EasyChair Preprint

№ 15149

On the Capacity of Scalar Gaussian Channels Subject to State Obfuscation

Omri Lev, Matthew Ho, Ligong Wang and Gregory Wornell

September 28, 2024

On the Capacity of Scalar Gaussian Channels Subject to State Obfuscation

Omri Lev*, Matthew Ho*, Ligong Wang†, and Gregory W. Wornell*
*Dept. EECS, MIT, Cambridge, MA 02139
†Dept. IT and EE, ETH Zurich, 8092 Zurich, Switzerland

***Abstract*—We study communication over the scalar Gaussian fading channel subject to a state-obfuscation constraint, which requires that the channel outputs and the fading coefficients be almost independent. We consider two cases for the fading coefficient: where it is independent and identically distributed in time, and where it is quasistatic, i.e., it is randomly generated but then remains the same during communication. For the transmitter, we study three different scenarios: where it only has access to the message; where it has channel-state information about the fading coefficient; and where it has access to feedback. We establish conditions for the communication capacity subject to obfuscation to be non-zero, and analyze this capacity in the high signal-to-noise ratio regime.**

***Index Terms*—Physical-layer security and privacy, Shannon theory, Gaussian channels, noncoherent communication.**

I. Introduction

In wireless communication, inherent imperfections of chipsets affect the transmitted signal, which, combined with the physical location of the transmitter, gives rise to a distinct radiometric fingerprint. This fingerprint can be employed by malicious parties to infer the transmitter's location. Recent studies propose practical fingerprinting solutions that can be readily implemented in commercial off-the-shelf devices [1], [2]. Channel state information (CSI)-based localization and user identification have been demonstrated to be possible in multiple scenarios, which could seriously threaten people's privacy at home or workplace [3]. Moreover, since these parameters can be intercepted by gaining remote access to the hardware (e.g., through unsecured internet connections) or by employing low-cost sensing nodes, malicious applications can potentially infer users' identities and locations remotely, exploiting their sensitive information for nefarious purposes. Consequently, a growing number of applications aim to design improved physical-layer waveforms that make such unauthorized eavesdropping tasks more difficult [3]–[7].

This paper addresses this issue from an information-theoretic perspective by trying to answer the next question: can we reliably communicate with a positive rate over a scalar fading channel in such a way that the output contains almost no information about the fading coefficients? We refer to this condition as *state obfuscation*, and call the maximum achievable communication rate under this condition the *obfuscated capacity*.

Our investigation builds upon a recent work on communication subject to state obfuscation over discrete channels by Wang and Wornell [8]. We aim to bridge the gap between the theoretical findings in [8] and physical channels by looking at several variants of the Gaussian fading channel. Our main focus is on the regime where signal-to-noise ratio (SNR) is high; in particular, we shall study the *multiplexing gain* in the obfuscated capacity in various scenarios.

The rest of the paper is organized as follows. The problem setup is presented in Sec. II, and background material is reviewed in Sec. III. The obfuscated capacity of the memoryless fading channel is analyzed in Sec. IV, and that of the quasistatic fading channel in Sec. V. We conclude the paper with remarks and future research directions in Sec. VI.

Notation: Random variables are denoted using sans-serif fonts like x, y, while their realizations are denoted with regular italic fonts like x, y. The joint distribution of (x, y) is denoted as $P_{\mathsf{x},\mathsf{y}}$. The phase of a complex number x is indicated by $\angle x$. We use j to denote the imaginary unit, i.e., $j \triangleq \sqrt{-1}$. The notation $[N]$ refers to the set $\{1, \ldots, N\}$. Throughout the paper, $o(1)$ terms are used to describe quantities that tend to zero as $\mathrm{SNR} \to \infty$. Mutual information is represented by $I(\cdot;\cdot)$, and differential entropy by $h(\cdot)$.

II. Channel and System Model

In this work, we consider variants of the scalar *fading* channel with additive Gaussian noise, described by

$$\mathsf{y}_n = \mathsf{h}_n \mathsf{x}_n + \mathsf{z}_n, \ n = 1, \ldots, N \tag{1}$$

where x_n and y_n are the transmitted and received signals at time n, respectively; the additive noises $\{\mathsf{z}_n\}$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with mean zero and variance $\frac{1}{\mathrm{SNR}}$. We assume $\mathsf{z}^N \perp\!\!\!\perp \mathsf{h}^N$ and we further assume that the fading coefficients have a bounded variance, namely $\mathbb{E}\left[|\mathsf{h}_n|^2\right] < \infty, \forall n \in [N]$. We consider two different scenarios regarding the distribution of the multiplicative gains $\{\mathsf{h}_n\}$. The first scenario is where the sequence $\{\mathsf{h}_n\}$ is i.i.d. and will be referred to as the *memoryless fading* case. The second scenario is where $\mathsf{h}_1 = \ldots = \mathsf{h}_N = \mathsf{h}$ and will be referred to as the *quasistatic fading* case. For the memoryless fading case, we denote by h a random variable whose distribution is the same as that of every h_n.

We now define the communication setting.

Encoder observes a message $\mathsf{M} \in \left[2^{RN}\right]$ and generates a codeword via a sequence of random mappings from M to $\mathsf{x}_n \in \mathbb{C}, \ n = 1, \ldots, N$. The codeword x^N is subject to an

This work was supported, in part, by ONR under Grant No. N000014-23-1-2803.

average input power constraint

$$\frac{1}{N}\sum_{n=1}^{N}\mathbb{E}\left[|\mathsf{x}_n|^2\right]\le 1$$

where the expectation is taken over the message, which is drawn uniformly at random, and over the random encoding mappings.

Some of our results are for the case where CSI is available at the encoder. This means the input symbol x_n is generated by a random mapping from the message M and the realization of the fading coefficients. The *causal* CSI case is where $\mathsf{x}_n = f_n\left(\mathsf{M},\mathsf{h}^n\right)$ and the *noncausal* CSI case is where $\mathsf{x}_n = f_n\left(\mathsf{M},\mathsf{h}^N\right)$.[1] In these cases, the average power is averaged also over the CSI.

We shall also consider cases where there is *feedback*, so $\mathsf{x}_n = f_n\left(\mathsf{M},\mathsf{y}^{n-1}\right)$. Here, the average input power will also be averaged over the channel outputs y^{n-1}. In the following, it shall be understood that, whenever feedback is not explicitly mentioned, we assume it is not present.

Decoder receives the channel outputs y^N and tries to decode the message M. We denote the decoded message by $\widehat{\mathsf{M}}$.

Obfuscation Constraint. The channel outputs are subject to an obfuscation constraint of the form of near independence between the sequence y^N and the sequence of the channel fading coefficients. For the memoryless fading channel, the constraint is

$$\lim_{N\to\infty}\frac{1}{N}I\left(\mathsf{y}^N;\mathsf{h}^N\right)=0 \tag{2}$$

while for the quasistatic case, the constraint is

$$\lim_{N\to\infty}I\left(\mathsf{y}^N;\mathsf{h}\right)=0. \tag{3}$$

As we shall see, the results in this paper hold when we replace the obfuscation constraints of (2) and (3) by the stronger constraints $I\left(\mathsf{y}^N;\mathsf{h}^N\right)=0,\forall N\ge 1$ and $I\left(\mathsf{y}^N;\mathsf{h}\right)=0,\forall N\ge 1$, respectively.

A rate R is said to be achievable if there exists a sequence of length-N codes such that the obfuscation constraint—(2) for the memoryless fading channel and (3) for the quasistatic fading channel—is satisfied and the probability of decoding error $P\left(\widehat{\mathsf{M}}\neq\mathsf{M}\right)$ approaches zero as $N\to\infty$. The *obfuscated capacity* is defined as the supremum of all achievable rates.

Remark 1. The memoryless and quasistatic models are similar, respectively, to the "IID state" and "constant state" cases of discrete channels studied in [8], whereas the encoders that we study correspond to the "with CSI" and "no CSI, stochastic encoder" cases in [8].

III. Background

A. The Non-Coherent Phase-Noise Channel

We shall use the capacity results on non-coherent phase-noise channels by Lapidoth [9] and Nuriyev *et al.* [10]. The memoryless phase-noise channel is the channel (1) with i.i.d. sequence $\{\mathsf{h}_n\}$ and when $|\mathsf{h}|$ is constant with probability (w.p.) 1. Its *non-coherent capacity*, denoted by $C_{\mathrm{nc}}(\mathrm{SNR})$, is the maximal achievable rate R in the same setting as we described in the previous section, but *without* the obfuscation constraint. (The terminology "non-coherent" refers to the fact that the decoder is oblivious of the values of the sequence h^N.)

Lemma 1 ([9])**.** *Consider the channel* (1) *under memoryless fading and assume that* $|\mathsf{h}|=\tilde{h}$ *for some positive constant* $\tilde{h}$ *w.p.* 1*, and that* $h\left(\angle\mathsf{h}\right)>-\infty$*. Then,*

$$\begin{aligned}C_{\mathrm{nc}}(\mathrm{SNR}) &= \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right]\le 1} I\left(\mathsf{x};\mathsf{y}\right)\\ &= \frac{1}{2}\log\left(\mathrm{SNR}\right)\cdot\left(1+o(1)\right).\end{aligned}$$

The quasistatic phase-noise channel is the channel (1) where $\mathsf{h}_n=\mathsf{h},\forall n\in[N]$ and where $|\mathsf{h}|=\tilde{h}$ w.p. 1. Its non-coherent capacity is defined similarly to that in the memoryless case.

Lemma 2. *Consider the channel* (1) *where* $\mathsf{h}_n=\mathsf{h},\forall n\in[N]$ *and assume that* $|\mathsf{h}|=\tilde{h}$ *w.p.* 1 *for some positive constant* $\tilde{h}$*. Then,*

$$C_{\mathrm{nc}}(\mathrm{SNR})=\log\left(\mathrm{SNR}\right)\cdot\left(1+o(1)\right).$$

Proof. The upper bound follows trivially by classical results on the capacity of the coherent Gaussian channel. The lower bound follows by using the results from [10, IV.C]. □

B. Independence in Addition

Lemma 3. *Let* $\mathsf{h},\mathsf{x},\mathsf{z}\in\mathbb{C}$ *be random variables s.t.* $\mathsf{z}\perp\!\!\!\perp(\mathsf{hx},\mathsf{h})$ *and let* $\mathsf{y}=\mathsf{hx}+\mathsf{z}$*. Then* $\mathsf{y}\perp\!\!\!\perp\mathsf{h}$ *if and only if* $\mathsf{hx}\perp\!\!\!\perp\mathsf{h}$.

Proof. Using the characteristic function to test independence between random variables [11, Ch. 7], $\mathsf{y}\perp\!\!\!\perp\mathsf{h}$ means

$$\phi_{\mathsf{y},\mathsf{h}}\left(v_1,v_2\right)=\phi_{\mathsf{y}}(v_1)\phi_{\mathsf{h}}(v_2) \tag{4}$$

where $\phi_{\mathsf{w}}(v)\triangleq\mathbb{E}\left[e^{j\mathsf{w}v}\right]$ and $\phi_{\mathsf{w}_1,\mathsf{w}_2}(v_1,v_2)\triangleq\mathbb{E}\left[e^{j(\mathsf{w}_1v_1+\mathsf{w}_2v_2)}\right]$ are characteristic functions of random variables. Using the independence between (h,hx) and z we get

$$\begin{aligned}\phi_{\mathsf{y},\mathsf{h}}\left(v_1,v_2\right)&=\phi_{\mathsf{z}}(v_1)\phi_{\mathsf{hx},\mathsf{h}}(v_1,v_2),\\ \phi_{\mathsf{y}}(v)&=\phi_{\mathsf{hx}}(v)\phi_{\mathsf{z}}(v).\end{aligned}$$

So a necessary and sufficient condition for (4) to hold is:

$$\phi_{\mathsf{hx},\mathsf{h}}(v_1,v_2)=\phi_{\mathsf{hx}}(v_1)\phi_{\mathsf{h}}(v_2)$$

which is equivalent to $\mathsf{hx}\perp\!\!\!\perp\mathsf{h}$. □

The next lemma is a consequence of Lem. 3.

Lemma 4. *Let* $\mathsf{h},\mathsf{x},\mathsf{z}\in\mathbb{C}$ *be random variables s.t.* $\mathsf{z}\perp\!\!\!\perp(\mathsf{hx},\mathsf{h})$ *and* $\mathsf{x}\perp\!\!\!\perp\mathsf{h}$ *and let* $\mathsf{y}=\mathsf{hx}+\mathsf{z}$*. Then* $\mathsf{y}\perp\!\!\!\perp\mathsf{h}$ *implies that either* $|\mathsf{h}|$ *is constant w.p.* 1 *or* $\mathbb{E}\left[|\mathsf{x}|^2\right]=0$*.*

Proof. By Lem. 3, $\mathsf{y}\perp\!\!\!\perp\mathsf{h}$ requires $\mathsf{hx}\perp\!\!\!\perp\mathsf{h}$, which further implies $|\mathsf{hx}|\perp\!\!\!\perp|\mathsf{h}|$. In particular, this requires that $\mathbb{E}\left[|\mathsf{hx}|^2\,\middle|\,|\mathsf{h}|\right]=\mathbb{E}\left[|\mathsf{x}|^2\right]|\mathsf{h}|^2$ be independent of $|\mathsf{h}|^2$, which is possible only if either $|\mathsf{h}|$ is constant w.p. 1 or $\mathbb{E}\left[|\mathsf{x}|^2\right]=0$. □

We shall also provide an alternative proof for Lem. 4 in App. A.

[1] There is no distinction between the causal and non-causal CSI cases when fading is quasistatic.

IV. Memoryless Fading

In this section, we analyze the obfuscated capacity of the memoryless fading Gaussian channel (1), which we denote by C^{IID}. We prove a single-letter upper bound on C^{IID}. We then show that this bound is tight as $\mathrm{SNR} \to \infty$. We end the section by calculating the asymptotic high-SNR obfuscated capacity with feedback and with CSI.

First note that the upper bound below is trivial, as it holds even without the obfuscation constraint:

$$C^{\mathrm{IID}} \leq \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1} I(\mathsf{x};\mathsf{y}). \tag{5}$$

We further have the following:

Lemma 5. *The capacity $C^{\mathrm{IID}} > 0$ only if $|\mathsf{h}|$ is constant w.p. 1.*

Proof. Repeating the proof of the converse of [8, Th. 3] and adding the power constraint we get that

$$C^{\mathrm{IID}} \leq \sup\ I(\mathsf{u};\mathsf{y})$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}} = P_{\mathsf{h}} P_{\mathsf{u}} P_{\mathsf{x}|\mathsf{u}} P_{\mathsf{y}|\mathsf{x},\mathsf{h}}$$

subject to

$$I(\mathsf{h};\mathsf{u},\mathsf{y}) = 0, \quad \mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1.$$

For a necessary condition for $C^{\mathrm{IID}} > 0$, we relax $I(\mathsf{h};\mathsf{u},\mathsf{y}) = 0$ to $I(\mathsf{h};\mathsf{y}) = 0$. By Lem. 4, this requires either $|\mathsf{h}|$ be constant w.p. 1 or $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$. Since $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$ will result in $I(\mathsf{u};\mathsf{y}) = 0$, we conclude that $C^{\mathrm{IID}} > 0$ only if $|\mathsf{h}|$ is constant w.p. 1. □

We now analyze C^{IID} in the regime where $\mathrm{SNR} \to \infty$.

Theorem 1. *Let y^N be the output of the channel (1) with $|\mathsf{h}| = \tilde{h} > 0$ w.p. 1. Then*

$$C^{\mathrm{IID}} \geq \frac{1}{2}\log(\mathrm{SNR}) \cdot (1 + o(1)). \tag{6}$$

If furthermore $h(\angle\mathsf{h}) > -\infty$, then

$$C^{\mathrm{IID}} = \frac{1}{2}\log(\mathrm{SNR}) \cdot (1 + o(1)). \tag{7}$$

Proof. We first prove (6). Consider the following strategy: pick a sequence $\tilde{\mathsf{x}}^N$, and map it to the input sequence x^N via

$$\mathsf{x}_n = e^{j\varphi_n}\tilde{\mathsf{x}}_n,$$

where $\{\varphi_n\}$ are i.i.d. uniformly over $[0, 2\pi)$ and independent of $\tilde{\mathsf{x}}^N$. Then we have the following "effective" channel from $\tilde{\mathsf{x}}$ to y:

$$\mathsf{y}_n = \mathsf{h}_n e^{j\varphi_n}\tilde{\mathsf{x}}_n + \mathsf{z}_n \triangleq \tilde{\mathsf{h}}_n\tilde{\mathsf{x}}_n + \mathsf{z}_n. \tag{8}$$

By [12, Ch. 4], $\{\angle\tilde{\mathsf{h}}_n\}$ is i.i.d. uniformly over $[0, 2\pi)$ and independent of $\{\angle\mathsf{h}_n\}$. Since $\left|\tilde{\mathsf{h}}_n\right| = \tilde{h}$ w.p. 1, this further implies that $\tilde{\mathsf{h}}^N \perp\!\!\!\perp \mathsf{h}^N$ and, irrespectively of the distribution of $\tilde{\mathsf{x}}^N$, $\{\tilde{\mathsf{h}}_n\tilde{\mathsf{x}}_n\} \perp\!\!\!\perp \mathsf{h}^N$, which in turn implies $\mathsf{y}^N \perp\!\!\!\perp \mathsf{h}^N$, so the obfuscation constraint is satisfied.

We can thus code over the channel from $\tilde{\mathsf{x}}$ to y given by (8) while ignoring the obfuscation constraint. The channel (8) is a phase-noise channel where the phases are i.i.d. uniformly over $[0, 2\pi)$. Its high-SNR capacity is given by [9, Sec. IV] as $\frac{1}{2}\log(\mathrm{SNR})(1 + o(1))$.

To prove (7), we note that whenever $|\mathsf{h}|$ is constant, the right-hand side of (5) is the non-coherent capacity of the memoryless scalar phase-noise Gaussian channel, which by Lem. 1 is given by $\frac{1}{2}\log(\mathrm{SNR}) \cdot (1 + o(1))$ whenever $h(\angle\mathsf{h}) > -\infty$. □

Remark 2 (Multiplexing Gain). When $h(\angle\mathsf{h}) = -\infty$, (7) may not hold. To see this, consider the example where $\mathsf{h} \in \{\pm 1\}$. Obfuscation can be achieved by multiplying the input symbols by a sequence a_n that is i.i.d. uniformly over $\{\pm 1\}$. Roughly speaking, we can transmit two real symbols per channel use (the real and the imaginary parts of the input symbol), resulting in a multiplexing gain of 2 as opposed to 1 in (7).

A. Memoryless fading with feedback

We now analyze the obfuscated capacity of the memoryless fading channel with feedback. We will show that in the regime where $\mathrm{SNR} \to \infty$ feedback does not increase the obfuscated capacity.

Theorem 2. *Whenever $h(\angle\mathsf{h}) > -\infty$, feedback does not increase the asymptotic high-SNR obfuscated capacity of the memoryless fading channel without CSI.*

Proof. We note that when we add feedback, the next Markov relationships hold

$$\begin{gathered}\left(\mathsf{y}^{i-1}, \mathsf{M}\right) \text{—} \mathsf{x}_i \text{—} \mathsf{y}_i,\ \forall i \in 1, \ldots, N, \\ \mathsf{M} \text{—} \mathsf{y}^N \text{—} \widehat{\mathsf{M}}.\end{gathered} \tag{9}$$

Thus, by defining the auxiliary variable $\mathsf{u}_i \triangleq \left(\mathsf{M}, \mathsf{y}^{i-1}\right)$ the same analysis of [8, Th. 3] and Lem. 5 still holds and we get the same capacity expressions as without feedback. □

Remark 3. We note that the proof of Th. 2 does not use the fact that the underlying channel is Gaussian, therefore holds for any memoryless channel. We further note that in the discrete case, the same achievability from [8, Th. 3] can be used, showing that feedback does not increase the capacity.

B. Memoryless fading with CSI

We next analyze the case where the encoder has access to (causal or non-causal) CSI, as defined in Sec. II. The capacity in this case is denoted as $C^{\mathrm{IID}}_{\mathrm{CSI}}$.[2]

Lemma 6. *The capacity $C^{\mathrm{IID}}_{\mathrm{CSI}}$ is greater than zero only if $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$.*

Proof. Repeating the proof of [8, Th. 1] and adding the power constraint, we get that the obfuscated capacity for memoryless fading with either causal or non-causal CSI is upper-bounded by

$$C^{\mathrm{IID}}_{\mathrm{CSI}} \leq \sup\ I(\mathsf{u};\mathsf{y})$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}} = P_{\mathsf{h}} P_{\mathsf{u}} P_{\mathsf{x}|\mathsf{u},\mathsf{h}} P_{\mathsf{y}|\mathsf{x},\mathsf{h}}$$

[2] We do not claim that the capacities with causal and with non-causal CSI are equal, so we are abusing notation when we denote these two capacities with the same expression. What we mean is that the relevant claims in the following hold for both capacities.

subject to

$$I(\mathsf{h};\mathsf{u},\mathsf{y})=0,\quad \mathbb{E}\left[|\mathsf{x}|^2\right]\le 1.$$

By Lem. 3, $I(\mathsf{h};\mathsf{u},\mathsf{y})=0$ implies $\mathsf{h}\mathsf{x}\perp\!\!\!\perp\mathsf{h}$. Thus, we have that $c\triangleq\mathbb{E}\left[|\mathsf{h}\mathsf{x}|^2\middle||\mathsf{h}|\right]=|\mathsf{h}|^2\,\mathbb{E}\left[|\mathsf{x}|^2\middle||\mathsf{h}|\right]$ is constant. This implies

$$1\ge\mathbb{E}\left[|\mathsf{x}|^2\right]=\mathbb{E}\left[\mathbb{E}\left[|\mathsf{x}|^2\middle||\mathsf{h}|\right]\right]=\mathbb{E}\left[\frac{c}{|\mathsf{h}|^2}\right]=c\cdot\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right].$$

Thus, whenever $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right]=\infty$, we must have $c=0$, i.e., $|\mathsf{h}\mathsf{x}|=0$ w.p. 1, which implies $I(\mathsf{u};\mathsf{y})=0$. □

Theorem 3. *If* $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right]<\infty$*, then*

$$C_{\mathrm{CSI}}^{\mathrm{IID}}=\log(\mathrm{SNR})\cdot(1+o(1)).$$

Proof. We first prove the converse. Using Cauchy-Schwarz inequality, we note that

$$\mathbb{E}\left[|\mathsf{h}\mathsf{x}|^2\right]\le\mathbb{E}\left[|\mathsf{h}|^2\right]\cdot\mathbb{E}\left[|\mathsf{x}|^2\right]\le\mathbb{E}\left[|\mathsf{h}|^2\right].$$

Since (u,h)—$\mathsf{h}\mathsf{x}$—y forms a Markov chain, we can upper-bound the capacity by that of the non-fading Gaussian channel

$$\mathsf{y}=\mathsf{x}^\star+\mathsf{z}$$

with the power constraint $\mathbb{E}\left[|\mathsf{x}^\star|^2\right]\le\mathbb{E}\left[|\mathsf{h}|^2\right]$. Therefore

$$\begin{aligned}C_{\mathrm{CSI}}^{\mathrm{IID}}&\le\log\left(\mathbb{E}\left[|\mathsf{h}|^2\right]\cdot\mathrm{SNR}\right)\cdot(1+o(1))\\&=\log(\mathrm{SNR})\cdot(1+o(1)).\end{aligned}$$

Now we provide a construction that achieves the same asymptotic behavior. Let $\bar{\mathsf{h}}_n\triangleq\frac{1}{\mathsf{h}_n\sqrt{\mathbb{E}\left[1/|\mathsf{h}|^2\right]}}$ and let the input sequence x^N be given by $\mathsf{x}_n=\bar{\mathsf{h}}_n\tilde{\mathsf{x}}_n$. Since $\mathsf{y}_n=\frac{1}{\sqrt{\mathbb{E}\left[1/|\mathsf{h}|^2\right]}}\tilde{\mathsf{x}}_n+\mathsf{z}_n$, we have $\mathsf{y}^N\perp\!\!\!\perp\mathsf{h}^N$ and the obfuscation constraint is satisfied irrespectively of the distribution of $\tilde{\mathsf{x}}^N$. We then note that

$$\mathbb{E}\left[|\mathsf{x}_n|^2\right]=\mathbb{E}\left[|\bar{\mathsf{h}}_n|^2\right]\mathbb{E}\left[|\tilde{\mathsf{x}}_n|^2\right]=\mathbb{E}\left[|\tilde{\mathsf{x}}_n|^2\right].$$

We can thus use the channel from $\tilde{\mathsf{x}}$ to y as a (non-fading) Gaussian channel with unit power constraint, whose high-SNR capacity is given by $\log(\mathrm{SNR})\cdot(1+o(1))$. □

V. Quasistatic Fading

We now analyze the obfuscated capacity of the Gaussian channel (1) with quasistatic fading, which we denote by C^{quasi}. The proofs follow the same lines as for memoryless fading. We first show that the $|\mathsf{h}|$ must be constant for the obfuscated capacity to be non-zero. Then we will use the capacity results of the block-noncoherent channel to derive the capacity. We also analyze the cases with feedback and with CSI.

Theorem 4. *The obfuscated capacity of the Gaussian channel with quasistatic fading and without CSI or feedback is greater than zero only if* $|\mathsf{h}|$ *is constant w.p.* 1 *and is given by*

$$C^{\mathrm{quasi}}=\log(\mathrm{SNR})\cdot(1+o(1)).$$

Proof. Using the same arguments as in [8, Th. 6] we can show

$$C^{\mathrm{quasi}}\le\sup\ I(\mathsf{u};\mathsf{y})$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}}=P_{\mathsf{h}}P_{\mathsf{u}}P_{\mathsf{x}|\mathsf{u}}P_{\mathsf{y}|\mathsf{x},\mathsf{h}}$$

subject to

$$I(\mathsf{h};\mathsf{y})=0,\quad\mathbb{E}\left[|\mathsf{x}|^2\right]\le 1.$$

By the same reasoning as in the proof of Lem. 5 we conclude that, for C^{quasi} to be positive, $|\mathsf{h}|$ must be constant w.p. 1.

We note that C^{quasi} when $|\mathsf{h}|=\bar{h}$ w.p. 1 is upper-bounded by the capacity of a non-fading Gaussian channel whose SNR is $\left|\bar{h}\right|^2\cdot\mathrm{SNR}$, the latter at high SNR being

$$\log\left(\left|\bar{h}\right|^2\mathrm{SNR}\right)(1+o(1))=\log(\mathrm{SNR})(1+o(1)).$$

We prove an asymptotically matching lower bound. Let the input sequence x^N be given by $\mathsf{x}_n=e^{j\varphi}\tilde{\mathsf{x}}_n$, where φ is uniform over $[0,2\pi)$ and independent of $\tilde{\mathsf{x}}^N$. The channel then becomes

$$\mathsf{y}_n=\tilde{\mathsf{h}}\tilde{\mathsf{x}}_n+z_n,\quad n\in[N]$$

where $\tilde{\mathsf{h}}\triangleq\mathsf{h}e^{j\varphi}$ is uniform on a circle and is independent of h (provided that $|\mathsf{h}|=\bar{h}$ for some constant $\bar{h}$ w.p. 1). It then follows that $\mathsf{h}\perp\!\!\!\perp\mathsf{y}^N$, so the obfuscation constraint is satisfied. The channel with input $\tilde{\mathsf{x}}^N$ and output y^N is a block non-coherent phase-noise channel, whose high-SNR capacity is $\log(\mathrm{SNR})\cdot(1+o(1))$ [10, Sec. IV.C]. □

Remark 4 (Deterministic Encoder). Th. 1 and Th. 4 both concern the case where the encoder can be stochastic, i.e., it can employ local randomness that is not shared with the receiver. In [8] the authors distinguish between the cases of stochastic encoder and deterministic encoder, the latter meaning that the mapping from the message to the input sequence must be deterministic. For our channel (1) with either memoryless or quasistatic fading, the obfuscated capacity with a deterministic encoder is zero (as long as there is fading). To see this, we note that the converse proofs of [8, Th. 2 and 6] are still valid, so the obfuscated capacity of interest is upper-bounded by $I(\mathsf{x};\mathsf{y})$ subject to $I(\mathsf{h};\mathsf{x},\mathsf{y})=0$. But $I(\mathsf{h};\mathsf{x},\mathsf{y})$ can be zero only when either $\mathsf{x}=0$ w.p. 1 or h is constant. The former clearly implies $I(\mathsf{x};\mathsf{y})=0$ so no positive rate can be achieved, and the latter is the case where there is no fading at all.

A. Quasistatic fading with feedback

Theorem 5. *The obfuscated capacity of the quasistatic fading channel with feedback and without CSI is greater than zero only if* $|\mathsf{h}|$ *is constant w.p.* 1 *and is given by*

$$C_{\mathrm{fb}}^{\mathrm{quasi}}=\log(\mathrm{SNR})\cdot(1+o(1)).$$

Proof. Similarly to Th. 2, the same Markov relations (9) hold in the quasistatic case. Thus, by defining the auxiliary variable $\mathsf{u}_i\triangleq\left(\mathsf{M},\mathsf{y}^{i-1}\right)$ the same converse of Th. 4 still holds, and thus we conclude that $|\mathsf{h}|$ must be constant w.p. 1 for the obfuscated capacity to be nonzero. That it cannot be larger than $\log(\mathrm{SNR})\cdot(1+o(1))$ follows because the latter is the asymptotic high-SNR capacity when the decoder knows h and when there is no obfuscation constraint. □

B. Quasistatic fading with CSI

We denote the obfuscated capacity under quasistatic fading with CSI (and without feedback) by $C_{\mathrm{CSI}}^{\mathrm{quasi}}$. Assume, like in Th. 3, that $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$. The same coding scheme from Th. 3 can be used, and thus $C_{\mathrm{CSI}}^{\mathrm{quasi}} \geq \log(\mathrm{SNR}) \cdot (1 + o(1))$. On the other hand, $C_{\mathrm{CSI}}^{\mathrm{quasi}}$ cannot exceed the capacity for the same channel without the obfuscation condition, therefore $C_{\mathrm{CSI}}^{\mathrm{quasi}} \leq \log(\mathrm{SNR}) \cdot (1 + o(1))$. Thus, asymptotically, $C_{\mathrm{CSI}}^{\mathrm{quasi}}$ coincides with $C_{\mathrm{CSI}}^{\mathrm{IID}}$, the capacity in the memoryless case with CSI.

Remark 5. To achieve the above asymptotic capacity, the average input power of the transmitted codeword needs to depend on the realization of $|\mathsf{h}|$. Due to the quasistatic nature of the channel, there is a significant outage probability (which depends on the distribution of $|\mathsf{h}|$) for the average power of the input sequence to exceed 1.

Remark 6. Unlike in the memoryless fading case, we have not shown that $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$ is a necessary condition for $C_{\mathrm{CSI}}^{\mathrm{quasi}}$ to be positive. This is because the converse part of [8, Th. 5] does not apply when the state (in our case h) is continuous.

VI. Concluding Remarks

For both memoryless and quasistatic fading, without encoder CSI, the obfuscated capacity can only be positive if the channel is a phase-noise channel. This is also true when there is feedback. With CSI, however, we have positive obfuscated capacity (for both i.i.d. and quasistatic fading) as long as $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$.

For memoryless fading, when the encoder does not have CSI (but may possibly have feedback), and when the obfuscated capacity is positive, the multiplexing gain is in general 1 (assuming $h(\angle\mathsf{h}) > -\infty$). When the encoder has CSI, the multiplexing gain becomes 2, which is also the multiplexing gain in all quasistatic fading cases. Thus, whenever the obfuscated capacity is positive, the multiplexing gain is essentially the same as though there were no obfuscation constraint.

Developing the obfuscated capacity of channels with more complex temporal structures (e.g., when h^N is a stationary process) or other variants of the scalar Gaussian channel (for example, the inter-symbol-interference channel) is the subject of ongoing research, as is characterizing the obfuscated capacity for multi-input multi-output (MIMO) channels, which arise when multi-antenna transmitters and/or receivers are involved.

Appendix A
Alternative Proof of Lem. 4

We now provide an alternative proof to Lem. 4. This proof does not require assumptions on the second moments of $|\mathsf{h}|$ nor $|\mathsf{x}|$. We start by giving an alternative way to prove the claim that $|\mathsf{hx}| \perp\!\!\!\perp |\mathsf{h}|$ implies that $|\mathsf{h}|$ is constant w.p. 1.

Lemma 7. *Let $|\mathsf{h}|$ and $|\mathsf{x}|$ be nonnegative-valued random variables satisfying $|\mathsf{h}| \perp\!\!\!\perp |\mathsf{x}|$, $|\mathsf{hx}| \perp\!\!\!\perp |\mathsf{h}|$, and $P(|\mathsf{h}| > 0, |\mathsf{x}| > 0) > 0$. Then, we must have that $|\mathsf{h}|$ is constant w.p. 1.*

Proof. Assume for the sake of contradiction that $|\mathsf{h}|$ is not constant w.p. 1, so there exists some a satisfying $0 < P(|\mathsf{h}| \leq a) < 1$. By right-continuity of CDFs, we have that there exists some $\varepsilon > 0$ such that $P(|\mathsf{h}| \leq a + 2\varepsilon) < 1$. Then, choose h to satisfy the property that

$$P\left(|\mathsf{x}| \in \left(\frac{a+\varepsilon}{a+2\varepsilon}h, \frac{a+\varepsilon}{a}h\right)\right) > 0$$

Using independence of $|\mathsf{h}|$ and $|\mathsf{x}|$ we obtain that

$$\begin{aligned} P\left(|\mathsf{hx}| \leq h(a+\varepsilon) \mid |\mathsf{h}| \leq a\right) &= P\left(|\mathsf{x}| \leq \frac{a+\varepsilon}{|\mathsf{h}|}h \middle| |\mathsf{h}| \leq a\right) \\ &\geq P\left(|\mathsf{x}| \leq \frac{a+\varepsilon}{a}h\right) \end{aligned}$$

and similarly

$$P\left(|\mathsf{hx}| \leq h(a+\varepsilon) \mid |\mathsf{h}| > a + 2\varepsilon\right) \leq P\left(|\mathsf{x}| < \frac{a+\varepsilon}{a+2\varepsilon}h\right).$$

By our choice of h we have that these two probabilities are not equal, and by our choice of a we have that the events $|\mathsf{h}| \leq a$ and $|\mathsf{h}| > a + 2\varepsilon$ happen with nonzero probability. Then $|\mathsf{hx}| \not\perp\!\!\!\perp |\mathsf{h}|$, which is a contradiction, so we conclude that $|\mathsf{h}|$ must be constant almost surely, or otherwise the events should have the same probability for any corresponding a, h and ϵ, which is possible only if $|\mathsf{x}| = 0$ w.p. 1, leading to $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$. □

We note that Lem. 4 follows by combining Lem. 7 with Lem. 3.

References

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Comm.*, vol. 17, no. 5, pp. 56–62, 2010.

[2] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE IoT. Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[3] M. Cominelli, F. Gringoli, and R. L. Cigno, "On the properties of device-free multi-point CSI localization and its obfuscation," *Computer Communications*, vol. 189, pp. 67–78, 2022.

[4] L. F. Abanto-Leon, A. Bäuml, G. H. Sim, M. Hollick, and A. Asadi, "Stay connected, leave no trace: Enhancing security and privacy in WiFi via obfuscating radiometric fingerprints," *Proc. of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 3, pp. 1–31, 2020.

[5] M. Cominelli, F. Kosterhon, F. Gringoli, R. Lo Cigno, and A. Asadi, "IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios," *Computer Networks*, vol. 191, p. 107970, 2021.

[6] H. Givehchian, N. Bhaskar, A. Redding, H. Zhao, A. Schulman, and D. Bharadia, "Practical obfuscation of BLE physical-layer fingerprints on mobile devices," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2023, pp. 73–73.

[7] R. Ayyalasomayajula, A. Arun, W. Sun, and D. Bharadia, "Users are closer than they appear: protecting user location from WiFi APs," in *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, 2023, pp. 124–130.

[8] L. Wang and G. W. Wornell, "Communication subject to state obfuscation," in *the International Zurich Seminar on Communication (IZS)*. ETH Zurich, 2020, pp. 78–82.

[9] A. Lapidoth, "On phase noise channels at high SNR," in *Proc. IEEE Info. Theory Workshop (ITW)*, 2002, pp. 1–4.

[10] R. Nuriyev and A. Anastasopoulos, "Capacity and coding for the block-independent noncoherent awgn channel," *IEEE transactions on information theory*, vol. 51, no. 3, pp. 866–883, 2005.

[11] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY: McGraw-Hill, 1965.

[12] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge University Press, 2014.