Physical Layer Security with Frequency-Hopping and Finite-Alphabet Inputs

Clément Leroy*, Tarak Arbi*, Benoit Geller*, Olivier Rioul‡
*U2IS, ENSTA, Institut Polytechnique de Paris, ‡LTCI, Télécom Paris, Institut Polytechnique de Paris
{firstname.lastname}@ensta-paris.fr, olivier.rioul@telecom-paris.fr

***Abstract*—This paper investigates the physical layer security of frequency-hopping (FH) transmission schemes when the hopping sequence is publicly known. We consider a single-antenna transmitter communicating with a legitimate receiver over a channel estimated with a known error distribution, in the presence of a passive eavesdropper whose channel statistics are available at the transmitter. We show that, when the number of hopping frequencies is sufficiently large, the instantaneous channel fluctuations induced by FH transmissions can be effectively averaged out, and the secrecy performance is accurately predicted by the ergodic secrecy rate (ESR). The ESR is maximized by selecting the optimal modulation order from a set of admissible finite constellations. We derive a closed-form condition on the optimal modulation order, which only depends on the tail probabilities of the legitimate and eavesdropper signal-to-noise ratio (SNR) distributions, and we propose an efficient algorithm for its computation. In particular, we demonstrate that a positive secrecy rate can be achieved even when the eavesdropper has a higher average SNR than the legitimate receiver, provided that the spread of the eavesdropper SNR distribution is sufficiently large. Numerical results validate the proposed framework under a variety of channel models.**

***Index Terms*—Physical layer security, frequency hopping, secrecy capacity, ergodic secrecy rate, finite-alphabet inputs, imperfect channel state information.**

I. Introduction

Secrecy in wireless communications has traditionally been achieved with upper-layer methods such as cryptographic protocols. However, these approaches require the establishment, management, and distribution of secret keys among legitimate users, which can be challenging in latency-sensitive or resource-constrained environments such as the Internet of Things (IoT), vehicular networks, and tactical communication systems. Physical Layer Security (PLS) has therefore emerged as an attractive complementary or alternative solution for ensuring confidentiality by exploiting the physical properties of the communication channel, rather than relying on a secret key [1].

Following Wyner's seminal work on the wiretap channel [2], Csiszár and Körner showed that perfect secrecy can be achieved through channel coding whenever the legitimate receiver has a better channel than the eavesdropper [3]. The maximum transmission rate at which reliable and secure communication is achievable is referred to as the secrecy capacity. Closed-form expressions for the secrecy capacity have been derived for a variety of wireless communication scenarios [4]–[6]. These models typically assume perfect channel state information (CSI) for both the legitimate and eavesdropper channels. The characterization of secrecy capacity under imperfect CSI remains largely open, although several bounds have been established [7], [8]. In [9], the beneficial impact of fast fading on secrecy performance has been highlighted.

Frequency-hopping (FH) transmission schemes employ a set of carrier frequencies that are sequentially used throughout the transmission [10]. FH is an attractive waveform for spectral efficiency, transmission discretion, and robustness against jamming attacks [11]. However, achieving these benefits generally requires the legitimate receiver to know the frequency-hopping sequence, which is often treated as a shared secret key. Nevertheless, such sequences can be recovered by sophisticated follower receivers capable of tracking the hopping pattern with very short acquisition delays. Consequently, the secrecy of the hopping sequence alone cannot be considered to be sufficient for ensuring the confidentiality of the transmitted information.

In this paper, we investigate the PLS provided by FH transmission schemes when the hopping sequence is publicly known. The transmitter is assumed to have access only to the eavesdropper channel statistics, while the legitimate channel is estimated with a known error distribution. Unlike most existing PLS methods that rely on multiple-antenna processing at the transmitter [12]–[14], the proposed scheme achieves secrecy with a single transmitting antenna. We show that, when a sufficiently large number of hopping frequencies is available, the uncertainty induced by the unknown instantaneous channel states can be effectively averaged out, enabling the transmitter to design a near-optimal transmission strategy despite the lack of instantaneous eavesdropper CSI. Furthermore, we demonstrate that frequency hopping induces an effect similar to the fast-fading scenario studied in [8], [9], in which channel fluctuations enhance the secrecy capacity. In particular, we show that secrecy can be achieved even when the average eavesdropper signal-to-noise ratio (SNR) exceeds that of the legitimate receiver by up to 1.5 dB in some scenarios. We propose a method for optimizing the secrecy rate by selecting the modulation order of finite-alphabet constellations (e.g., M-QAM or M-PSK). The secrecy performance is analyzed using information-theoretic tools and is further validated through

This study was funded by the AID CIEDS project SEPHYTEL.

numerical simulations.

The remainder of this paper is organized as follows: Section II introduces the communication model. Section III presents our analysis of the secrecy capacity of FH transmission and a method to optimize it. Simulation results are presented in Section IV. Finally, Section V concludes the paper.

II. System Model

A. Channel and Signal Model

We consider a SIMOME (Single-Input Multiple-Output Multiple-Eavesdropper) communication system in which the transmitter is equipped with a single antenna, the legitimate receiver is equipped with N_R antennas, and the passive eavesdropper is equipped with N_E antennas. This model encompasses both the scenario of a single eavesdropper equipped with N_E antennas and the scenario of multiple colluding eavesdroppers jointly equipped with a total of N_E antennas.

The transmitter employs a FH scheme. The information bits are encoded into a sequence of symbols drawn from a complex normalized constellation, such as QAM or PSK. The carrier frequency hops at a rate f_H among frequencies selected from the set $\mathcal{F} = \{f_0, \ldots, f_{K-1}\}$, which contains K distinct frequencies chosen such that they experience independent channel realizations (e.g., they are separated by more than the channel coherence bandwidth). The frequency-hopping sequence $k(t)$ is shared with the legitimate receiver. To account for the worst-case scenario, the eavesdropper is assumed to be capable of perfectly estimating this sequence.

The channel gain vector of the main channel at the k^{th} frequency is denoted by $\mathbf{h}_k$, whereas the eavesdropper channel gain vector is denoted by $\mathbf{g}_k$. After dehopping, the received signal at the legitimate receiver is expressed as

$$\mathbf{y}_R(t) = \mathbf{h}_{k(t)} x(t) + \mathbf{n}_R(t), \tag{1}$$

while the received signal at the eavesdropper is given by

$$\mathbf{y}_E(t) = \mathbf{g}_{k(t)} x(t) + \mathbf{n}_E(t), \tag{2}$$

where $x(t)$ denotes the symbol transmitted at time t, and $\mathbf{n}_R(t)$ and $\mathbf{n}_E(t)$ represent zero-mean additive white Gaussian noise (AWGN) vectors with covariance matrix $\mathbf{I}$.

B. Imperfect CSI at the Transmitter

The legitimate channel is estimated at the transmitter using time-division duplexing (TDD) synchronization and channel reciprocity. The channel estimation error at frequency f_k is classically modeled as [15]

$$\hat{\mathbf{h}}_k = \sqrt{1-\sigma_\epsilon^2}\,\mathbf{h}_k + \boldsymbol{\epsilon}_k, \tag{3}$$

where $\hat{\mathbf{h}}_k$ denotes the estimated CSI, $\mathbf{h}_k$ is the true channel vector, and $\boldsymbol{\epsilon}_k$ is a zero-mean circularly symmetric complex Gaussian random vector with covariance matrix $\sigma_\epsilon^2\mathbf{I}$. The error vector is assumed independent of $\mathbf{h}_k$.

The legitimate channel is assumed to be known at both the legitimate receiver and the eavesdropper, whereas the eavesdropper channel is assumed to be known only to the eavesdropper. It is important to note that the eavesdropper is assumed to have perfect knowledge of the carrier frequency and the legitimate CSI at every time instant t. Consequently, the secrecy considered in this paper does not rely on any secret shared between the legitimate parties.

C. Statistical Model of the Eavesdropper Channel

The transmitter is not synchronized with the eavesdropper; therefore, the eavesdropper channel gains remain unknown to the legitimate parties. However, environmental parameters provide statistical information about the distribution of the eavesdropper channel. For instance, in a rich scattering environment, the channel gains at different frequencies are independent and follow a complex Gaussian distribution. In a line-of-sight (LOS) scenario, the channel gain is primarily determined by the eavesdropper's position and exhibits a deterministic dependence on the propagation geometry.

The eavesdropper channel distribution is assumed to be known to the transmitter. Several channel distributions are investigated in the numerical results section.

III. Secrecy Capacity Analysis of Frequency-Hopping Transmissions

A. From Instantaneous Secrecy Capacity to Ergodic Secrecy Rate

The secrecy capacity of a general wiretap channel is defined in [3] as the supremum of all achievable rates for which the probability of error at the legitimate receiver can be made arbitrarily small as the block length tends to infinity, while the equivocation rate at the eavesdropper approaches the message entropy. This implies that reliable communication can be achieved at the legitimate receiver while ensuring that the eavesdropper obtains asymptotically no information about the transmitted message, provided that the transmission rate is below the secrecy capacity. In general, the secrecy capacity is expressed as the maximum secrecy rate, given by

$$C_S = \max_{p_{(u,x)}} \big[I(u;y) - I(u;z) \big], \tag{4}$$

where $I(\cdot;\cdot)$ denotes Shannon mutual information, x is the transmitted signal, y is the signal received at the legitimate receiver, and z is the signal received at the eavesdropper. The random variable u is an auxiliary variable, and $p_{(u,x)}$ denotes the joint distribution of (u, x).

The auxiliary random variable u enables randomized encoding schemes; however, such constructions typically incur additional implementation and decoding complexity at the legitimate receiver. Therefore, in the remainder of this paper, we restrict the analysis to deterministic encoders, i.e., $u \equiv x$. When the input distribution $p_{(u,x)}$ is constrained, the secrecy capacity is sometimes defined as the positive part of the right-hand side of (4), since negative values can be avoided simply by suspending transmission. In this paper, however, we adhere to the definition (4), allowing the secrecy capacity to take

negative values, as this provides additional insight into its overall behavior.

In fast-fading channels, the instantaneous channel gain is modeled as a random process independent of the transmitted information. It can thus be interpreted as a channel output driven by the underlying propagation environment. The FH transmission scheme emulates this behavior, as the effective channel gains vary over time due to the time-varying carrier frequency. Thus, the secrecy capacity of the FH transmission scheme can be expressed as

$$C_{S,\mathrm{FH}} = \max_{p_x} \left[I(x; \mathbf{y}_R, \mathbf{h}) - I(x; \mathbf{y}_E, \mathbf{g}) \right] \tag{5}$$

$$= \max_{p_x} \left[I(x; \mathbf{y}_R \mid \mathbf{h}) - I(x; \mathbf{y}_E \mid \mathbf{g}) \right] \tag{6}$$

$$= \max_{p_x} \mathbb{E}_k \left[I(x; \mathbf{y}_R \mid \mathbf{h} = \mathbf{h}_k) - I(x; \mathbf{y}_E \mid \mathbf{g} = \mathbf{g}_k) \right], \tag{7}$$

where (6) follows from the independence between the transmitted signal and the channel states, i.e., $I(x; \mathbf{h}) = I(x; \mathbf{g}) = 0$, together with the chain rule of mutual information; and (7) follows from the fact that conditional mutual information can be expressed as the expectation of the instantaneous mutual information over the channel realizations. The carrier index k is modeled as a random variable taking values in the set $\{0, 1, \ldots, K-1\}$.

In a SIMO (Single-Input Multiple-Output) setting, a matched filter at the receiver is an information-preserving operation. Hence, the secrecy capacity can be expressed in terms of the equivalent scalar channels obtained after matched filtering at both the legitimate receiver and the eavesdropper:

$$C_{S,\mathrm{FH}} = \max_{p_x} \mathbb{E}_k \left[I(x; \|\mathbf{h}_k\| x + n_R) - I(x; \|\mathbf{g}_k\| x + n_E) \right], \tag{8}$$

where n_R and n_E are zero-mean additive white Gaussian noise (AWGN) terms with unit variance. The instantaneous secrecy capacity depends on the particular realizations of the legitimate and eavesdropper channels. However, when the number of hopping frequencies K is sufficiently large, the empirical average over the frequency index k approaches the statistical expectation over the channel realizations. Consequently, for large values of K, (8) corresponds to the maximization of what we referred to in [8] as the ergodic secrecy rate (ESR):

$$\mathrm{ESR} = \mathbb{E}_{\rho_R, \rho_E} \left[I(x; \sqrt{\rho_R} x + n_R) - I(x; \sqrt{\rho_E} x + n_E) \right], \tag{9}$$

where $\rho_R = \|\mathbf{h}_k\|^2$ and $\rho_E = \|\mathbf{g}_k\|^2$ are the legitimate receiver and eavesdropper SNR respectively. The eavesdropper channel statistics and the legitimate channel estimation are accounted for in (9), as the expectation is taken over the legitimate and eavesdropper SNRs.

For a fixed input distribution, in particular the one that maximizes the ESR, the probability that the instantaneous secrecy capacity deviates from the ESR by more than a can be bounded using the Bienaymé–Chebyshev inequality:

$$\Pr\left[|C_{S,\mathrm{FH}} - \mathrm{ESR}| > a \right] \leq \frac{\mathrm{Var}\left[I\left(x; \sqrt{\rho_R} x + n_R\right) \right] + \mathrm{Var}\left[I\left(x; \sqrt{\rho_E} x + n_E\right) \right]}{K a^2}. \tag{10}$$

This upper bound tends to zero as K increases. Therefore, when K is large, the transmitter may select a coding rate slightly below the ESR and obtain a high probability that the selected rate remains below the actual secrecy capacity, thereby ensuring secure communication. The impact of K on the gap between the instantaneous secrecy capacity and the ESR is further investigated in the simulation section.

In [8, Theorem 6], we investigated the maximization of the ESR under specific channel distribution assumptions and showed that, unlike many classical information-theoretic rate expressions, a Gaussian input distribution for p_x is not generally optimal. Furthermore, no single input distribution is optimal across all eavesdropper channel models and legitimate channel estimation error distributions. Although this result makes the general optimization problem analytically intractable, it is beneficial from an implementation perspective. Indeed, Gaussian signaling is not practically feasible, and the maximization of the ESR can instead be performed over a finite set of admissible modulation schemes, which may even achieve higher ESR values than those obtained under a Gaussian input assumption.

B. Optimal Modulation Order Selection

We consider the class of finite input distributions, which is of particular importance since practical communication systems employ discrete constellations. Our objective is to determine the optimal modulation order M that maximizes the secrecy capacity of the FH transmission scheme. More precisely, we focus on two families of finite modulations: M-PSK and M-QAM. M-PSK constellations can be defined for any integer $M \geq 2$, whereas square M-QAM constellations are typically defined only for $M = 4^n$, with $n \in \mathbb{N}$.

The analysis of the ESR requires a detailed characterization of the mutual information between a finite-alphabet input x_M of size M and the channel output $y = \sqrt{\rho}\, x + n$, where ρ denotes the SNR, and n is AWGN. However, the exact expression of this mutual information is analytically intractable in general, which motivates the use of approximations.

In [16], an accurate numerical approximation of this mutual information for QAM inputs was proposed. However, the resulting expressions remain purely numerical and do not yield closed-form formulas, which limits further theoretical analysis. In this work, we propose a simpler approximation based on the asymptotic regimes. The exact mutual information expressions are used in the simulations section to evaluate the secrecy performance.

The capacity of a channel with a finite input of size M exhibits similar asymptotic behavior for all inputs x_M in both the low- and high-SNR regimes [18]. Indeed, when $\rho \simeq 0$, the mutual information between a finite-alphabet input x_M of size M and the output $\sqrt{\rho} x_M + n$ approaches the capacity achieved with a Gaussian input distribution. When $\rho \to \infty$, the mutual information saturates at $\log(M)$. This leads to the following approximation also studied in [17]:

$$I(x_M; \sqrt{\rho} x_M + n) \simeq \min(\log(1+\rho), \log(M)). \tag{11}$$

We denote the right-hand side of (11) by $I_M(\rho)$. Using this approximation, the ESR can be expressed as:

$$\mathrm{ESR} = \mathbb{E}_{\rho_R}\left[I(x;\sqrt{\rho_R}x+n_R)\right] - \mathbb{E}_{\rho_E}\left[I(x;\sqrt{\rho_E}x+n_E)\right] \tag{12}$$

$$\simeq \mathbb{E}_{\rho_R}\left[I_M(\rho_R)\right] - \mathbb{E}_{\rho_E}\left[I_M(\rho_E)\right]. \tag{13}$$

In (13), the integer M can be relaxed to any positive real number m. This allows us to first determine the real-valued m^* that maximizes the ESR approximation, and then select the integer modulation order M^* that maximizes the ESR approximation. We therefore study the derivative of (13) with respect to m. First, the expectation can be decomposed as

$$\mathbb{E}_{\rho_R}[I_m(\rho_R)] = \mathbb{E}_{\rho_R}\left[\log(1+\rho_R)\mathbf{1}_{\rho_R\le m-1}\right] + \mathbb{E}_{\rho_R}\left[\log(m)\mathbf{1}_{\rho_R>m-1}\right]. \tag{14}$$

Denoting by f_{ρ_R} the probability density function of ρ_R, this can be written as

$$\mathbb{E}_{\rho_R}[I_m(\rho_R)] = \int_0^{m-1}\log(1+\rho)\,f_{\rho_R}(\rho)\,d\rho + \log(m)\,\mathbb{P}[\rho_R > m-1]. \tag{15}$$

We have

$$\frac{d}{dm}\left(\log(m)\,\mathbb{P}[\rho_R>m-1]\right) = \frac{1}{m}\,\mathbb{P}[\rho_R>m-1] - \log(m)\,f_{\rho_R}(m-1), \tag{16}$$

which yields

$$\frac{d}{dm}\mathbb{E}_{\rho_R}[I_m(\rho_R)] = \frac{\mathbb{P}[\rho_R>m-1]}{m}. \tag{17}$$

Similarly,

$$\frac{d}{dm}\mathbb{E}_{\rho_E}[I_m(\rho_E)] = \frac{\mathbb{P}[\rho_E>m-1]}{m}. \tag{18}$$

Therefore, the derivative of the ESR approximation is

$$\frac{d\,\mathrm{ESR}}{dm} = \frac{1}{m}\left(\mathbb{P}[\rho_R>m-1] - \mathbb{P}[\rho_E>m-1]\right), \tag{19}$$

and the real-valued optimizer m^* satisfies

$$\mathbb{P}\left[\rho_R > m^*-1\right] = \mathbb{P}\left[\rho_E > m^*-1\right]. \tag{20}$$

Finally, if $M_1 \le m^* < M_2$, where M_1 and M_2 are two consecutive admissible modulation orders, the optimal modulation order M^* is selected as the value in $\{M_1, M_2\}$ that maximizes the ESR approximation. The procedure is summarized in Algorithm 1, where the search is restricted to either M-PSK or M-QAM constellations.

Equations (19) and (20) suggest that increasing the modulation order M is beneficial when the legitimate receiver experiences saturation of its mutual information more frequently than the eavesdropper. Conversely, when the eavesdropper experiences saturation more often, decreasing the modulation order induces stronger saturation at the eavesdropper while relatively preserving the achievable rate at the legitimate receiver.

The resulting optimal modulation order depends primarily on the tail behavior of the SNR distributions, rather than on their full distributions. Consequently, secrecy can still be achieved even when the eavesdropper has a higher average SNR than the legitimate receiver, provided that the SNR distribution of the eavesdropper exhibits a heavier tail than that of the legitimate channel. In particular, when the eavesdropper SNR distribution has a large variance, implying a non-negligible probability of very high SNR realizations, secrecy can be achieved at a higher rate. Although this observation may appear counter-intuitive, it can be understood by noting that, for finite-alphabet inputs, the mutual information saturates at high SNR, so that further increases in SNR provide only marginal rate improvements, while the achievable rate in this regime becomes mainly determined by the modulation order. Therefore, the spread of the SNR distribution plays a critical role, since larger variability increases the likelihood of operating in the saturation regime.

Algorithm 1: Optimal Modulation Order Selection

Input: Distribution of ρ_R and ρ_E
$\Delta_{\text{tails}}(m) = \mathbb{P}[\rho_R > m-1] - \mathbb{P}[\rho_E > m-1]$
$\mathcal{Z} \leftarrow \{z : \Delta_{\text{tails}}(z) = 0\}$
if $\mathcal{Z} = \varnothing$ **then**
  if $\Delta_{\text{tails}} > 0$ **then**
    $m^* \leftarrow \infty$
  else
    $m^* \leftarrow 2$
else
  Find m^* in $\mathcal{Z}$ such that $\mathrm{ESR}(m^*)$ is maximized.
// M-PSK modulations
$M_1 \leftarrow \lfloor m^* \rfloor$; $M_2 \leftarrow \lfloor m^* \rfloor + 1$
// M-QAM modulations
$M_1 \leftarrow 4^{\lfloor \log_4(m^*) \rfloor}$; $M_2 \leftarrow 4^{\lfloor \log_4(m^*) \rfloor + 1}$
Compute $\mathrm{ESR}(M_1)$ and $\mathrm{ESR}(M_2)$
if $\mathrm{ESR}(M_2) > \mathrm{ESR}(M_1)$ **then**
  $M^* \leftarrow M_2$
else
  $M^* \leftarrow M_1$
Output: Optimal modulation order M^*

IV. Simulation Results

A. Concentration of the Secrecy Capacity around the ESR

Figure 1 shows the cumulative distribution function (CDF) of $C_{S,FH}$ for different numbers of frequencies $K \in \{1, 2, 8, 64, 256\}$, under a Rician eavesdropper channel model, with $N_R = N_E = 2$, an average legitimate receiver SNR of 20 dB, an average eavesdropper SNR of 15 dB, $\sigma_\epsilon^2 = 0.2$, $M = 64$, and an eavesdropper SNR variance of $\sigma_E^2 = 1$. The randomness in $C_{S,FH}$ stems entirely from the instantaneous realizations of the legitimate and eavesdropper channels. As K increases, $C_{S,FH}$ becomes less dispersed and converges toward the ESR, which is indicated by a vertical dashed line. The CDF corresponding to $K = 1$ exhibits a wide spread and includes a significant probability of negative values of $C_{S,FH}$,

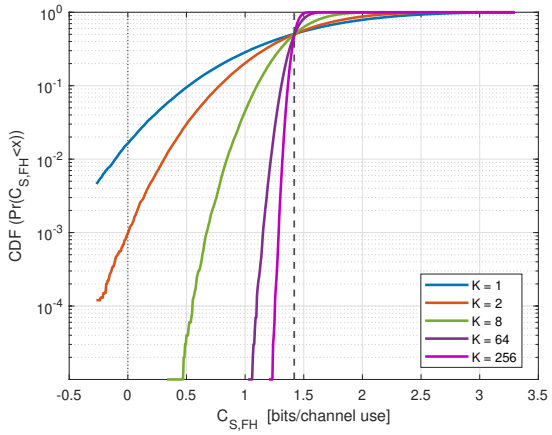

Fig. 1: CDF of the secrecy capacity for a Rician-faded eavesdropper channel and various numbers of hopping frequencies K.

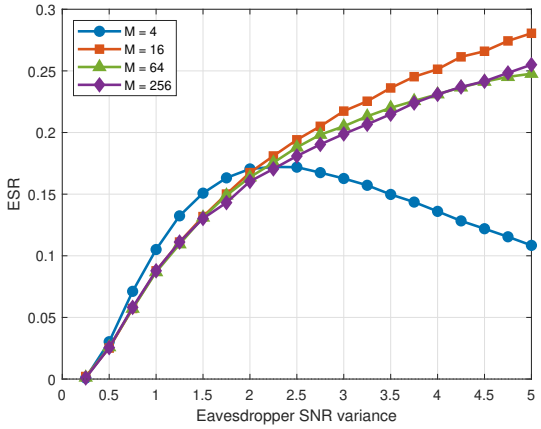

Fig. 2: Exact ESR as a function of the eavesdropper SNR variance for various modulation orders M.

corresponding to channel realizations for which no positive coding rate can ensure secrecy. As K increases, the distribution concentrates around the ESR and approaches a step function, confirming that frequency hopping over a large number of carriers provides an effective self-averaging mechanism that stabilizes the secrecy performance around its statistical mean.

In particular, with the proposed parameters and $K = 256$, if the transmitter selects a coding rate that is 0.2 bit per channel use below the theoretical ESR, the probability that the instantaneous channel realizations result in information leakage to the eavesdropper is less than 10^{-3}.

B. SNR Variance Asymmetry as a Source of Secrecy

Figure 2 depicts the ESR of the FH transmission scheme as a function of the eavesdropper channel variance σ_E^2 for $M \in \{4, 16, 64, 256\}$, with $N_R = N_E = 2$, and $\sigma_\epsilon^2 = 0.2$. The eavesdropper channel undergoes Rayleigh fading, i.e., $g_i \sim \mathcal{CN}(0, \sigma_E^2)$, $i = 1, \ldots, N_E$. To isolate the impact of the eavesdropper SNR variance on the secrecy performance, the average SNRs of the legitimate receiver and the eavesdropper are constrained to be equal.

At low σ_E^2, the eavesdropper SNR variance is comparable to that of the legitimate receiver, resulting in similar SNR distributions for both channels and a secrecy capacity close to zero. Due to the saturation of the mutual information under finite-alphabet inputs, large eavesdropper SNR do not translate into a large eavesdropper rate. As a result, the secrecy capacity becomes strictly positive, confirming that a positive secrecy rate can be achieved when the eavesdropper SNR distribution is more dispersed than that of the legitimate receiver, even if both channels have the same average SNR. The results further show that the optimal modulation order depends on the operating regime. Higher modulation orders tend to achieve larger secrecy capacities at high σ_E^2, as the eavesdropper rate is frequently saturated while the legitimate receiver rate remains relatively unaffected. Conversely, at low σ_E^2, lower

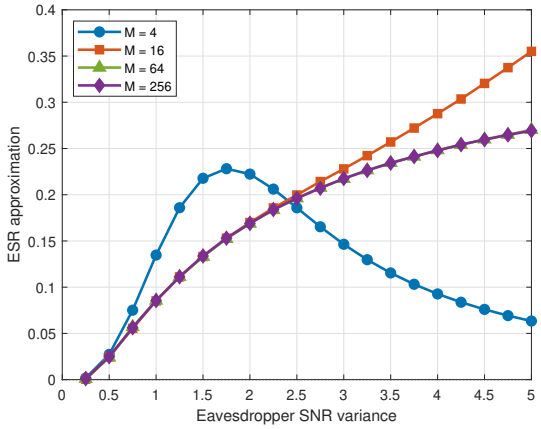

Fig. 3: Approximation of the ESR as a function of the eavesdropper SNR variance for various modulation orders M.

modulation orders tend to be better, as they induce saturation of the eavesdropper channel at lower SNR values. The optimal modulation order M^* therefore represents a trade-off between these two effects.

The ESR approximation introduced in (13) is evaluated in Figure 3. This figure presents the same scenario as Figure 2, but with the ESR computed using the proposed mutual-information approximation for finite inputs. The results show that the approximate and exact curves exhibit very similar trends, indicating that the proposed approximation accurately captures the overall behavior of the ESR. Furthermore, the optimal modulation orders obtained with the approximation match those obtained from the exact computation, demonstrating that Algorithm 1 provides an efficient and near-optimal modulation order selection strategy for secrecy enhancement.

C. Secrecy under Unfavorable Average SNR Conditions

We now show that secrecy can be achieved at a positive rate even when the average eavesdropper SNR is larger than

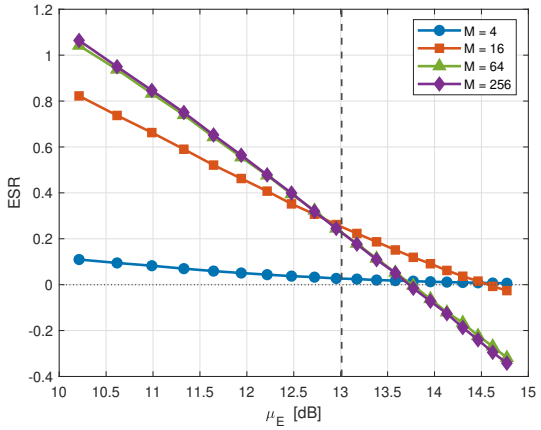

Fig. 4: ESR as a function of the eavesdropper average SNR for various modulation orders M.

the average legitimate receiver SNR. Figure 4 presents the ESR as a function of the eavesdropper average SNR μ_E, for $M \in \{4, 16, 64, 256\}$, $N_R = N_E = 2$, $\sigma_\epsilon^2 = 0.2$, and a fixed eavesdropper SNR spread variance $\sigma_E^2 = 5$. The eavesdropper channel is modeled as a Rician channel. The legitimate channel SNR has a mean equal to $\mu_R = 13$ dB marked by a vertical dashed line. As the average eavesdropper SNR μ_E increases beyond μ_R, the eavesdropper benefits from a better channel on average than the legitimate receiver, which drives the ESR toward zero. However, for $\mu_E < \mu_R$, a strictly positive ESR is observed for all modulation orders, confirming that the FH scheme achieves secrecy when the eavesdropper is weaker on average. Notably, the ESR obtained with the optimal modulation order M^* ($M^* = 16$ in this case) remains positive when μ_E is larger than μ_R by 1.5 dB, owing to the spread asymmetry between ρ_R and ρ_E.

V. Conclusion

This paper has studied the physical layer security of frequency-hopping transmission schemes under the assumption that the hopping sequence is publicly known. The transmitter had access only to a noisy estimate of the legitimate channel and to the statistical distribution of the eavesdropper channel. We have shown that the secrecy capacity of the FH scheme converges to the ergodic secrecy rate when the number of hopping frequencies is large, providing an effective self-averaging mechanism that stabilizes the secrecy performance around its statistical mean regardless of the instantaneous channel realization. We have proposed a simple and analytically tractable condition for the optimal modulation order selection, expressed as an equation on the tail probabilities of the SNR distributions of the legitimate and eavesdropper channels. We have proposed an efficient algorithm for computing the optimal modulation order with low complexity.

A central finding of this work is that the secrecy performance is governed by the spread of the SNR distributions rather than by their means alone. Since the mutual information under finite-alphabet inputs saturates at high SNR, realizations of the eavesdropper SNR that exceed the saturation threshold contribute only marginally to the eavesdropper rate, while the legitimate receiver rate remains relatively unaffected. Consequently, a positive secrecy rate can be achieved even when the eavesdropper has a higher average SNR than the legitimate receiver, as confirmed by the numerical simulations.

Acknowledgement

The authors would like to thank Oudomsack Pierre Pasquero for his very useful comments on this work.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[5] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] F. Oggier and B. Hassibi, "Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

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

[8] C. Leroy, T. Arbi, B. Geller, and O. Rioul, "On the optimum secrecy outage probability and ergodic secrecy rate over wireless channels," preprint *arXiv:2604.22587*, Apr. 2026.

[9] P. K. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[10] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*. Boston, MA, USA: Springer, 2005.

[11] M. M. Olama, X. Ma, T. P. Kuruganti, S. F. Smith, and S. M. Djouadi, "Hybrid DS/FFH spread-spectrum: A robust, secure transmission technique for communication in harsh environments," in *IEEE Military Commun. Conf. (MILCOM)*, Baltimore, MD, USA, 2011, pp. 520–525.

[12] L. C. Robert Sellin and F. Kragh, "A Noise-Masking Physical Layer Security Technique for MIMO Communications Systems," in *IEEE Military Commun. Conf. (MILCOM)*, Los Angeles, CA, USA, 2018, pp. 536-540.

[13] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[14] C. Leroy, T. Arbi, O. P. Pasquero, and B. Geller, "Secrecy through Precoding: a Novel Physical Layer Encryption Scheme with Optimal PAPR," in *IEEE Military Commun. Conf. (MILCOM)*, Los Angeles, CA, USA, 2025, pp. 434-439.

[15] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO Interference Alignment Over Correlated Channels With Imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.

[16] C. Ouyang, A. Bereyhi, S. Asaad, R. R. Müller, J. Cheng, and H. Yang, "On the Ergodic Mutual Information of Keyhole MIMO Channels With Finite-Alphabet Inputs," *IEEE Commun. Lett.*, vol. 27, no. 1, pp. 90–94, Jan. 2023.

[17] K. D. Nguyen, A. Guillén i Fàbregas, and L. K. Rasmussen, "A Tight Lower Bound to the Outage Probability of Discrete-Input Block-Fading Channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4314–4322, Nov. 2007.

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