022, pp. 1–6.
[2] B. Paul, A. R. Chiriyath, and D. W. Bliss, “Survey of RF communications and sensing convergence research,” IEEE Access, vol. 5, pp. 252–270, 2017.
[3] G. Fettweis et al., Joint Communication & Sensing: VDE Positionspapier, VDE e.V., Frankfurt, Germany, Jul. 2021.
[4] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, “Robust transmit beamforming for beyond 5G and 6G systems,” IEEE Trans. Signal Process., vol. 64, no. 2, pp. 464–474, Jan. 2016.
[5] L. Zheng, M. Lops, Y. C. Eldar, and X. Wang, “Radar and communication coexistence: An overview,” Proc. IEEE, vol. 109, no. 5, pp. 85–99, Sep. 2019.
[6] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, “Joint radar and communication design: Applications, state-of-the-art, and the road ahead,” IEEE Trans. Commun., vol. 68, no. 6, pp. 3834–3862, Jun. 2020.
[7] T. Wild, V. Braun, and H. Viswanathan, “Joint design of communication and sensing for beyond 5G and 6G systems,” IEEE Access, vol. 9, pp. 30845–30857, 2021.
[8] Y. H. Kim, A. Sutivong, and T. M. Cover, “State amplification,” IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 1850–1859, May 2008.
[9] C. Choudhuri, Y.-H. Kim, and U. Mitra, “Causal state amplification,” in Proc. IEEE Int. Symp. Inf. Theory, Aug. 2011, pp. 2110–2114.
[10] 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.
[11] M. Kobayashi, G. Caire, and G. Kramer, “Joint state sensing and communication: Optimal tradeoff for a memoryless case,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2018, pp. 111–115.
[12] M. Ahmadipour, M. Kobayashi, M. Wigger, and G. Caire, “An information-theoretic approach to joint sensing and communication,” IEEE Trans. Inf. Theory, early access, May 30, 2022, doi: 10.1109/TIT.2022.3176139.
[13] M. Kobayashi, H. Hamad, R. G. Kramer, and G. Caire, “Joint state sensing and communication over memoryless multiple access channels,” in Proc. IEEE Int. Symp. Inf. Theory, Paris, France, Jul. 2019, pp. 270–274.
[14] M. Ahmadipour, M. Wigger, and M. Kobayashi, “Joint sensing and communication over memoryless broadcast channels,” in Proc. IEEE Int. Theory Workshop, Apr. 2021, pp. 1–5.
[15] 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.
[16] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, “Robust transmit beamforming for secure integrated sensing and communication,” Jul. 2022, arXiv:2207.13863.
[17] O. Günlü, M. R. Bloch, R. Schaefer, and A. Yener, “Secure joint communication and sensing,” in Proc. IEEE Int. Symp. Inf. Theory, Helsinki, Finland, Jun. 2022, pp. 844–849.
[18] Y. Xiong, F. Liu, Y. Cui, W. Yuan, and T. X. Han, “Flowing the information from Shannon to Fisher: Towards the fundamental tradeoff in ISAC,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2022, pp. 5601–5606.
[19] H. Joudeh and F. M. J. Willems, “Joint communication and binary state
detection,” IEEE J. Sel. Areas Inf. Theory, vol. 3, no. 1, pp. 113–124,
Mar. 2022.
[20] H. Wu and H. Joudeh, “On joint communication and channel discrimi-
nation,” in Proc. IEEE Int. Symp. Inf. Theory, Espoo, Finland, Jun. 2022,
pp. 3321–3326.
[21] S. Nitinawarat, G. K. Atia, and V. V. Veeravalli, “Controlled sensing for
multihypothesis testing,” IEEE Trans. Autom. Control, vol. 58, no. 10,
pp. 2451–2464, Oct. 2013.
[22] M. Naghsvar and T. Javidi, “Sequentiality and adaptivity gains in active
hypothesis testing,” IEEE J. Sel. Topics Signal Process., vol. 7, no. 5,
pp. 768–782, Oct. 2013.
[23] M. Naghsvar and T. Javidi, “Active sequential hypothesis testing,” Ann.
Stat., vol. 41, no. 6, pp. 2703–2738, Dec. 2013.
[24] A. Tchamkerten and I. E. Telatar, “On the use of training sequences
for channel estimation,” IEEE Trans. Inf. Theory, vol. 52, no. 3,
pp. 1171–1176, Mar. 2006.
[25] A. Mahajan and S. Tatikonda, “Opportunistic capacity and error expo-
nent region for the compound channel with feedback,” IEEE Trans. Inf.
Theory, vol. 58, no. 7, pp. 4331–4341, Jul. 2012.
[26] B. Shradar and H. Permuter, “Feedback capacity of the compound
channel,” IEEE Trans. Inf. Theory, vol. 55, no. 8, pp. 3629–3644,
Aug. 2009.
[27] I. Csiszar and J. Körner, Information Theory: Coding Theorems for
Discrete Memoryless Systems. Cambridge, U.K.: Cambridge Univ. Press,
Jan. 2011.
[28] T. M. Cover and J. A. Thomas, Elements of Information Theory (Wiley
Series in Telecommunications and Signal Processing). New York, NY,
USA: Wiley-Intersci., 2006.
[29] R. Gallager. “Fixed composition arguments and lower bounds to error
probability.” Accessed: Oct. 8, 2022. [Online]. Available: http://web.mit.
edu/gallager/www/notes/notes5.pdf

Shi-Yuan Wang (Student Member, IEEE) received the B.Sc. degree in electrical engineering from National Taiwan University, Taiwan, in 2018. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Georgia Institute of Technology.

Meng-Che Chang (Student Member, IEEE) received the B.Sc. degree in electrical engineering and the M.S. degree in communication engineering from National Chiao-Tung University in 2014 and 2016, respectively. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Georgia Institute of Technology.

Tuna Erdoğan (Graduate Student Member, IEEE) received the B.S. degree in electrical and electronics engineering and the B.S. degree in physics from Bilkent University, Turkey, in 2021. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Georgia Institute of Technology.

Matthieu R. Bloch (Senior Member, IEEE) received the engineering degree from Supélec, Gif-sur-Yvette, France, the M.S. degree in electrical engineer-
ing from the Georgia Institute of Technology, Atlanta, in 2003, the first Ph.D. degree in engi-
neering science from the Université de Franche-
Comté, Besançon, France, in 2006, and the second
Ph.D. degree in electrical engineering from the
Georgia Institute of Technology in 2008, where he
is a Professor with the School of Electrical and
Computer Engineering. From 2008 to 2009, he
was a Postdoctoral Research Associate with the University of Notre Dame, South
Bend, IN, USA. Since July 2009, he has been on the faculty of the School of Electrical and Computer Engineering, and from 2009 to 2013, he was with Georgia Tech Europe. He is the coauthor of the textbook Physical-
Layer Security: From Information Theory to Security Engineering (Cambridge
University Press). His research interests are in the areas of information the-
ory, error-control coding, wireless communications, and cryptography. He is
the co-recipient of the IEEE Communications Society and IEEE Information
Theory Society 2011 Joint Paper Award. He has served on the organizing com-
mittee of several international conferences. He was the Chair of the Online
Committee of the IEEE Information Theory Society from 2011 to 2014,
and an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION
THEORY from 2016 to 2019 and again since 2021. He has been on the
Board of Governors of the IEEE Information Theory Society since 2016 and
currently serves as the President. He was an Associate Editor of the IEEE
TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY from 2019
to 2023.