Secrecy Metrics over Random Gaussian SIMOME and MIMOME Channels

Clément Leroy, Tarak Arbi, Benoît Geller
ENSTA, Institut Polytechnique de Paris, France
{firstname.lastname}@ensta-paris.fr

Olivier Rioul
LTCI, Télécom Paris, Institut Polytechnique de Paris, France
olivier.rioul@telecom-paris.fr

***Abstract*—The achievable secrecy of time-invariant wireless channels is typically characterized by the secrecy capacity of the communication system, whose mathematical expression is well established. However, in most practical scenarios, channels cannot be assumed to remain constant or to be perfectly known at both the transmitter and the legitimate receiver. In such cases, no closed-form expression for the secrecy capacity is available.**

To address this, several metrics are studied, that characterize secrecy in random channel environments: *Ergodic Secrecy Rate* (*ESR*), *Ergodic Positive Secrecy Rate* (*EPSR*), and *Secrecy Outage Probability* (*SOP*). We derive the optimal values of these metrics for SIMOME channels (Single-Input, Multiple-Output, Multiple-Eavesdropper) and various MIMOME (Multiple-Input, Multiple-Output, Multiple-Eavesdropper) scenarios.

I. Introduction

In modern wireless networks, where devices operate in open and dynamic environments, ensuring confidentiality at the physical layer has become a critical complement to higher-layer cryptographic techniques. Since Wyner's seminal work [1] on the wiretap channel, and the subsequent contributions by Csiszár and Körner [2], it is known that perfect secrecy can be achieved through channel coding over wireless channels with an eavesdropper, provided that the legitimate receiver's channel is *better* than that of the eavesdropper. However, the secrecy gain obtained through encoding comes at the cost of a rate loss, and the resulting maximum reliable secure transmission rate is defined as the secrecy capacity [2].

The characterization of secrecy capacity over wireless channels was independently initiated by Khisti and Wornell [3], and by Oggier and Hassibi [4]. They showed that the optimal input distribution is Gaussian and does not require any auxiliary precoding. Subsequently, several closed-form expressions for the secrecy capacity have been proposed, characterizing the optimal covariance matrix of the Gaussian input [5], [6].

However, achieving the secrecy capacity requires perfect knowledge of the instantaneous channel state information, which is often impractical. More realistic communication models consider random channel states, accounting for imperfect channel estimation, fast fading, and unknown eavesdropper locations. In such scenarios, the secrecy capacity is expressed as an average of instantaneous secrecy rates, often referred to as the *Ergodic Secrecy Rate*. In general, no closed-form expression is known, and only bounds have been derived under very specific assumptions on the channel distributions [7], [8].

Moreover, secrecy capacity is not the only relevant metric for assessing system security. Other metrics, such as *Ergodic Positive Secrecy Rate* and *Secrecy Outage Probability*, have also been extensively studied in similar contexts. However, most existing works rely on restrictive assumptions on the signaling strategy, such as limiting the analysis to non-precoded Gaussian inputs [9]–[12], or joint Gaussian input and artificial noise [13]–[15]. While such assumptions are optimal in certain settings, their general validity remains unclear, especially in more complex and realistic channel models. A unified framework for optimizing secrecy metrics without restrictive assumptions on the input distribution is still lacking.

In this paper, we present a detailed analysis of various secrecy metrics and derive their optimal values with respect to the input distribution. Our approach is both original and general, as it does not restrict the optimization to Gaussian inputs or to schemes combining artificial noise with Gaussian signaling. For SIMOME channels and a broad class of MIMOME channels, we show that most optimal metrics are indeed achieved using a Gaussian input without any auxiliary precoding. This result suggests that, despite the apparent complexity of random channel models, the structure of optimal signaling strategies remains simple for many channels statistics. However, some metrics are maximized with more complex inputs.

The remainder of this paper is organized as follows. Section II introduces the system model, including the communication model, the secrecy metrics under consideration, and the partial ordering of channels. Section III is devoted to the optimization of the *Secrecy Outage Probability* (*SOP*) and the *Ergodic Positive Secrecy Rate* (*EPSR*) for both a broad class of MIMOME channels and SIMOME channels. Section IV addresses the optimization of the *Ergodic Secrecy Rate* (*ESR*) in the same settings. Section IV-C provides bounds on the maximum achievable *ESR*. Section V concludes.

Due to lack of space, some proofs are outlined in this paper and for full technical details, the reader is referred to its extended version available online [16].

II. System model

A. Communication model

Consider a wireless communication system consisting of a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve). Bob is equipped with N_B receive antennas,

while Eve has N_E receive antennas. In SIMOME channels, Alice has a single transmit antenna ($N_A = 1$), whereas in MIMOME channels, Alice is equipped with an arbitrary number of transmit antennas ($N_A \geq 1$).

Alice wishes to transmit a message u, drawn from an arbitrary set $\mathcal{U}$, which is encoded into a signal $\mathbf{x}$. The transmitted signal $\mathbf{x}$ is modeled as a complex random vector in $\mathbb{C}^{N_A}$. Bob observes $\mathbf{y} \in \mathbb{C}^{N_B}$ given by

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}_B, \tag{1}$$

while Eve observes $\mathbf{z} \in \mathbb{C}^{N_E}$ given by

$$\mathbf{z} = \mathbf{G}\mathbf{x} + \mathbf{w}_E, \tag{2}$$

where $\mathbf{w}_B$ and $\mathbf{w}_E$ are independent, identically distributed (i.i.d.) circularly symmetric complex Gaussian noise vectors with identity covariance matrix $\mathbf{I}$. The matrix $\mathbf{H} \in \mathbb{C}^{N_B \times N_A}$ (respectively, $\mathbf{G} \in \mathbb{C}^{N_E \times N_A}$) represents the channel between Alice and Bob (resp. Alice and Eve), and is modeled as a random matrix with distribution $p_{\mathbf{H}}$ (resp. $p_{\mathbf{G}}$). These distributions characterize the channel statistics and capture the randomness of the propagation environment. The system model is illustrated in Figure 1. Since the instantaneous channel state information is unknown at the transmitter, the random matrices $\mathbf{H}$ and $\mathbf{G}$ are assumed to be independent of both message u and transmitted signal $\mathbf{x}$.

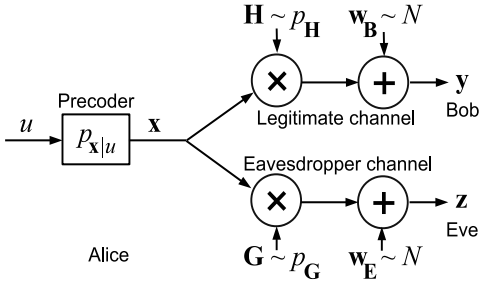

Fig. 1: System Model

B. Secrecy Metrics

1) Ergodic Secrecy Rate (ESR)

The natural extension of secrecy capacity to random wireless channels is the *Ergodic Secrecy Rate* (ESR). When the receiver knows the instantaneous channel state while the transmitter does not, the channel can be viewed as having outputs that include both the received signal and the channel states. The secrecy rate can thus be expressed as

$$\begin{aligned} \textit{ESR} &\triangleq I(u;\mathbf{y},\mathbf{H},\mathbf{G}) - I(u;\mathbf{z},\mathbf{H},\mathbf{G}) && (3)\\ &= I(u;\mathbf{y}|\mathbf{H},\mathbf{G}) - I(u;\mathbf{z}|\mathbf{H},\mathbf{G}) && (4)\\ &= \mathbb{E}_{\mathbf{H},\mathbf{G}}\left[I(u;\mathbf{y}) - I(u;\mathbf{z})\right], && (5)\end{aligned}$$

where $I(\cdot;\cdot)$ denotes Shannon's mutual information, (4) follows from the independence of $\mathbf{H}$, $\mathbf{G}$ from u and (5) follows from the definition of conditional mutual information. The corresponding secrecy capacity for the random channel model is

$$C_S \triangleq \max_{p_{u,\mathbf{x}}} [\textit{ESR}]. \tag{6}$$

2) Ergodic Positive Secrecy Rate (EPSR)

When the transmitter has access to the instantaneous channel state in a fast-fading environment, an on/off transmission strategy can be employed: Transmission occurs only when the instantaneous secrecy rate is positive, and is suspended otherwise. The resulting secrecy rate is the expectation of the positive part of the instantaneous secrecy rate:

$$\textit{EPSR} \triangleq \mathbb{E}_{\mathbf{H},\mathbf{G}}\left[\left(I(u;\mathbf{y}) - I(u;\mathbf{z})\right)^+\right], \tag{7}$$

where $x^+ \triangleq \max(0,x)$.

3) Secrecy Outage Probability (SOP)

When the eavesdropper's channel state is unknown to the legitimate parties, the transmitter selects a fixed coding rate r. If this rate exceeds the instantaneous secrecy rate, either some information may be leaked to the eavesdropper or decoding errors may occur at the legitimate receiver. For any given rate $r \geq 0$, the *Secrecy Outage Probability* (*SOP*) is defined as

$$\textit{SOP}(r) \triangleq \mathbb{P}\left[I(u;\mathbf{y}) - I(u;\mathbf{z}) < r\right]. \tag{8}$$

C. Partial ordering of channels

Over non-varying channels, the expression of the secrecy capacity may be simplified when channels satisfy some partial *ordering*: When the main channel is *more capable* or is *less noisy* than the eavesdropper's channel (according to the definition in [2], [17]), secrecy capacity is achieved with no auxiliary precoding. Additional simplifications arise in the case of *degraded* channels. Since such classical channel orderings are for nonrandom channels, it is necessary to extend these to random channels for the secrecy metrics considered in this work. Therefore, we define the following channel orderings.

Less noisy on average: An ergodic channel given by $\mathbf{H}$ is said to be *less noisy on average* than $\mathbf{G}$ (or $\mathbf{G}$ is *noisier on average* than $\mathbf{H}$) if for any auxiliary precoder $u \to \mathbf{x}$, one has the inequality

$$\mathbb{E}_{\mathbf{H}}\left[I(u;\mathbf{y})\right] \geq \mathbb{E}_{\mathbf{G}}\left[I(u;\mathbf{z})\right]. \tag{9}$$

This definition is obtained by averaging the inequality defining the classical *less noisy* order, over all instantaneous channel states.

Uniformly less noisy: An ergodic channel given by $\mathbf{H}$ is said to be *uniformly less noisy* than $\mathbf{G}$ (or $\mathbf{G}$ is *uniformly noisier* than $\mathbf{H}$) if for any $(\mathbf{H}_0,\mathbf{G}_0)$ in the support of distribution $p_{\mathbf{H},\mathbf{G}}$ and for any auxiliary precoder $u \to \mathbf{x}$, one has the inequality

$$I(u;\mathbf{y}|\mathbf{H}=\mathbf{H}_0) \geq I(u;\mathbf{z}|\mathbf{G}=\mathbf{G}_0). \tag{10}$$

It is easily seen that if $\mathbf{H}$ is *uniformly* less noisy than $\mathbf{G}$, then it is also less noisy *on average*. Besides, if the legitimate receiver output $\mathbf{y}$ is passed through another channel whose output is the eavesdropper signal $\mathbf{z}$, then channel $\mathbf{G}$ can be expressed as the cascade of two channels, $\mathbf{H}$ and $\tilde{\mathbf{G}}$, i.e., $\mathbf{G} = \mathbf{H}\tilde{\mathbf{G}}$. In this simple case, the eavesdropper channel is a degraded version of the legitimate channel, and it is easily seen that $\mathbf{H}$ is both *less noisy on average* and *uniformly less noisy* than $\mathbf{G}$.

III. Optimization of Secrecy Outage Probability and Ergodic Positive Secrecy Rate

A. MIMOME channel

Consider the general MIMOME channel, where Alice, Bob, and Eve are equipped with arbitrary numbers of antennas. We show that, under the assumption that the legitimate channel is *uniformly less noisy* than the eavesdropper's, a Gaussian input without auxiliary precoding is optimal: It simultaneously minimizes the *SOP* and maximizes the *EPSR*.

Theorem 1. *If the ergodic channel* $\mathbf{H}$ *is uniformly less noisy than the ergodic channel* $\mathbf{G}$*, then the input distribution* $p_{u,\mathbf{x}}$ *minimizing the SOP with a fixed input covariance matrix* $\mathbf{K_x}$ *is the one for which* $u \equiv \mathbf{x}$ *and* $\mathbf{x}$ *is a complex Gaussian random variable. That is, for any* $r \geq 0$*,*

$$\min_{\substack{p_{u,\mathbf{x}} \\ \mathrm{cov}[\mathbf{x}]=\mathbf{K_x}}} \mathit{SOP}(r) = \mathbb{P}\Big[\log \frac{\det(\mathbf{I}+\mathbf{H}^\dagger\mathbf{K_x}\mathbf{H})}{\det(\mathbf{I}+\mathbf{G}^\dagger\mathbf{K_x}\mathbf{G})} < r\Big]. \quad (11)$$

Note that in Theorem 1, $\mathbf{K_x}$ determines the input power since its trace $\mathrm{Tr}(\mathbf{K_x})$ is the total transmitting power. In this theorem, as well as in the following ones, the input covariance is fixed; a general optimization of the metric would also involve optimizing over $\mathbf{K_x}$. This is carried out on a case-by-case basis, as it strongly depends on the channel statistics $p_{\mathbf{H}}$ and $p_{\mathbf{G}}$. However, in many cases, such as Rayleigh fading [16], symmetries in the channel statistics imply that the optimal $\mathbf{K_x}$ is proportional to $\mathbf{I}$.

To prove the Theorem, we need the following lemma.

Lemma 1. *If for all* $u \to \mathbf{x}$*,*

$$I(u; \mathbf{H}_0\mathbf{x} + \mathbf{w}_B) \geq I(u; \mathbf{G}_0\mathbf{x} + \mathbf{w}_E) \quad (12)$$

then

$$\max_{\substack{p_{u,\mathbf{x}} \\ \mathrm{cov}[\mathbf{x}]=\mathbf{K_x}}} [I(u;\mathbf{y}) - I(u;\mathbf{z})] = I(\mathbf{x}_g;\mathbf{y}) - I(\mathbf{x}_g;\mathbf{z}), \quad (13)$$

where $\mathbf{x}_g$ *is the Gaussian vector with covariance matrix* $\mathbf{K_x}$*.*

Proof Outline (see [16] for details). Using the simplification of the secrecy capacity for *less noisy* channels [2], we obtain

$$I(u;\mathbf{y}) - I(u;\mathbf{z}) \leq I(\mathbf{x};\mathbf{y}) - I(\mathbf{x};\mathbf{z}). \quad (14)$$

Then, using Van Dijk's characterization of *less noisy* channels [20], we obtain the concavity in $p_{\mathbf{x}}$ of the r.h.s. of (14). Using Pinsker's decomposition [22], [23] we get:

$$\begin{aligned} &I(\mathbf{x};\mathbf{y}) - I(\mathbf{x};\mathbf{z}) \\ &= (I(\mathbf{x}_\mathrm{g};\mathbf{y}_\mathrm{g}) - I(\mathbf{x}_\mathrm{g};\mathbf{z}_\mathrm{g})) + (D(\mathbf{z}\,\|\,\mathbf{z}_\mathrm{g}) - D(\mathbf{y}\,\|\,\mathbf{y}_\mathrm{g})), \end{aligned} \quad (15)$$

where the subscript "g" indicates that the variable is Gaussian with the same covariance as the original random variable, and $D(\cdot\,\|\,\cdot)$ denotes the Kullback–Leibler divergence. When the covariance matrix $\mathbf{K_x}$ of $\mathbf{x}$ is fixed, the first term in the r.h.s. of (15) is constant, so the second term is concave in the input distribution $p_{\mathbf{x}}$. Moreover, both $D(\mathbf{z}\,\|\,\mathbf{z}_\mathrm{g})$ and $D(\mathbf{y}\,\|\,\mathbf{y}_\mathrm{g})$ are minimal $= 0$ when $\mathbf{x} = \mathbf{x}_\mathrm{g}$. Therefore, $p_{\mathbf{x}_\mathrm{g}}$ is a stationnary point of the second term in (15). Since it is also concave, (15) achieves its maximum at $p_{\mathbf{x}_\mathrm{g}}$. Therefore, the maximum in (12) is also achieved at $p_{\mathbf{x}_\mathrm{g}}$. □

Proof of Theorem 1. Minimizing the *SOP* is equivalent to maximizing $\mathbb{P}\left[I(u;\mathbf{y}) - I(u;\mathbf{z}) \geq r\right]$, which implies that the rate difference $I(u;\mathbf{y}) - I(u;\mathbf{z})$ should be as large as possible as often as possible. By the uniformly less noisy assumption, Lemma 1 can be used for every pair of instantaneous channels $(\mathbf{H}_0, \mathbf{G}_0)$. Therefore, the maximizing input of $I(u;\mathbf{y}) - I(u;\mathbf{z})$ is the non-precoded Gaussian $u \equiv \mathbf{x}_\mathrm{g}$, regardless of the pair of instantaneous channels. Therefore, $\mathbf{x}_\mathrm{g}$ also minimizes the *SOP*. Finally, observe that

$$I(\mathbf{x}_\mathrm{g};\mathbf{y}_\mathrm{g}) - I(\mathbf{x}_\mathrm{g};\mathbf{z}_\mathrm{g}) = \log\left(\frac{\det(\mathbf{I}+\mathbf{H}^\dagger\mathbf{K_x}\mathbf{H})}{\det(\mathbf{I}+\mathbf{G}^\dagger\mathbf{K_x}\mathbf{G})}\right). \quad (16)$$

which gives (11). □

Theorem 2. *Under the same assumption as in Theorem 1, the same non-precoded Gaussian input also maximizes the EPSR:*

$$\max_{\substack{p_{u,\mathbf{x}} \\ \mathrm{cov}[\mathbf{x}]=\mathbf{K_x}}} \mathit{EPSR} = \mathbb{E}_{\mathbf{H},\mathbf{G}}\Big[\log \frac{\det(\mathbf{I}+\mathbf{H}^\dagger\mathbf{K_x}\mathbf{H})}{\det(\mathbf{I}+\mathbf{G}^\dagger\mathbf{K_x}\mathbf{G})}\Big]. \quad (17)$$

Proof. By Theorem 1, $1 - \mathit{SOP}(r)$ is maximized by the non-precoded Gaussian input. By the well-known formula $\mathbb{E}(X) = \int_0^\infty \mathbb{P}(X > x)\,\mathrm{d}x$ for $X \geq 0$, the *EPSR* is given by

$$\mathit{EPSR} = \int_0^\infty \big(1 - \mathit{SOP}(r)\big)\,dr. \quad (18)$$

so is maximized by the same input distribution. □

It can be shown [16] that the ordering assumptions in both Theorems 1 and 2 cannot be easily removed in general: one can find examples violating these conditions with different values of optimal *SOP* and *EPSR*.

B. SIMOME channel

In the SIMOME scenario, where Alice has a single transmit antenna and both receivers have arbitrary numbers of antennas, we show that the optimal input for both the *SOP* and *EPSR* is a Gaussian signal without precoding. This result contrasts with the MIMOME case, as it requires no assumptions regarding channel ordering to achieve optimality.

Theorem 3. *When* $N_A = 1$*, the input distribution* $p_{u,x}$ *minimizing the SOP under the average power constraint* $\mathcal{P}_T$ *is the one for which* $u \equiv x$ *and* x *is a complex Gaussian random variable with variance* $\mathcal{P}_T$*. That is,*

$$\min_{\substack{p_{(u,x)} \\ \mathbb{E}[|x|^2] \leq \mathcal{P}_T}} \mathit{SOP}(r) = \mathbb{P}\Big[\log \frac{1+\mathcal{P}_T\|\mathbf{h}\|^2}{1+\mathcal{P}_T\|\mathbf{g}\|^2} < r\Big], \quad (19)$$

where $\mathbf{h}$ *(resp.* $\mathbf{g}$*) is the legitimate (resp. eavesdropper) channel matrix of dimension* $1 \times N_B$ *(resp.* $1 \times N_E$*).*

Proof. First simplify the SIMOME model into a SISOSE (Single Input, Single Output, Single Eavesdropper) equivalent model using basic matrix transformations: Define $\mathbf{\Phi_h}$ and $\mathbf{\Phi_g}$ as unitary matrices such that the first column of $\mathbf{\Phi_h}$ is $\frac{\mathbf{h}}{\|\mathbf{h}\|}$ and

the first column of $\mathbf{\Phi_g}$ is $\frac{\mathbf{g}}{\|\mathbf{g}\|}$. We have: $\mathbf{h} = \mathbf{\Phi_h}.(\|\mathbf{h}\|0...0)^T$ and $\mathbf{g} = \mathbf{\Phi_g}.(\|\mathbf{g}\|0...0)^T$. Therefore,

$$I(u;\mathbf{y}) - I(u;\mathbf{z}) = I(u;\mathbf{h}x + \mathbf{w}_B) - I(u;\mathbf{g}x + \mathbf{w}_E) \quad (20)$$

$$= I(u;(\|\mathbf{h}\|0...0)^T x + \mathbf{\Phi}_\mathbf{h}^T.\mathbf{w}_B) - I(u;(\|\mathbf{g}\|0...0)^T x + \mathbf{\Phi}_\mathbf{g}^T.\mathbf{w}_E) \quad (21)$$

$$= I(u;\|\mathbf{h}\|x + w_B) - I(u;\|\mathbf{g}\|x + w_E), \quad (22)$$

where w_B and w_E are unit-variance circularly symmetric complex Gaussian noises. In this equivalent model, the secrecy rate is positive if and only if the main channel gain $\|\mathbf{h}\|$ exceeds that of the eavesdropper, $\|\mathbf{g}\|$. Moreover, when this condition holds, the secrecy rate is maximized by a Gaussian input without precoding [21]. Conversely, when it does not hold, no input distribution can yield a positive secrecy rate. Therefore, the *SOP* is minimized by the non-precoded Gaussian input. □

Theorem 4. *When $N_A = 1$, the input distribution $p_{(u,x)}$ that maximizes the EPSR under the average power constraint $\mathcal{P}_T$ is the one for which $u \equiv x$ and x is a complex Gaussian random variable with variance $\mathcal{P}_T$; that is:*

$$\max_{\substack{p_{(u,x)} \\ \mathbb{E}[|x|^2] \leq \mathcal{P}_T}} \textit{EPSR} = \mathbb{E}_{\mathbf{h},\mathbf{g}}\Big[\log\Big(\frac{1+\mathcal{P}_T\|\mathbf{h}\|^2}{1+\mathcal{P}_T\|\mathbf{g}\|^2}\Big)^+\Big]. \quad (23)$$

Proof. By Theorem 3, the non-precoded Gaussian input maximizes $1 - \textit{SOP}(r)$. By (18) it also maximizes the *EPSR*. □

The optimal *EPSR* given in Theorem 4 is very similar to the secrecy capacity expression in [11] when the legitimate channel gain is known at the transmitter. The main difference is that, in the scenario studied in [11], knowledge of the channel gain allows the transmitter to adapt its transmission rate to the quality of the legitimate channel, whereas in our setting, the transmission rate is not influenced by any channel state information at the transmitter.

IV. Ergodic Secrecy Rate (*ESR*) optimization

A. MIMOME channel

We now show that a non-precoded Gaussian input minimizes the *ESR* for the MIMOME case, under the condition that the legitimate channel is *less noisy on average* than the eavesdropper's channel.

Theorem 5. *If the ergodic channel $\mathbf{H}$ is less noisy on average than the ergodic channel $\mathbf{G}$, then the ESR is maximized by a non-precoded Gaussian input:*

$$\max_{\substack{p_{u,\mathbf{x}} \\ \mathrm{cov}[\mathbf{x}]=\mathbf{K_x}}} \textit{ESR} = \mathbb{E}_{\mathbf{H},\mathbf{G}}\Big[\log\frac{\det(\mathbf{I}+\mathbf{H}^\dagger\mathbf{K_x}\mathbf{H})}{\det(\mathbf{I}+\mathbf{G}^\dagger\mathbf{K_x}\mathbf{G})}\Big]. \quad (24)$$

Proof Outline (see [16] for details). Following an approach similar to [20], we can prove that the *less noisy on average* assumption implies

$$\max_{p_{u,\mathbf{x}}} \textit{ESR} = \max_{p_\mathbf{x}} \mathbb{E}_{\mathbf{H},\mathbf{G}}\left[I(\mathbf{x};\mathbf{y}) - I(\mathbf{x};\mathbf{z})\right]. \quad (25)$$

By the channel ordering, the right-hand side of (25) is concave with respect to the input distribution $p_\mathbf{x}$. Similarly as in Lemma 1, Pinsker's decomposition [22], [23] implies that $\mathbf{x}_\mathrm{g}$ is a stationary point of this expression, hence achieves the maximum. □

The *less noisy on average* ordering is central to the proof of Theorem 5. Its role is essential, as it cannot be relaxed without affecting optimality: [16] gives a counterexample for which violating this condition results in the non-precoded Gaussian input no longer achieving the maximum *ESR*.

B. SIMOME channel

Whereas reducing the problem to the SIMOME case leads to a unified solution for the optimization of the *SOP* and *EPSR*, no such simplification arises for the optimization of the *ESR*.

Theorem 6. *When $N_A = 1$, let $c_{x|u}$ denote a fixed precoder and let $p_{u,x} = p_u c_{x|u}$ and $q_{u,x} = q_u c_{x|u}$ be two input distributions sharing the same precoder, such that $\mathbb{E}\big[|x|^2\big] = \mathcal{P}_T$. Denote by ESR$(p_{u,x}, p_\mathbf{h}, p_\mathbf{g})$ (resp. ESR$(q_{u,x}, p_\mathbf{h}, p_\mathbf{g})$) the ESR obtained with the input distribution $p_{u,x}$ (resp. $q_{u,x}$) and the channel statistics $p_\mathbf{h}$ and $p_\mathbf{g}$. Then exactly one of the following two statements holds:*

(i) For all channel statistics $p_\mathbf{h}$ and $p_\mathbf{g}$,

$$\textit{ESR}(p_{u,x}, p_\mathbf{h}, p_\mathbf{g}) = \textit{ESR}(q_{u,x}, p_\mathbf{h}, p_\mathbf{g}). \quad (26)$$

(ii) There exist channel statistics $p_\mathbf{h}$ and $p_\mathbf{g}$ such that

$$\textit{ESR}(p_{u,x}, p_\mathbf{h}, p_\mathbf{g}) < \textit{ESR}(q_{u,x}, p_\mathbf{h}, p_\mathbf{g}). \quad (27)$$

Here *(i)* corresponds to a trivial case in which the distributions $p_{u,x}$ and $q_{u,x}$ induce identical behavior. This occurs, for instance, when $p_{u,x} = q_{u,x}$. In *(ii)*, the distributions $p_{u,x}$ and $q_{u,x}$ play symmetric roles, and can be interchanged without affecting the result. As a result, there is no universally optimal input distribution that maximizes the *ESR*, as the optimum depends critically on the channel statistics. In particular, Gaussian inputs are not always optimal: one can construct examples where a binary input distribution achieves a higher *ESR* than a Gaussian input [16].

Finally, since SIMOME channels form a special case of MIMOME channels, Theorem 6 also implies that no single input distribution is optimal across all MIMOME channel configurations, when the *less noisy on average* ordering is not assumed.

Proof Outline (see [16] for details). The SIMOME model can be reduced to an equivalent SISOSE (Single Input, Single Output, Single Eavesdropper) representation using standard matrix transformations. Now consider

$$\Delta(\gamma) = I_p(\gamma) - I_q(\gamma),$$

where I_p (resp. I_q) denotes the mutual information between the input following distribution p (resp. q) and the SISO output with channel gain γ.

We show from [18], [19] that Δ is infinitely differentiable and that

$$\Delta(0) = \Delta'(0) = \lim_{\gamma \to +\infty} \Delta'(\gamma) = 0. \tag{28}$$

Therefore, if Δ is concave over $\mathbb{R}_{\geq 0}$, it must be identically zero, i.e., $\Delta(\gamma) = 0$ for all $\gamma \geq 0$, which implies that *(i)* holds. Otherwise, Δ is convex over some open interval of $\mathbb{R}_{\geq 0}$. On this interval, we can construct γ_1, γ_2, and γ_h such that

$$\tfrac{1}{2}\big(\Delta(\gamma_1) + \Delta(\gamma_2)\big) \geq \Delta(\gamma_h). \tag{29}$$

By defining channel statistics $p_{\mathbf{h}}$ concentrated at $\sqrt{\gamma_h}$ and $p_{\mathbf{g}}$ with two equally weighted mass points at $\sqrt{\gamma_1}$ and $\sqrt{\gamma_2}$, one obtains *(ii)*. □

Corollary 1. *If the fixed precoder $c_{x|u}$ is such that I_p is concave in the input distribution p_x, then both sides of* (27) *can be chosen to be nonnegative. In particular, this holds if the precoder is trivial such that $u \equiv x$ (no precoding).*

C. Bounds on the maximum ESR

When the *less noisy on average* ordering does not hold, the maximization of the *ESR* becomes analytically intractable. Nonetheless, upper and lower bounds can still be derived.

Theorem 7. *The maximum ESR for a MIMOME scenario with fixed covariance matrix $\mathbf{K_x}$ for $\mathbf{x}$ can be bounded as follows:*

$$C_S^- \leq \max_{\substack{p_{u,\mathbf{x}} \\ \mathrm{cov}(\mathbf{x}) = \mathbf{K_x}}} \mathit{ESR} \leq C_S^+, \tag{30}$$

with

$$C_S^- = \mathbb{E}_{\mathbf{H},\mathbf{G}}\Big[\log \frac{\det(\mathbf{I} + \mathbf{H}\mathbf{K_x}\mathbf{H}^\dagger)}{\det(\mathbf{I} + \mathbf{G}\mathbf{K_x}\mathbf{G}^\dagger)}\Big] + \max_{0 \preceq \mathbf{K}_M \preceq \mathbf{K_x}} \mathbb{E}_{\mathbf{H},\mathbf{G}}\Big[\log \frac{\det(\mathbf{I} + \mathbf{G}\mathbf{K}_M\mathbf{G}^\dagger)}{\det(\mathbf{I} + \mathbf{H}\mathbf{K}_M\mathbf{H}^\dagger)}\Big], \tag{31}$$

and

$$C_S^+ = \int \log(\mathbf{I} + \mathbf{A}\mathbf{K_x}\mathbf{A}^\dagger)(p_{\mathbf{H}}(\mathbf{A}) - p_{\mathbf{G}}(\mathbf{A}))^+ d\mathbf{A}. \tag{32}$$

Proof Outline (see [16]). The lower bound C_S^- is obtained by evaluating the *ESR* for a specific input distribution, namely a Gaussian signaling scheme combining an information-bearing signal $\mathbf{x}_I \equiv u$ and an artificial noise $\mathbf{x}_M$ independent of u, with covariance matrix $\mathbf{K}_M$. Therefore, we get:

$$I(u;\mathbf{y}) - I(u;\mathbf{z}) \tag{33}$$
$$= \log\left(\frac{\det(\mathbf{I} + \mathbf{H}\mathbf{K_x}\mathbf{H}^\dagger)}{\det(\mathbf{I} + \mathbf{H}\mathbf{K}_M\mathbf{H}^\dagger)}\right) - \log\left(\frac{\det(\mathbf{I} + \mathbf{G}\mathbf{K_x}\mathbf{G}^\dagger)}{\det(\mathbf{I} + \mathbf{G}\mathbf{K}_M\mathbf{G}^\dagger)}\right).$$

Reordering the terms, averaging over all instantaneous channels $\mathbf{H}$ and $\mathbf{G}$ and maximizing over all possible $\mathbf{K}_M$ yields $C_S^- \leq \max \mathit{ESR}$.

The upper bound C_S^+ is derived by expanding the *ESR* as

$$\mathit{ESR} = \int I(u;\mathbf{y} \mid \mathbf{H} = \mathbf{A})\big(p_{\mathbf{H}}(\mathbf{A}) - p_{\mathbf{G}}(\mathbf{A})\big)\, d\mathbf{A}, \tag{34}$$

and by upper bounding the integrand using the non-negativity of mutual information, together with the fact that a Gaussian input maximizes $I(u;\mathbf{y} \mid \mathbf{H} = \mathbf{A})$. □

Theorem 8. *When $N_A = 1$ (SIMOME scenario), the maximum ESR can be framed as follows:*

$$C_{S,\mathit{SIMOME}}^- \leq \max_{\substack{p_{u,x} \\ \mathbb{E}[|x|^2] \leq \mathcal{P}_T}} \mathit{ESR} \leq C_{S,\mathit{SIMOME}}^+, \tag{35}$$

with

$$C_{S,\mathit{SIMOME}}^- = \max_{0 \leq P \leq \mathcal{P}_T} \mathbb{E}_{\mathbf{h},\mathbf{g}}\Big[\log \frac{1 + \mathcal{P}_T - P + P\|\mathbf{h}\|^2}{1 + \mathcal{P}_T - P + P\|\mathbf{g}\|^2}\Big] \tag{36}$$

and

$$C_{S,\mathit{SIMOME}}^+ = \min\{C_{S,\mathit{SIMOME}}^{+(0)}, C_{S,\mathit{SIMOME}}^{+(1)}\}, \tag{37}$$

where

$$C_{S,\mathit{SIMOME}}^{+(0)} = \int_0^\infty \log(1 + \mathcal{P}_T a^2)(p_{\|\mathbf{h}\|}(a) - p_{\|\mathbf{g}\|}(a))^+ da \tag{38}$$

$$C_{S,\mathit{SIMOME}}^{+(1)} = \int_0^\infty \frac{\mathcal{P}_T(\mathbb{P}\left[\|\mathbf{h}\| \geq a\right] - \mathbb{P}\left[\|\mathbf{g}\| \geq a\right])^+}{1 + \mathcal{P}_T a^2} da \tag{39}$$

Proof Outline (see [16]). Lower and upper bounds $C_{S,\mathrm{SIMOME}}^-$, $C_{S,\mathrm{SIMOME}}^{+(0)}$ are obtained by applying Theorem 7 to the SIMOME setting. The upper bound $C_{S,\mathrm{SIMOME}}^{+(1)}$ is specific to the SIMOME case and is derived using an argument similar to that used for $C_{S,\mathrm{SIMOME}}^{+(0)}$: one writes *ESR* as

$$\int \frac{d}{d(a^2)}(I(u;\mathbf{y} \mid \|\mathbf{h}\| = a))\big(\mathbb{P}[\|\mathbf{h}\| \geq a] - \mathbb{P}[\|\mathbf{g}\| \geq a]\big)^+ da. \tag{40}$$

The integrand is then upper-bounded by approximating the derivative as the secrecy rate between two channels with close gains. Using the result of [21], this derivative is maximized by a Gaussian input, which yields the desired upper bound. □

V. Conclusion

In this work, we analyzed the optimization of three secrecy metrics for wireless channels when the transmitter has knowledge only of channel statistics: the Secrecy Outage Probability (*SOP*), the Ergodic Positive Secrecy Rate (*EPSR*), and the Ergodic Secrecy Rate (*ESR*). Our results show that a non-precoded Gaussian input achieves optimal performance for both the *SOP* and the *EPSR* when the eavesdropper's MIMO channel is *uniformly noisier* than the legitimate MIMO channel. Notably, the same Gaussian input also maximizes the *ESR* under the weaker condition that the eavesdropper's channel is *noisier on average* than the legitimate channel.

We also examined the SIMOME scenario, where the transmitter has a single antenna. In this case, the optimal input remains Gaussian and non-precoded for both the *SOP* and *EPSR*, even without imposing any channel ordering assumptions. However, for the *ESR*, no single input distribution guarantees general optimality. This highlights that *ESR* optimization must be tailored to the specific statistical properties of the channels.

Our findings offer theoretical insight for the fundamental limits of wireless secrecy under statistical channel knowledge, with the prominent role of Gaussian inputs. As a perspective, limitations associated with the *ESR* optimization in the general MIMOME setting may be further clarified in a future work.

REFERENCES

[1] A.D. Wyner, “The wire-tap channel”, in *The Bell System Technical Journal*, vol: 54, no: 8, pp. 1355-1387, Oct. 1975.

[2] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” in *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” in *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[4] F. Oggier and B. Hassibi, “Secrecy capacity of the MIMO wiretap channel,” in *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[5] R. Bustin, R. Liu, H. V. Poor and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *2009 IEEE ISIT*, Seoul, Korea (South), 2009, pp. 2602-2606.

[6] A. Khina, Y. Kochman and A. Khisti, "The MIMO wiretap channel decomposed," in *IEEE Trans. Inform. Theory*, vol. 64, no. 2, pp. 1046-1063, Feb. 2018.

[7] Z. Rezki, A. Khisti and M. -S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," in *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652-3664, Oct. 2014.

[8] A. Hyadi, Z. Rezki, A. Khisti and M. -S. Alouini, "Secure broadcasting with imperfect channel state information at the transmitter," in *IEEE Trans. Wireless Comm.*, vol. 15, no. 3, pp. 2215-2230, March 2016.

[9] Q. Li and W. -K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," in *IEEE Trans. Signal Proc.*, vol. 59, no. 8, pp. 3799-3812, Aug. 2011.

[10] S. -C. Lin and C. -L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," in *IEEE Trans. Wireless Comm.*, vol. 13, no. 6, pp. 3293-3306, June 2014.

[11] P. K. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of fading channels," in *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[12] Y. Liang, H. V. Poor and S. Shamai, "Secure communication over fading channels," in *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470-2492, June 2008.

[13] S. Goel, and R. Negi, “Guaranteeing secrecy using artificial noise”, in *IEEE Trans. Wireless Comm.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[14] P. -H. Lin, S. -H. Lai, S. -C. Lin and H. -J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," in *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728-1740, September 2013.

[15] G. Shi, Y. Li, W. Cheng, X. Gao and W. Zhang, "An artificial-noise-based approach for the secrecy rate maximization of MISO VLC wiretap channel with multi-eves," in *IEEE Access*, vol. 9, pp. 651-659, 2021.

[16] C. Leroy, T. Arbi, B. Geller, and O. Rioul, On the optimum secrecy outage probability and ergodic secrecy rate over wireless channels. Available online: https://arxiv.org/abs/2604.22587, Apr. 2026.

[17] J. Körner and K. Marton, "Comparison of two noisy channels," *Topics in Information Theory*, vol. IT-23, no. 1, pp. 60-64 May 1978.

[18] Dongning Guo, S. Shamai and S. Verdu, "Mutual information and minimum mean-square error in Gaussian channels," in *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1261-1282, April 2005.

[19] D. Guo, Y. Wu, S. S. Shitz and S. Verdú, "Estimation in Gaussian nboise: Properties of the minimum mean-square error," in *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2371-2385, April 2011.

[20] M. Van Dijk, "On a special class of broadcast channels with confidential messages," in *IEEE Trans. Inform. Theory*, vol. 43, no. 2, pp. 712-714, March 1997.

[21] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," in *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[22] M. S. Pinsker, "Calculation of the rate of information production by means of stationary random process and the capacity of stationary channel," *Doklady Akademii Nauk USSR*, vol 111, pp. 753-756, 1956 (in Russian).

[23] M. S. Pinsker, V. V. Prelov and S. Verdu, "Sensitivity of channel capacity," in *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1877-1888, Nov. 1995.