## IV. Conclusion

The full enumeration of Costas arrays of order $27$ was presented: $204$ arrays were found in total, falling into $29$ equivalence classes. One is a symmetric $T_4, 6$ are $W_2$, and the remaining $21$ are $G_2$, out of which $6$ are symmetric, and one is sporadic.

## Acknowledgment

The authors wish to acknowledge a number of individuals.

- From UCD: Mark Hargaden, Prof. Adrian Ottewill, Aaron Quigley, Gianluca Pollastri, and IT services (in particular Ruth Lynch, Valentin Tchoulkov, and Winnie Ryan) for allowing us to run jobs on their clusters, providing support, and even running our jobs for us.
- The University of Edinburgh's EPCC administration (in particular Lorna Smith and Fiona Reid) for allowing us to use their BlueGene, as well as Liam O'Carroll who mediated and arranged all bureaucratic technicalities for us.

## References

[1] J. K. Beard, J. C. Russo, K. G. Erickson, M. C. Monteleone, and M. T. Wright, "Costas arrays generation and search methodology," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, Apr. 2007.

[2] S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade, "The enumeration of Costas arrays of size 26," in *CISS*, 2006.

[3] J. P. Costas, Medium Constraints on Sonar Design and Performance 1965, Tech. Rep. Class 1 Rep. R65EMH33, GE Co.

[4] J. P. Costas, "A study of detection waveforms having nearly ideal range-doppler ambiguity properties," *Proc. IEEE*, vol. 72, pp. 996–1009, Aug. 1984.

[5] K. Drakakis, "A review of Costas arrays," *J. Appl. Math.*, vol. 2006, 2006.

[6] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combin. Theory Series A*, vol. 37, no. 1, pp. 13–21, 1984.

[7] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, pp. 1143–1163, Sep. 1984.

[8] S. Golomb, "The T4 and G4 constructions for Costas arrays," *IEEE Trans. Inf. Theory*, vol. 38, pp. 1404–1406, Jul. 1992.

[9] K. Drakakis, R. Gow, and L. O'Carroll, "On some properties of Costas arrays generated via finite fields," in *Proc. CISS*, 2006.

[10] J. Beard, Private Communication, 2008.

[11] S. Rickard, "Open problems in Costas arrays," in *Proc. IMA Int. Conf. Math. Signal Processing*, Cirencester, U.K., Dec. 2006.

# On the Secrecy Capacity of Fading Channels

Praveen Kumar Gopala, Lifeng Lai, *Member, IEEE*, and Hesham El Gamal, *Senior Member, IEEE*

***Abstract*—We consider the secure transmission of information over an ergodic fading channel in the presence of an eavesdropper. Our eavesdropper can be viewed as the wireless counterpart of Wyner's wiretapper. The secrecy capacity of such a system is characterized under the assumption of asymptotically long coherence intervals. We first consider the full channel state information (CSI) case, where the transmitter has access to the channel gains of the legitimate receiver and the eavesdropper. The secrecy capacity under this full CSI assumption serves as an upper bound for the secrecy capacity when only the CSI of the legitimate receiver is known at the transmitter, which is characterized next. In each scenario, the perfect secrecy capacity is obtained along with the optimal power and rate allocation strategies. We then propose a low-complexity on/off power allocation strategy that achieves near-optimal performance with only the main channel CSI. More specifically, this scheme is shown to be asymptotically optimal as the average signal-to-noise ratio (SNR) goes to infinity, and interestingly, is shown to attain the secrecy capacity under the full CSI assumption. Overall, channel fading has a positive impact on the secrecy capacity and rate adaptation, based on the main channel CSI, is critical in facilitating secure communications over slow fading channels.**

***Index Terms*—Channel state information (CSI), fading, list decoding, secrecy capacity, wiretap channel.**

## I. Introduction

The notion of information-theoretic secrecy was first introduced by Shannon [1]. This strong notion of secrecy does not rely on any assumptions on the computational resources of the eavesdropper. More specifically, perfect information-theoretic secrecy requires that $I(W;Z) = 0$, i.e., the signal $Z$ received by the eavesdropper does not provide any additional information about the transmitted message $W$. Shannon considered a scenario where both the legitimate receiver and the eavesdropper have direct access to the transmitted signal. Under this model, Shannon proved that the one-time pad scheme achieves perfect secrecy, if the entropy of the private key $K$, used to encrypt the message $W$, is larger than or equal to the entropy of the message itself (i.e., $H(K) \geq H(W)$ for perfect secrecy). Wyner [2] introduced the wiretap channel which accounts for the difference in the two noise processes, as observed by the destination and the wiretapper. In this model, the wiretapper has no computational limitations and is assumed to know the codebook used by the transmitter. Under the assumption that the wiretapper's signal is

Manuscript received October 11, 2006; revised February 25, 2008. Current version published September 17, 2008. The material in this correspondence was presented in part at IEEE International Symposium on Information Theory, Nice, France, June 2007.

P. K. Gopala was with the Department of Electrical and Computer Engineering, the Ohio State University, Columbus, OH 43210 USA. He is now with Nextwave Wireless Inc., San Diego, CA 92130 USA (e-mail: pgopala@nextwave.com).

L. Lai was with the Department of Electrical and Computer Engineering, the Ohio State University, Columbus, OH 43210 USA. He is now with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: llai@princeton.edu).

H. El Gamal is with the Department of Electrical and Computer Engineering, the Ohio State University, Columbus, OH 43210 USA. and also with the Wireless Intelligent Networks Center (WINC), Nile University, Cairo, Egypt (e-mail: helgamal@ece.osu.edu).

Communicated by G. Kramer, Associate Editor for Shannon Theory.

Color versions of Figures 2 and 3 in this correspondence are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.928990

a degraded version of the destination's signal, Wyner characterized the tradeoff between the information rate to the destination and the level of ignorance at the wiretapper (measured by its equivocation), and showed that it is possible to achieve a nonzero secrecy capacity. This work was .later extended to nondegraded channels by Csiszár and Körner [3]

More recently, the effect of slow fading on the secrecy capacity was studied in [4]–[6]. In these works, it is assumed that the fading is quasi-static and the channel state information (CSI) of the eavesdropper and receiver is not available at the source. Under this setup, these papers provide an alternative definition of outage probability, wherein secure communications can be guaranteed for the fraction of time when the main channel is stronger than the channel seen by the eavesdropper. In this correspondence, we focus on delay-tolerant applications which allow for the adoption of an ergodic version of the slow-fading channel, instead of the outage-based formulation. Nonreal time data traffic, such as e-mail and document transmission, are examples of delay-tolerant applications. Quite interestingly, we show in the sequel that, under this model, one can achieve a nonzero perfectly secure rate even when the eavesdropper channel is more capable than the legitimate channel **on the average**. In particular, our work here characterizes the secrecy capacity of the slow-fading channel in the presence of an eavesdropper. Our eavesdropper is the wireless counterpart of Wyner's wiretapper. We first assume that the transmitter knows the CSI of both the legitimate and eavesdropper channels, and derive the optimal power allocation strategy that achieves the secrecy capacity. Next, we consider the case where the transmitter only knows the legitimate channel CSI and, again, derive the optimal power allocation strategy. We then propose an on/off power transmission scheme, with variable-rate allocation, which approaches the optimal performance for asymptotically large average signal-to-noise ratio (SNR). Interestingly, this scheme is also shown to attain the secrecy capacity under the full CSI assumption which implies that, at high-SNR values, the additional knowledge of the eavesdropper CSI does not yield any gains in terms of the secrecy capacity for slow-fading channels. Finally, our theoretical and numerical results are used to argue that rate adaptation plays a more critical role than power control in achieving the secrecy capacity of slow-fading channels. This observation contrasts the scenario without secrecy constraints, where transmission strategies with constant rate are able to achieve capacity [7].

The study of secure communications over fading channels under ergodic setup has also been reported in [8]–[10], in which the result in Theorem 1 was derived concurrently and independently with this correspondence. But, the result for the scenario in which the source does not have CSI of the eavesdropper has not been studied elsewhere. Other than the study of secure communications over fading channels, there has been recently a growing interest in the analysis and design of secure wireless communication networks based on information-theoretic principle. In particular, the secrecy capacity of networks involving relay nodes is studied in [11], [12], while the secrecy capacity of the wiretap channel with feedback is studied by [13]. Multiple-access channels with secrecy constraints are considered in [14]–[17] whereas the broadcast channel scenario is analyzed in [18]. Also, the role of multiple antennas is studied in [19], [20].

## II. System Model

The system model is illustrated in Fig. 1. The source $S$ communicates with a destination $D$ in the presence of an eavesdropper $E$. During any coherence interval $i$, the signal received by the destination and the eavesdropper are given by, respectively

$$y(i) = g_M(i)x(i) + w_M(i)$$
$$z(i) = g_E(i)x(i) + w_E(i)$$

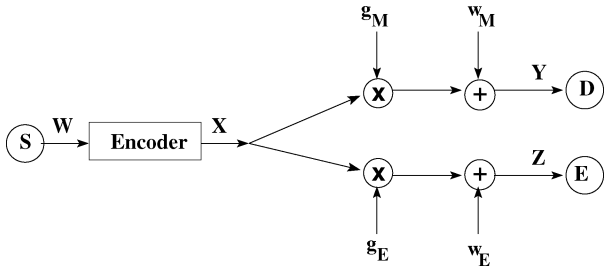


Fig. 1. The fading channel with an eavesdropper.

where $g_M(i), g_E(i)$ are complex channel gains from the source to the legitimate receiver (main channel) and the eavesdropper (eavesdropper channel), respectively, and $w_M(i), w_E(i)$ represent the independent and identically distributed (i.i.d.) additive Gaussian noise with unit variance at the destination and the eavesdropper, respectively. We denote the fading power gains of the main and eavesdropper channels by $h_M(i) = |g_M(i)|^2$ and $h_E(i) = |g_E(i)|^2$, respectively. We assume that both channels experience block fading, where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. The fading process is assumed to be ergodic with a bounded continuous distribution. Moreover, the fading coefficients of the destination and the eavesdropper in any coherence interval are assumed to be independent of each other. We further assume that the number of channel uses $n_1$ within each coherence interval is large enough to allow for invoking random coding arguments. As shown in the sequel, this assumption is instrumental in our achievability proofs.

The source wishes to send a message $W \in \mathcal{W} = \{1, 2, \ldots, M\}$ to the destination. An $(M, n)$ code consists of the following elements: 1) a stochastic encoder $f_n(\cdot)$ at the source that maps the message[1] $w$ to a codeword $x^n \in \mathcal{X}^n$, and 2) a decoding function $\phi$: $\mathcal{Y}^n \to \mathcal{W}$ at the legitimate receiver. The average error probability of an $(M, n)$ code at the legitimate receiver is defined as

$$P_e^n = \sum_{w \in \mathcal{W}} \frac{1}{M} \Pr(\phi(y^n) \neq w | w \text{ was sent}). \tag{1}$$

The equivocation rate $R_e$ at the eavesdropper is defined as the entropy rate of the transmitted message conditioned on the available CSI and the channel outputs at the eavesdropper, i.e.,

$$R_e \triangleq \frac{1}{n} H(W | Z^n, h_M^n, h_E^n) \tag{2}$$

where $h_M^n = \{h_M(1), \ldots, h_M(n)\}$ and $h_E^n = \{h_E(1), \ldots, h_E(n)\}$ denote the channel power gains of the legitimate receiver and the eavesdropper in $n$ coherence intervals, respectively. It indicates the level of ignorance of the transmitted message $W$ at the eavesdropper. In this correspondence, we consider only perfect secrecy which requires the equivocation rate $R_e$ to be equal to the message rate. The perfect secrecy rate $R_s$ is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes $(2^{nR_s}, n)$ such that for any $n \geq n(\epsilon)$, we have

$$P_e^n \leq \epsilon$$
$$R_e = \frac{1}{n} H(W | Z^n, h_M^n, h_E^n) \geq R_s - \epsilon.$$

The secrecy capacity $C_s$ is defined as the maximum achievable perfect secrecy rate, i.e.,

$$C_s \triangleq \sup_{P_e^n \leq \epsilon} R_s. \tag{3}$$

[1]The realizations of the random variables $W, X, Y, Z$ are represented by $w, x, y, z$, respectively, in the sequel.

We note that, as pointed out in [21], the perfect secrecy notion, defined in [2] and adopted in this correspondence, is weaker than the strong sense perfect secrecy requirement as defined in [1] which requires $I(W;Z^n) = 0$. In the definition above, we only require $I(W;Z^n) \leq n\epsilon$. Thus, although $\epsilon \to 0$ as $n$ increases, it is not clear whether $n\epsilon \to 0$ or not. Nevertheless, we follow the convention in the literature and call the secrecy rate that satisfies the definition above as perfect secrecy. Throughout the sequel, we assume that the CSI is known at the destination perfectly. Based on the available CSI, the transmitter adapts its transmission power **and rate** to maximize the perfect secrecy rate subject to a long-term average power constraint $\bar{P}$.

## III. Full CSI at the Transmitter

Here we assume that at the beginning of each coherence interval, the transmitter knows the channel states of the legitimate receiver and the eavesdropper perfectly. When $h_M$ and $h_E$ are both known at the transmitter, one would expect the optimal scheme to allow for transmission only when $h_M > h_E$, and to adapt the transmitted power according to the instantaneous values of $h_M$ and $h_E$. The following result formalizes this intuitive argument.

*Theorem 1:* When the channel gains of both the legitimate receiver and the eavesdropper are known at the transmitter, the secrecy capacity is given by (4) at the bottom of the page, such that

$$\mathbb{E}\{P(h_M,h_E)\} \leq \bar{P}. \tag{5}$$

*Proof:* A detailed proof of achievability and the converse part is provided in the Appendix A. Here, we outline the scheme used in the achievability part. In this scheme, transmission occurs only when $h_M > h_E$, and uses the power allocation policy $P(h_M,h_E)$ that satisfies the average power constraint (5). Moreover, the codeword rate at each instant is set to be $\log(1+h_M P(h_M,h_E))$, which varies according to the instantaneous channel gains. The achievable perfect secrecy rate at any instant is then given [5] by $[\log(1+h_M P(h_M,h_E)) - \log(1+h_E P(h_M,h_E))]^+$, in which $[x]^+ = \max\{x,0\}$. Averaging over all fading realizations, we get the average achievable perfect secrecy rate as shown in the second equation at the bottom of the page. One can then optimize over all feasible power control policies $P(h_M,h_E)$ to maximize the perfect secrecy rate. □

We now derive the optimal power allocation policy that achieves the secrecy capacity under the full CSI assumption. It is easy to check that when $h_M > h_E$

$$f(P) = \log(1+h_M P) - \log(1+h_E P)$$

is concave in $P$. Also, it is well known that nonnegative weighted sums (or integral) preserves concavity [22, Sec. 3.2.1], hence the objective function is concave in $P$. Thus, by using the Lagrangian maximization approach for solving (4), we get the following optimality condition:

$$\frac{\partial R_s^{(F)}}{\partial P(h_M,h_E)} = \frac{h_M}{1+h_M P(h_M,h_E)} - \frac{h_E}{1+h_E P(h_M,h_E)} - \lambda = 0$$

whose solution is

$$P(h_M,h_E) = \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E}-\frac{1}{h_M}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_E}-\frac{1}{h_M}\right)} - \left(\frac{1}{h_M}+\frac{1}{h_E}\right)\right]. \tag{6}$$

If for some $(h_M,h_E)$, the value of $P(h_M,h_E)$ obtained from (6) is negative, then it follows from the concavity of the objective function with respect to (w.r.t.) $P(h_M,h_E)$ that the optimal value of $P(h_M,h_E)$ is 0. Thus, the optimal power allocation policy at the transmitter is given by

$$P(h_M,h_E) = \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E}-\frac{1}{h_M}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_E}-\frac{1}{h_M}\right)} - \left(\frac{1}{h_M}+\frac{1}{h_E}\right)\right]^+ \tag{7}$$

where $[x]^+ = \max\{0,x\}$, and the parameter $\lambda$ is a constant that satisfies the power constraint in (5) with equality. The secrecy capacity is then determined by substituting this optimal power allocation policy for $P(h_M,h_E)$ in (4).

## IV. Only Main Channel CSI at the Transmitter

In this section, we assume that at the beginning of each coherence interval, the transmitter only knows the CSI of the main channel (legitimate receiver).

### A. Optimal Power Allocation

We first characterize the secrecy capacity under this scenario in the following theorem.

*Theorem 2:* When only the channel gain of the legitimate receiver is known at the transmitter, the secrecy capacity is given by (8) at the bottom of the page, such that

$$\mathbb{E}\{P(h_M)\} \leq \bar{P}. \tag{9}$$

$$C_s^{(F)} = \max_{P(h_M,h_E)} \int_0^\infty \int_{h_E}^\infty \left[\log(1+h_M P(h_M,h_E)) - \log(1+h_E P(h_M,h_E))\right] f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \tag{4}$$

$$\begin{aligned} R_s^{(F)} &= \int\int \left[\log(1+h_M P(h_M,h_E)) - \log(1+h_E P(h_M,h_E))\right]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \\ &= \int_0^\infty \int_{h_E}^\infty \left[\log(1+h_M P(h_M,h_E)) - \log(1+h_E P(h_M,h_E))\right] f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \,. \end{aligned}$$

$$C_s^{(M)} = \max_{P(h_M)} \int\int \left[\log(1+h_M P(h_M)) - \log(1+h_E P(h_M))\right]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \tag{8}$$

*Proof:* A detailed proof of achievability and converse part are provided in Appendix B. Here, we outline the scheme used to show achievability. We use the following **variable-rate** transmission scheme. During a coherence interval with main channel fading state $h_M$, the transmitter transmits codewords at rate $\log(1+h_M P(h_M))$ with power $P(h_M)$. This variable-rate scheme relies on the assumption of large coherence intervals and ensures that when $h_E > h_M$, the mutual information between the source and the eavesdropper is upper-bounded by $\log(1+h_M P(h_M))$. When $h_E \leq h_M$, this mutual information will be $\log(1+h_E P(h_M))$. Averaging over all the fading states, the average rate of the main channel is given by

$$\int\int \log\left(1+h_M P(h_M)\right) f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E$$

while the information accumulated at the eavesdropper is

$$\int\int \log\left(1+\min\{h_M, h_E\} P(h_M)\right) f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E.$$

Hence, for a given power control policy $P(h_M)$, the achievable perfect secrecy rate is given by (10), at the bottom of the page. One can then optimize over all feasible power control policies $P(h_M)$ to maximize the perfect secrecy rate. Finally, we observe that our secure message is **hidden** across different fading states (please refer to our proof for more details). □

We now derive the optimal power allocation policy that achieves the secrecy capacity under the main channel CSI assumption. Similar to Theorem 1, the objective function under this case is concave, and using the Lagrangian maximization approach for solving (8), we get the following optimality condition:

$$\frac{\partial R_s^{(M)}}{\partial P(h_M)} = \frac{h_M \Pr(h_E \leq h_M)}{1+h_M P(h_M)} - \int_0^{h_M} \left(\frac{h_E}{1+h_E P(h_M)}\right) f(h_E)\mathrm{d}h_E - \lambda = 0,$$

where $\lambda$ is a constant that satisfies the power constraint in (9) with equality. For any main channel fading state $h_M$, the optimal transmit power level $P(h_M)$ is determined from the above equation. If the obtained power level turns out to be negative, then the optimal value of $P(h_M)$ is equal to 0. This follows from the concavity of the objective function in (8) w.r.t. $P(h_M)$. The solution to this optimization problem depends on the distributions $f(h_M)$ and $f(h_E)$. In the following, we focus on the Rayleigh fading scenario with $\mathbb{E}\{h_M\} = \overline{\gamma}_M$ and $\mathbb{E}\{h_E\} = \overline{\gamma}_E$ in detail. With Rayleigh fading, the objective function in (8) simplifies to (11) at the bottom of the page, where

$$\mathrm{Ei}(x) = \int_x^\infty \frac{e^{-t}}{t}\,\mathrm{d}t.$$

Specializing the optimality conditions to the Rayleigh fading scenario, it can be shown that the power level of the transmitter at any fading state $h_M$ is obtained by solving the equation

$$\left(1-e^{-(h_M/\overline{\gamma}_E)}\right)\left(\frac{h_M}{1+h_M P(h_M)}\right)\lambda - \frac{\left(1-e^{-(h_M/\overline{\gamma}_E)}\right)}{P(h_M)} + \frac{\exp\left(\frac{1}{\overline{\gamma}_E P(h_M)}\right)}{\overline{\gamma}_E (P(h_M))^2}\left[\mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E P(h_M)}\right) - \mathrm{Ei}\left(\frac{h_M}{\overline{\gamma}_E}+\frac{1}{\overline{\gamma}_E P(h_M)}\right)\right] = 0.$$

If there is no positive solution to this equation for a particular $h_M$, then we set $P(h_M) = 0$. The secrecy capacity is then determined by substituting this optimal power allocation policy for $P(h_M)$ in (11).

We observe that, unlike the traditional ergodic fading scenario, achieving the optimal performance under a security constraint relies heavily on using a variable-rate transmission strategy. This can be seen by evaluating the performance of a constant rate strategy where a single codeword is interleaved across infinitely many fading realizations. This interleaving will result in the eavesdropper **gaining more information**, than the destination, when its channel is better than the main channel, thereby yielding a perfect secrecy rate that is strictly smaller than that in (10). It is easy to see that the achievable perfect secrecy rate of the constant rate scheme, assuming a Gaussian codebook, is given by the third equation at the bottom of the page, such that

$$\mathbb{E}\{P(h_M)\} \leq \bar{P}.$$

Unlike the two previous optimization problems, the objective function in this optimization problem is not a concave function of $P(h_M)$. Using the Lagrangian formulation, we only get the following *necessary* Karush–Kuhn–Tucker (KKT) conditions for the optimal point

$$P(h_M)\left[\lambda - \frac{h_M}{1+h_M P(h_M)} + \int \frac{h_E}{1+h_E P(h_M)} f(h_E)\mathrm{d}h_E\right] = 0,$$
$$\lambda \geq \frac{h_M}{1+h_M P(h_M)} - \int \frac{h_E}{1+h_E P(h_M)} f(h_E)\mathrm{d}h_E,$$
$$\mathbb{E}\{P(h_M)\} = \bar{P}. \tag{12}$$

$$R_s^{(M)} = \int\int \left[\log\left(1+h_M P(h_M)\right) - \log\left(1+h_E P(h_M)\right)\right]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E. \tag{10}$$

$$\begin{aligned} C_s^{(M)} &= \max_{P(h_M)} \int_0^\infty \left[\left(1-e^{-(h_M/\overline{\gamma}_E)}\right)\log\left(1+h_M P(h_M)\right) - \int_0^{h_M} \log\left(1+h_E P(h_M)\right)\frac{1}{\overline{\gamma}_E} e^{-(h_E/\overline{\gamma}_E)}\mathrm{d}h_E\right]\frac{1}{\overline{\gamma}_M} e^{-(h_M/\overline{\gamma}_M)}\mathrm{d}h_M \\ &= \max_{P(h_M)} \int_0^\infty \left[\log\left(1+h_M P(h_M)\right) - \exp\left(\frac{1}{\overline{\gamma}_E P(h_M)}\right)\left(\mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E P(h_M)}\right) - \mathrm{Ei}\left(\frac{h_M}{\overline{\gamma}_E}+\frac{1}{\overline{\gamma}_E P(h_M)}\right)\right)\right]\frac{1}{\overline{\gamma}_M} e^{-(h_M/\overline{\gamma}_M)}\mathrm{d}h_M, \end{aligned} \tag{11}$$

$$\max_{P(h_M)} \int\int \left[\log\left(1+h_M P(h_M)\right) - \log\left(1+h_E P(h_M)\right)\right] f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E$$

### B. On/Off Power Control

We now propose a transmission policy wherein the transmitter sends information only when the channel gain of the legitimate receiver $h_M$ exceeds a predetermined constant threshold $\tau > 0$. Moreover, when $h_M > \tau$, the transmitter always uses the same power level $P$. However, it is crucial to adapt the rate of transmission instantaneously as $\log(1+Ph_M)$ with $h_M$. It is clear that for an average power constraint $\bar{P}$, the constant power level used for transmission will be

$$P = \frac{\bar{P}}{\Pr(h_M > \tau)}.$$

From Theorem 2 (since it is true for any form of power control), we know that we can achieve the following perfect secrecy rate using this particular form of power control and Gaussian inputs shown in the first equation at the bottom of the page. Specializing to the Rayleigh fading scenario, we get

$$P = \frac{\bar{P}}{\Pr(h_M > \tau)} = \bar{P}e^{(\tau/\overline{\gamma}_M)}$$

and the secrecy capacity simplifies to the second equation at the bottom of the page, which then simplifies to

$$\begin{aligned} R_s^{(CP)} &= e^{-(\tau/\overline{\gamma}_M)} \log\left(1+\tau\bar{P}e^{(\tau/\overline{\gamma}_M)}\right) \\ &\quad + \exp\left(\frac{1}{\overline{\gamma}_M\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right) \mathrm{Ei}\left(\frac{\tau}{\overline{\gamma}_M} + \frac{1}{\overline{\gamma}_M\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right) \\ &\quad + \exp\left(\frac{1}{\overline{\gamma}_E\bar{P}e^{(\tau/\overline{\gamma}_M)}} - \frac{\tau}{\overline{\gamma}_M}\right) \left[\mathrm{Ei}\left(\frac{\tau}{\overline{\gamma}_E} + \frac{1}{\overline{\gamma}_E\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right)\right. \\ &\qquad \left. - \mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right)\right] \\ &\quad - \exp\left(\frac{\left[\frac{1}{\overline{\gamma}_M}+\frac{1}{\overline{\gamma}_E}\right]}{\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right) \mathrm{Ei}\left(\left[\frac{1}{\overline{\gamma}_M}+\frac{1}{\overline{\gamma}_E}\right]\left[\tau+\frac{1}{\bar{P}e^{(\tau/\overline{\gamma}_M)}}\right]\right). \end{aligned}$$

One can then optimize over the threshold $\tau$ to get the maximum achievable perfect secrecy rate.

Finally, we establish the asymptotic optimality of this on/off scheme as the available average transmission power $\bar{P} \to \infty$. For the on/off power allocation policy, we have

$$R_s^{(CP)} = \lim_{\bar{P}\to\infty} \int_{\tau^*}^{\infty} \int_0^{h_M} \log\left(\frac{1+h_MP}{1+h_EP}\right) f(h_M)f(h_E)\mathrm{d}h_E\mathrm{d}h_M.$$

Taking $\tau^* = 0$, we get $P = \bar{P}$ and (13) at the bottom of the page, where (a) follows from the Dominated Convergence Theorem, since

$$\left|\log\left(\frac{(1/\bar{P})+h_M}{(1/\bar{P})+h_E}\right)\right| \le \left|\log\left(\frac{h_M}{h_E}\right)\right|, \quad \forall \bar{P} \text{ when } h_M > h_E$$

and

$$\int_0^{\infty}\int_0^{h_M} \log\left(\frac{h_M}{h_E}\right) f(h_M)f(h_E)\mathrm{d}h_E\mathrm{d}h_M < \infty$$

since $\mathbb{E}\{h_M\} < \infty$, $\left|\int_0^1 \log x \, \mathrm{d}x\right| = 1 < \infty$, and $f(h_M), f(h_E)$ are continuous and bounded.

Now under the full CSI assumption, we have

$$\begin{aligned} C_s^{(F)} &= \mathbb{E}_{\{h_M>h_E\}}\left\{\log\left(\frac{\frac{1}{P(h_M,h_E)}+h_M}{\frac{1}{P(h_M,h_E)}+h_E}\right)\right\} \\ &\le \mathbb{E}_{\{h_M>h_E\}}\left\{\log\left(\frac{h_M}{h_E}\right)\right\}. \end{aligned} \tag{14}$$

From (13) and (14), it is clear that the proposed on/off power allocation policy that uses only the main channel CSI achieves the secrecy capacity under the full CSI assumption as $\bar{P} \to \infty$. Thus, the absence of eavesdropper CSI at the transmitter does not reduce the secrecy capacity at high SNR values.

## V. Numerical Results

As an additional benchmark, we first obtain the performance when the transmitter does not have any knowledge of both the main and eavesdropper channels (only receiver CSI). In this scenario, the transmitter is unable to exploit rate/power adaptation and always transmits with power $\bar{P}$. It is straightforward to see that the achievable perfect secrecy rate in this scenario (using Gaussian inputs) is given by the first equation at the bottom of the following page. which reduces to the second equation at the bottom of the following page for the Rayleigh fading scenario.Thus, when $\overline{\gamma}_E \ge \overline{\gamma}_M$, $R_s^{(R)} = 0$. The results for the Rayleigh normalized-symmetric case ($\overline{\gamma}_M = \overline{\gamma}_E = 1$) are presented in Fig. 2. It is clear that the performance of the on/off power control scheme is very close to the secrecy capacity (with only main channel

$$R_s^{(CP)} = \int_0^{\infty}\int_{\tau}^{\infty} \left[\log(1+h_MP) - \log(1+h_EP)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E\,.$$

$$R_s^{(CP)} = \int_{\tau}^{\infty}\int_0^{h_M} \left[\log\left(1+h_M\bar{P}e^{(\tau/\overline{\gamma}_M)}\right) - \log\left(1+h_E\bar{P}e^{(\tau/\overline{\gamma}_M)}\right)\right] \frac{1}{\overline{\gamma}_M}e^{-(h_M/\overline{\gamma}_M)}\frac{1}{\overline{\gamma}_E}e^{-(h_E/\overline{\gamma}_E)}\mathrm{d}h_E\mathrm{d}h_M\,,$$

$$\begin{aligned} R_s^{(CP)} &\ge \lim_{\bar{P}\to\infty} \int_0^{\infty}\int_0^{h_M} \log\left(\frac{(1/\bar{P})+h_M}{(1/\bar{P})+h_E}\right) f(h_M)f(h_E)\mathrm{d}h_E\mathrm{d}h_M \\ &\overset{(a)}{=} \int_0^{\infty}\int_0^{h_M} \lim_{\bar{P}\to\infty} \log\left(\frac{(1/\bar{P})+h_M}{(1/\bar{P})+h_E}\right) f(h_M)f(h_E)\mathrm{d}h_E\mathrm{d}h_M \\ &= \int_0^{\infty}\int_0^{h_M} \log\left(\frac{h_M}{h_E}\right) f(h_M)f(h_E)\mathrm{d}h_E\mathrm{d}h_M = \mathbb{E}_{\{h_M>h_E\}}\left\{\log\left(\frac{h_M}{h_E}\right)\right\} \end{aligned} \tag{13}$$

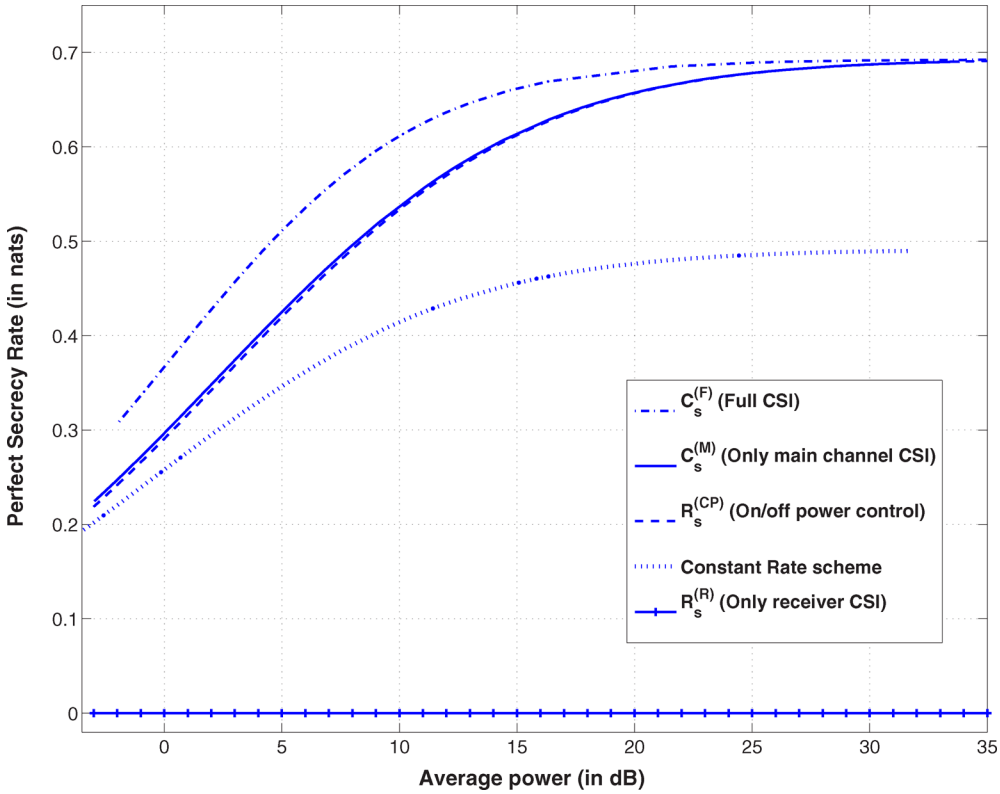


Fig. 2. Performance comparison for the symmetric scenario $\overline{\gamma}_M = \overline{\gamma}_E = 1$.

CSI) for a wide range of SNRs and, as expected, approaches the secrecy capacities, under both the full CSI and main channel CSI assumptions, at high values of SNR. The performance of the constant rate scheme is much worse than other schemes that employ rate adaptation. Here we note that the performance curve for the constant rate scheme might be a lower bound to the secrecy capacity (since the KKT conditions are necessary but not sufficient for nonconvex optimization). We then consider an asymmetric scenario, wherein the eavesdropper channel is more capable than the main channel, with $\overline{\gamma}_M = 1$ and $\overline{\gamma}_E = 2$. The performance results for this scenario are plotted in Fig. 3. Again it is clear from the plot that the performance of the on/off power control scheme is optimal at high values of SNR, and that rate adaptation schemes yield higher perfect secrecy rates than constant rate transmission schemes.

## VI. Conclusion

We have characterized the secrecy capacity of the slow-fading channel with an eavesdropper under different assumptions on the available transmitter CSI. Our work establishes the interesting result that a nonzero perfectly secure rate is achievable in the fading channel even when the eavesdropper is more capable than the legitimate receiver (on the average). By contrasting this conclusion with the traditional additive white Gaussian noise (AWGN) scenario, one can see the positive impact of fading on **enhancing** the secrecy capacity. Furthermore, we proposed a low-complexity on/off power transmission scheme and established its asymptotic optimality. This optimality shows that the presence of eavesdropper CSI at the transmitter does not offer additional gains in the secrecy capacity for slow-fading channels, at high enough SNR levels. The knowledge of the main channel CSI, however, is crucial since it is easy to see that the absence of this information leads to a zero secrecy capacity when the eavesdropper is more capable than the legitimate receiver on the average. Finally, our theoretical and numerical results established the critical role of appropriate rate adaptation in facilitating secure communications over slow fading channels.

## Appendix A
## Proof of Theorem 1

We first prove the achievability of (4) by showing that for any perfect secrecy rate $R_s < C_s^{(F)}$, there exists a sequence of $(2^{nR_s}, n)$ block codes with average power $\bar{P}$, equivocation rate $R_e > R_s - \epsilon$, and probability of error $P_e^n \to 0$ as $n \to \infty$. Let $R_s = C_s^{(F)} - 3\delta$ for some

$$R_s^{(R)} = \left[\int_0^\infty \int_0^\infty \left[\log\left(1+h_M\bar{P}\right) - \log\left(1+h_E\bar{P}\right)\right] f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E\right]^+$$
$$= \left[\int_0^\infty \log\left(1+h_M\bar{P}\right) f(h_M)\mathrm{d}h_M - \int_0^\infty \log\left(1+h_E\bar{P}\right) f(h_E)\mathrm{d}h_E\right]^+$$

$$R_s^{(R)} = \left[\exp\left(\frac{1}{\overline{\gamma}_M\bar{P}}\right)\mathrm{Ei}\left(\frac{1}{\overline{\gamma}_M\bar{P}}\right) - \exp\left(\frac{1}{\overline{\gamma}_E\bar{P}}\right)\mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E\bar{P}}\right)\right]^+.$$

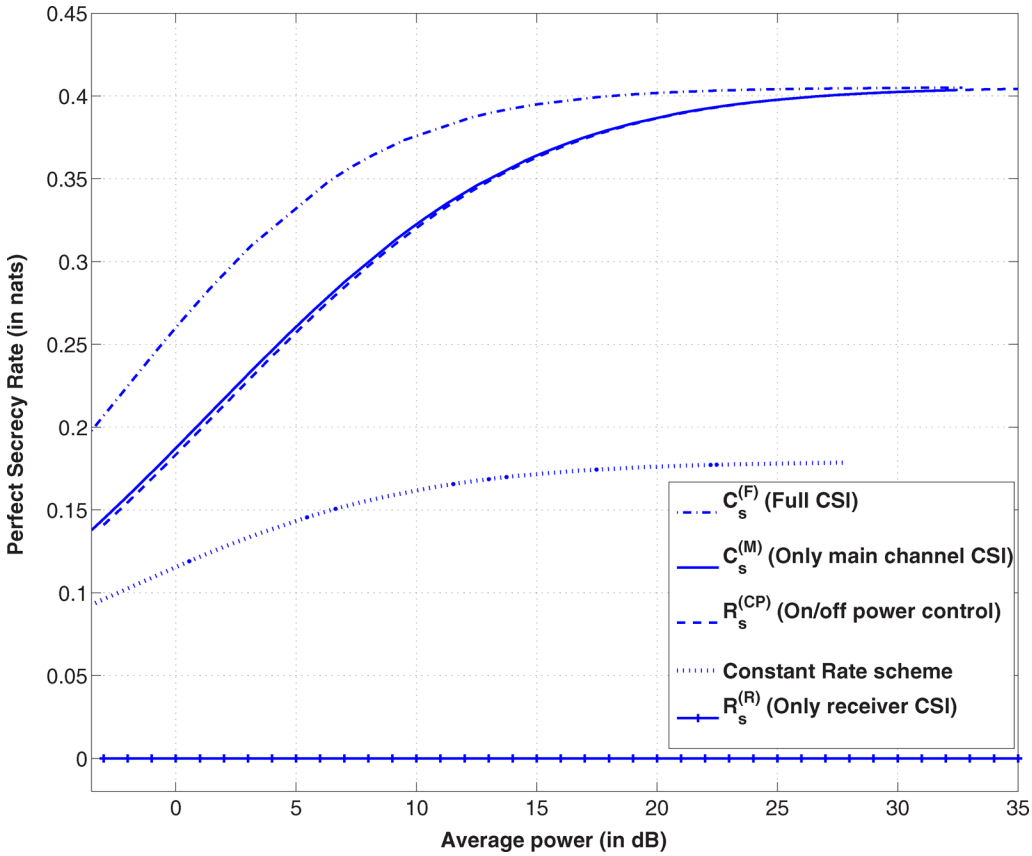


Fig. 3. Performance comparison for the asymmetric scenario $\overline{\gamma}_M = 1$ and $\overline{\gamma}_E = 2$.

$\delta > 0$. We quantize the main channel gains $h_M \in [0, M_1]$ into uniform bins $\{h_{M,i}\}_{i=1}^{q_1}$, and the eavesdropper channel gains $h_E \in [0, M_2]$ into uniform bins $\{h_{E,j}\}_{j=1}^{q_2}$. Here, the term "uniform bins" means that all the bins have the same length. The channels are said to be in state $s_{ij}$ ($i \in [1, q_1]$, $j \in [1, q_2]$), if $h_{M,i} \leq h_M < h_{M,(i+1)}$ and $h_{E,j} \leq h_E < h_{E,(j+1)}$, where $h_{M,(q_1+1)} = M_1, h_{E,(q_2+1)} = M_2$. We also define a power control policy for any state $s_{ij}$ by

$$P(h_{M,i}, h_{E,j}) = \inf_{h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}} P(h_M, h_E) \tag{15}$$

where $P(h_M, h_E)$ is the optimal power allocation policy in (7) that satisfies $P(h_M, h_E) = 0$ for all $h_M \leq h_E$, and the power constraint

$$\int_0^\infty \int_{h_E}^\infty P(h_M, h_E) f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \leq \bar{P}. \tag{16}$$

Consider a time-invariant AWGN channel with channel gains $h_M \in [h_{M,i}, h_{M,(i+1)})$ and $h_E \in [h_{E,j}, h_{E,(j+1)})$. It is shown in [17], [23] that for this channel, we can develop a sequence of $(2^{n_{ij}(R_s)_{ij}}, n_{ij})$ codes with codeword rate $\log(1 + h_{M,i} P(h_{M,i}, h_{E,j}))$ and perfect secrecy rate

$$(R_s)_{ij} = \Big[\log(1 + h_{M,i} P(h_{M,i}, h_{E,j})) - \log\left(1 + h_{E,(j+1)} P(h_{M,i}, h_{E,j})\right)\Big]^+ \tag{17}$$

such that the average power is $P(h_{M,i}, h_{E,j})$ and with error probability $P_e^{ij} \to 0$ as $n_{ij} \to \infty$, where

$$n_{ij} = n \Pr\left(h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}\right)$$

for sufficiently large $n$. Note that the expression in (17) is obtained by considering the worst case scenario $h_M = h_{M,i}, h_E = h_{E,(j+1)}$ that yields the smallest perfect secrecy rate.

For transmitting the message index $w \in \{1, \ldots, 2^{nR_s}\}$, we first map $w$ to the indices $\{w_{ij}\}$ by dividing the $nR_s$ bits which determine the message index into sets of $n_{ij}(R_s)_{ij}$ bits. The transmitter uses a multiplexing strategy and transmits codewords $\{x_{w_{ij}}\}$ at codeword rate

$$\log(1 + h_{M,i} P(h_{M,i}, h_{E,j}))$$

and perfect secrecy rate $(R_s)_{ij}$, when the channel is in state $s_{ij}$. As $n \to \infty$, this scheme achieves the perfect secrecy rate (using the ergodicity of the channel), as shown in the equation at the bottom of the page.

The equivocation calculation is similar and is actually simpler than that of the proof in Theorem 2. For simplicity, we omit it here.

$$R_s = \sum_{i=1}^{q_1} \sum_{j=1}^{q_2} \left[\log\left(\frac{1 + h_{M,i} P(h_{M,i}, h_{E,j})}{1 + h_{E,(j+1)} P(h_{M,i}, h_{E,j})}\right)\right]^+ \Pr\left(h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}\right).$$

Thus, for a fixed $\delta$, we can find a sufficiently large $n$ such as shown in (18) at the bottom of the page. For asymptotically large $n$, using the ergodicity of the channel, the average power of the multiplexing scheme satisfies the second equation at the bottom of the page, where (a) follows from the definition of $P(h_{M,i}, h_{E,j})$ in (15) and (b) follows from (16). Moreover, the error probability of the multiplexing scheme is upper-bounded by

$$P_e^n \leq \sum_{i=1}^{q_1}\sum_{j=1}^{q_2} P_e^{ij} \to 0, \quad \text{as } n \to \infty.$$

Now since $C_s^{(F)}$ is as shown in the third the equation at the bottom of the page (because $\mathbb{E}\{h_M\} < \infty$, $\left|\int_0^1 \log x \, \mathrm{d}x\right| = 1 < \infty$, and $f(h_M), f(h_E)$ are continuous and bounded), there exist $M_1$ and $M_2$ for a fixed $\delta$ such that we get (19) at the bottom of the page. Moreover, for fixed $M_1$ and $M_2$, the dominated convergence theorem implies (20), at the bottom of the page. Choosing $M_1, M_2$ that satisfy (19) and combining (19) and (20), we see that for a given $\delta$, there exist sufficiently large $q_1, q_2$ such that we get (21) at the bottom of the page. Combining (18) and (21), we get the desired result.

We now prove the converse part by showing that for any perfect secrecy rate $R_s$ with equivocation rate $R_e > R_s - \epsilon$ and error prob-

$$R_s \geq \sum_{i=1}^{q_1}\sum_{j=1}^{q_2}\left[\log\left(\frac{1+h_{M,i}P(h_{M,i},h_{E,j})}{1+h_{E,(j+1)}P(h_{M,i},h_{E,j})}\right)\right]^+ \Pr\left(h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}\right) - \delta. \tag{18}$$

$$\begin{aligned}\sum_{i=1}^{q_1}\sum_{j=1}^{q_2} P(h_{M,i},h_{E,j}) \int_{h_{M,i}}^{h_{M,(i+1)}} \int_{h_{E,j}}^{h_{E,(j+1)}} f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E \\ \overset{(a)}{\leq} \int_0^\infty \int_0^\infty P(h_M,h_E)f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E \overset{(b)}{\leq} \bar{P}\end{aligned}$$

$$\begin{aligned}C_s^{(F)} &= \int_0^\infty \int_0^\infty \left[\log\left(1+h_M P(h_M,h_E)\right) - \log\left(1+h_E P(h_M,h_E)\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E \\ &\leq \int_0^\infty \int_{h_E}^\infty \log\left(\frac{h_M}{h_E}\right) f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E < \infty\end{aligned}$$

$$\begin{aligned}&\int_0^{M_1}\int_{M_2}^\infty \left[\log\left(1+h_M P(h_M,h_E)\right) - \log\left(1+h_E P(h_M,h_E)\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E < \frac{\delta}{3} \\ &\int_{M_1}^\infty\int_0^{M_2} \left[\log\left(1+h_M P(h_M,h_E)\right) - \log\left(1+h_E P(h_M,h_E)\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E < \frac{\delta}{3} \\ &\int_{M_1}^\infty\int_{M_2}^\infty \left[\log\left(1+h_M P(h_M,h_E)\right) - \log\left(1+h_E P(h_M,h_E)\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E < \frac{\delta}{3}.\end{aligned} \tag{19}$$

$$\begin{aligned}&\lim_{(q_1,q_2)\to\infty} \sum_{i=1}^{q_1}\sum_{j=1}^{q_2}\left[\log\left(\frac{1+h_{M,i}P(h_{M,i},h_{E,j})}{1+h_{E,(j+1)}P(h_{M,i},h_{E,j})}\right)\right]^+ \\ &\Pr(h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}) \\ &\quad = \lim_{(q_1,q_2)\to\infty} \sum_{i=1}^{q_1}\sum_{j=1}^{q_2} \int_{h_{M,i}}^{h_{M,(i+1)}} \int_{h_{E,j}}^{h_{E,(j+1)}} \left[\log\left(\frac{1+h_{M,i}P(h_{M,i},h_{E,j})}{1+h_{E,(j+1)}P(h_{M,i},h_{E,j})}\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E \\ &\quad = \int_0^{M_1}\int_0^{M_2} \left[\log\left(\frac{1+h_M P(h_M,h_E)}{1+h_E P(h_M,h_E)}\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E.\end{aligned} \tag{20}$$

$$\begin{aligned}&\sum_{i=1}^{q_1}\sum_{j=1}^{q_2}\left[\log\left(\frac{1+h_{M,i}P(h_{M,i},h_{E,j})}{1+h_{E,(j+1)}P(h_{M,i},h_{E,j})}\right)\right]^+ \Pr\left(h_{M,i} \leq h_M < h_{M,(i+1)}, h_{E,j} \leq h_E < h_{E,(j+1)}\right) \\ &\quad \geq \int_0^\infty\int_0^\infty \left[\log\left(\frac{1+h_M P(h_M,h_E)}{1+h_E P(h_M,h_E)}\right)\right]^+ f(h_M)f(h_E)\mathrm{d}h_M\mathrm{d}h_E - 2\delta.\end{aligned} \tag{21}$$

ability $P_e^n \to 0$ as $n \to \infty$, there exists a power allocation policy $P(h_M, h_E)$ satisfying the average power constraint, shown in the first equation at the bottom of the page. Consider any sequence of $(2^{nR_s}, n)$ codes with perfect secrecy rate $R_s$ and equivocation rate $R_e$, such that $R_e > R_s - \epsilon$, with average power less than or equal to $\bar{P}$ and error probability $P_e^n \to 0$ as $n \to \infty$. Let $N(h_M, h_E)$ denote the number of times the channel is in fading state $(h_M, h_E)$ over the interval $[0, n]$. Also let

$$P^n(h_M, h_E) = \mathbb{E}\left\{\sum_{i=1}^{n} |x_w(i)|^2 \mathbf{1}_{\{h_M(i)=h_M, h_E(i)=h_E\}}\right\}$$

where $\{x_w\}$ are the codewords corresponding to the message $w$ and the expectation is taken over all codewords. We note that the equivocation $H(W|Z^n, h_M^n, h_E^n)$ only depends on the marginal distribution of $Z^n$, and thus does not depend on whether $Z(i)$ is a physically or stochastically degraded version of $Y(i)$ or *vice versa*. Hence, we assume in the following derivation that for any fading state, either $Z(i)$ is a physically degraded version of $Y(i)$ or *vice versa* (since the noise processes are Gaussian), depending on the instantaneous channel state. Thus, we have (22) at the bottom of the page. In the derivation (22), (a) follows from the Fano inequality, (b) follows from the data processing inequality since $W \to X^n \to (Y^n, Z^n)$ forms a Markov chain, (c) follows from the fact that conditioning does not increase entropy and from the memoryless property of the channel, and (d) follows from the fact that given $h_M$ and $h_E$, the fading channel reduces to an AWGN channel with channel gains $(h_M, h_E)$ and average transmission power $P^n(h_M, h_E)$, for which

$$I(X;Y|Z, h_M, h_E) \le [\log(1 + h_M P^n(h_M, h_E)) - \log(1 + h_E P^n(h_M, h_E))]^+$$

as shown in [17], [23]. Since the codewords satisfy the power constraint, we have

$$\int\int P^n(h_M, h_E)\left(\frac{N(h_M, h_E)}{n}\right) \mathrm{d}h_M \mathrm{d}h_E \le \bar{P}.$$

For any $h_M, h_E$ such that $f(h_M, h_E) \neq 0$, $\{P^n(h_M, h_E)\}$ are bounded sequences in $n$. Thus there exists a subsequence that converges to a limit $P(h_M, h_E)$ as $n \to \infty$. Since for each $n$, the power constraint is satisfied, we have

$$\int\int P(h_M, h_E) f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \le \bar{P}. \tag{23}$$

Now, we have $R_e$ defined in the third equation at the bottom of the page. Taking the limit along the convergent subsequence and using the ergodicity of the channel, we get the fourth equation at the bottom page.

The claim is thus proved for sufficiently large $n$. Now, if there exists a code with finite length $n$ that can achieve a larger perfect secrecy

$$R_s \le \int\int [\log(1 + h_M P(h_M, h_E)) - \log(1 + h_E P(h_M, h_E))]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E.$$

$$\begin{aligned}
nR_e &= H(W|Z^n, h_M^n, h_E^n) \\
&\overset{(a)}{\le} H(W|Z^n, h_M^n, h_E^n) - H(W|Z^n, Y^n, h_M^n, h_E^n) + n\delta_n \\
&= I(W; Y^n|Z^n, h_M^n, h_E^n) + n\delta_n \\
&\overset{(b)}{\le} I(X^n; Y^n|Z^n, h_M^n, h_E^n) + n\delta_n \\
&= H(Y^n|Z^n, h_M^n, h_E^n) - H(Y^n|X^n, Z^n, h_M^n, h_E^n) + n\delta_n \\
&= \sum_{i=1}^{n}\left[H(Y(i)|Y^{i-1}, Z^n, h_M^n, h_E^n) - H(Y(i)|Y^{i-1}, X^n, Z^n, h_M^n, h_E^n)\right] + n\delta_n \\
&\overset{(c)}{\le} \sum_{i=1}^{n}[H(Y(i)|Z(i), h_M(i), h_E(i)) - H(Y(i)|X(i), Z(i), h_M(i), h_E(i))] + n\delta_n \\
&= \sum_{i=1}^{n} I(X(i); Y(i)|Z(i), h_M(i), h_E(i)) + n\delta_n \\
&= \sum_{i=1}^{n}\int\int I(X;Y|Z, h_M, h_E)\mathbf{1}_{\{h_M(i)=h_M, h_E(i)=h_E\}} \mathrm{d}h_M \mathrm{d}h_E + n\delta_n \\
&= \int\int I(X;Y|Z, h_M, h_E) N(h_M, h_E) \mathrm{d}h_M \mathrm{d}h_E + n\delta_n \\
&\overset{(d)}{\le} \int\int N(h_M, h_E)\,[\log(1 + h_M P^n(h_M, h_E)) - \log(1 + h_E P^n(h_M, h_E))]^+ \,\mathrm{d}h_M \mathrm{d}h_E + n\delta_n.
\end{aligned} \tag{22}$$

$$R_e \le \int\int \frac{N(h_M, h_E)}{n}\left[\log\left(\frac{1 + h_M P^n(h_M, h_E)}{1 + h_E P^n(h_M, h_E)}\right)\right]^+ \mathrm{d}h_M \mathrm{d}h_E + \delta_n.$$

$$R_e \le \int\int \left[\log\left(\frac{1 + h_M P(h_M, h_E)}{1 + h_E P(h_M, h_E)}\right)\right]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E + \delta_n.$$

rate than (4), one can concatenate these codes with small length $n$ to a code with sufficiently large length and achieve a perfect secrecy rate larger than (4). This is in contradiction with the claim we proved for sufficiently large $n$. Hence, there does not exist a code with finite length $n$ that can achieve a perfect secrecy rate larger than (4). This completes the proof.

## Appendix B
## Proof of Theorem 2

Let $R_s = C_s^{(M)} - \delta$ for some small $\delta > 0$. Let $n = n_1 m$, where $n_1$ represents the number of symbols transmitted in each coherence interval, and $m$ represents the number of coherence intervals over which the message $W$ is transmitted. Let $R = \mathbb{E}\{\log(1 + h_M P(h_M))\} - \epsilon$. We first generate all binary sequences $\{\boldsymbol{V}\}$ of length $nR$ and then independently assign each of them randomly to one of $2^{nR_s}$ groups, according to a uniform distribution. This ensures that any of the sequences are equally likely to be within any of the groups. Each secret message $w \in \{1, \ldots, 2^{nR_s}\}$ is then assigned a group $\boldsymbol{V}(w)$. To encode a particular message $w$, the stochastic encoder randomly selects a sequence $\boldsymbol{v}$ from the corresponding group $\boldsymbol{V}(w)$, according to a uniform distribution. Thus, $\boldsymbol{V}$ is uniformly distributed over $\{0,1\}^{nR_s}$, and hence, its coordinates are i.i.d. uniform binary random variables [24]. This sequence $\boldsymbol{v}$ consisting of $nR$ bits is then subdivided into independent blocks $\{\boldsymbol{v}(1), \ldots, \boldsymbol{v}(m)\}$, where the block $\boldsymbol{v}(i)$ consists of $n_1 [\log(1 + h_M(i)P(h_M(i))) - \epsilon]$ bits, and is transmitted in the $i$th coherence interval ($i \in \{1, \ldots, m\}$). As $m \to \infty$, using the ergodicity of the channel, we have

$$\lim_{m\to\infty} \sum_{i=1}^{m} n_1 [\log(1 + h_M(i)P(h_M(i))) - \epsilon] = n_1 m [\mathbb{E}\{\log(1 + h_M P(h_M))\} - \epsilon] = nR.$$

We then generate i.i.d. Gaussian codebooks $\{X^{n_1}(i) : i = 1, \ldots, m\}$ consisting of $2^{n_1[\log(1+h_M(i)P(h_M(i)))-\epsilon]}$ codewords, each of length $n_1$ symbols. In the $i$th coherence interval, the transmitter encodes the block $\boldsymbol{v}(i)$ into the codeword $x^{n_1}(i)$, which is then transmitted over the fading channel. The legitimate receiver receives $y^{n_1}(i)$ while the eavesdropper receives $z^{n_1}(i)$ in the $i$th coherence interval. The equivocation rate at the eavesdropper can then be lower-bounded as follows:

$$\begin{aligned}
nR_e &= H(W|Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\
&= H(W, Z^{n_1}(1), \ldots, Z^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(Z^{n_1}(1), \ldots, Z^{n_1}(m)|h_M^n, h_E^n) \\
&= H(W, Z^{n_1}(1), \ldots, Z^{n_1}(m), X^{n_1}(1), \ldots, X^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(Z^{n_1}(1), \ldots, Z^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&= H(X^{n_1}(1), \ldots, X^{n_1}(m)|h_M^n, h_E^n) \\
&\quad + H(W, Z^{n_1}(1), \cdots, Z^{n_1}(m)|X^{n_1}(1), \cdots, X^{n_1}(m), h_M^n, h_E^n) \\
&\quad - H(Z^{n_1}(1), \ldots, Z^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\geq H(X^{n_1}(1), \ldots, X^{n_1}(m)|h_M^n, h_E^n) \\
&\quad + H(Z^{n_1}(1), \cdots, Z^{n_1}(m)|X^{n_1}(1), \cdots, X^{n_1}(m), h_M^n, h_E^n) \\
&\quad - H(Z^{n_1}(1), \ldots, Z^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&= H(X^{n_1}(1), \ldots, X^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - I(Z^{n_1}(1), \cdots, Z^{n_1}(m); X^{n_1}(1), \cdots, X^{n_1}(m)|h_M^n, h_E^n) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&= H(X^{n_1}(1), \cdots, X^{n_1}(m)|Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\overset{(a)}{=} \sum_{i=1}^{m} H(X^{n_1}(i)|Z^{n_1}(i), h_M(i), h_E(i)) \\
&\quad - H(X^{n_1}(1), \cdots, X^{n_1}(m)|W, Z^{n_1}(1), \cdots, Z^{n_1}(m), h_M^n, h_E^n).
\end{aligned}$$

Here, (a) follows from the memoryless property of the channel and the independence of the $X^{n_1}(i)$'s.

We continue with (24) at the bottom of the page. In the derivation (24), (b) is obtained by removing all those terms which correspond to the coherence intervals $i \notin \mathcal{N}_m$, where $\mathcal{N}_m = \{i \in \{1, \ldots, m\} : h_M(i) > h_E(i)\}$, and (c) follows from the ergodicity of the channel as $m \to \infty$.

Now we show that the term

$$H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n)$$

vanishes as $m, n_1 \to \infty$ by using a list decoding argument. In this list decoding, at coherence interval $i$, the eavesdropper first constructs a list $\mathcal{L}_i$ such that $x^{n_1}(i) \in \mathcal{L}_i$ if $(x^{n_1}(i), z^{n_1}(i))$ are jointly typical. Let $\mathcal{L} = \mathcal{L}_1 \times \mathcal{L}_2 \times \cdots \times \mathcal{L}_m$. Given $w$, the eavesdropper declares that $\hat{x}^n = (x^{n_1}(1), \ldots, x^{n_1}(m))$ was transmitted, if $\hat{x}^n$ is the only

$$\begin{aligned}
nR_e &\overset{(b)}{\geq} \sum_{i\in\mathcal{N}_m} H(X^{n_1}(i)|Z^{n_1}(i), h_M(i), h_E(i)) \\
&\quad - H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\
&= \sum_{i\in\mathcal{N}_m} [H(X^{n_1}(i)|h_M(i), h_E(i)) - I(X^{n_1}(i); Z^{n_1}(i)|h_M(i), h_E(i))] \\
&\quad - H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\geq \sum_{i\in\mathcal{N}_m} n_1 [\log(1 + h_M(i)P(h_M(i))) - \log(1 + h_E(i)P(h_M(i))) - \epsilon] \\
&\quad - H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\geq \sum_{i=1}^{m} n_1 \{[\log(1 + h_M(i)P(h_M(i))) - \log(1 + h_E(i)P(h_M(i)))]^+ - \epsilon\} \\
&\quad - H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\
&\overset{(c)}{=} nC_s^{(M)} - H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) - n\epsilon. \qquad (24)
\end{aligned}$$

codeword such that $\hat{x}^n \in B(w) \cap \mathcal{L}$, where $B(w)$ is the set of codewords corresponding to the message $w$. If the eavesdropper finds none or more than one such sequence, then it declares an error. Hence, there are two type of error events: 1) $\mathcal{E}_1$: the transmitted codeword $x_t^n$ is not in $\mathcal{L}$, 2) $\mathcal{E}_2$: $\exists x^n \neq x_t^n$ such that $x^n \in B(w) \cap \mathcal{L}$. Thus, the error probability $\Pr(\hat{x}^n \neq x_t^n) = \Pr(\mathcal{E}_1 \cup \mathcal{E}_2) \leq \Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2)$. Based on the asymptotic equipartition property (AEP), we know that $\Pr(\mathcal{E}_1) \leq \epsilon_1$. In order to bound $\Pr(\mathcal{E}_2)$, we first bound the size of $\mathcal{L}_i$. We let

$$\phi_i(x^{n_1}(i)|z^{n_1}(i)) = \begin{cases} 1, & \text{when } (x^{n_1}(i),\ z^{n_1}(i)) \text{ are jointly typical,} \\ 0, & \text{otherwise.} \end{cases} \tag{25}$$

Now

$$\begin{aligned} &\mathbb{E}\{\|\mathcal{L}_i\|\} \\ &= \mathbb{E}\left\{ \sum_{x^{n_1}(i)} \phi_i(x^{n_1}(i)|z^{n_1}(i)) \right\} \\ &\leq \mathbb{E}\left\{ 1 + \sum_{x^{n_1}(i) \neq x_t^{n_1}(i)} \phi_i(x^{n_1}(i)|z^{n_1}(i)) \right\} \\ &\leq 1 + \sum_{x^{n_1}(i) \neq x_t^{n_1}(i)} \mathbb{E}\{\phi_i(x^{n_1}(i)|z^{n_1}(i))\} \\ &\leq 1 + 2^{n_1[\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i))) - \epsilon]} \\ &\leq 2^{n_1\left([\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i)))-\epsilon]^+ + \frac{1}{n_1}\right)}. \end{aligned} \tag{26}$$

Hence we get (27) at the bottom of the page. Thus, we have (28), also at the bottom of the page, where (a) follows from the uniform distribution of the codewords in $B(w)$. Now as $n_1 \to \infty$ and $m \to \infty$, we get

$$\Pr(\mathcal{E}_2) \leq 2^{-n(C_s - \delta - C_s + c\epsilon)} = 2^{-n(c\epsilon - \delta)}$$

where $c = \Pr(h_M > h_E)$. Thus, by choosing $\epsilon > (\delta/c)$, the error probability $\Pr(\mathcal{E}_2) \to 0$ as $n \to \infty$. Now using Fano's inequality, we get

$$\begin{aligned} &H(X^{n_1}(1), \ldots, X^{n_1}(m)|W, Z^{n_1}(1), \ldots, Z^{n_1}(m), h_M^n, h_E^n) \\ &\qquad \leq n\delta_n \to 0, \quad \text{as } n \to \infty. \end{aligned}$$

Combining this with (24), we get the desired result.

For the converse part, consider any sequence of $(2^{nR_s}, n)$ codes with perfect secrecy rate $R_s$ and equivocation rate $R_e$, such that $R_e > R_s - \epsilon$, with average power less than or equal to $\bar{P}$ and error probability $P_e^n \to 0$ as $n \to \infty$. We follow the same steps used in the proof of the converse in Theorem 1 with the only difference that now the transmission power $P^n(\cdot)$ only depends on $h_M$. From (22), we get the third equation at the bottom of the page. This follows from the fact that given $h_M$ and $h_E$, the fading channel reduces to an AWGN channel with channel gains $(h_M, h_E)$ and average transmission power $P^n(h_M)$, for which Gaussian inputs are known to be optimal [17], [23].

Similar to the proof of Theorem 1, we take the limit over the convergent subsequence and use the ergodicity of the channel to obtain (29) at the bottom of the page, where $\mathbb{E}\{P(h_M)\} \leq \bar{P}$. The claim is proved for sufficiently large $n$. Following the same argument as that of

$$\mathbb{E}\{\|\mathcal{L}\|\} = \prod_{i=1}^{m} \mathbb{E}\{\|\mathcal{L}_i\|\} \leq 2^{\sum_{i=1}^{m} n_1\left([\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i)))-\epsilon]^+ + \frac{1}{n_1}\right)}. \tag{27}$$

$$\begin{aligned} \Pr(\mathcal{E}_2) &\leq \mathbb{E}\left\{ \sum_{x^n \in \mathcal{L}, x^n \neq x_t^n} \Pr(x^n \in B(w)) \right\} \\ &\overset{(a)}{\leq} \mathbb{E}\left\{ \|\mathcal{L}\| 2^{-nR_s} \right\} \\ &\leq 2^{-nR_s} 2^{\sum_{i=1}^{m} n_1\left([\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i)))-\epsilon]^+ + \frac{1}{n_1}\right)} \\ &\leq 2^{-n\left(R_s - \frac{1}{m}\sum_{i=1}^{m}\left([\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i)))-\epsilon]^+ + \frac{1}{n_1}\right)\right)} \\ &= 2^{-n\left(R_s - \frac{1}{m}\sum_{i=1}^{m}\left([\log(1+h_M(i)P(h_M(i))) - \log(1+h_E(i)P(h_M(i)))]^+ + \frac{1}{n_1}\right) + \frac{|\mathcal{N}_m|\epsilon}{m}\right)} \end{aligned} \tag{28}$$

$$\begin{aligned} nR_e &\leq \sum_{i=1}^{n} \int\int I(X;Y|Z,h_M,h_E)\mathbf{1}_{\{h_M(i)=h_M, h_E(i)=h_E\}} \mathrm{d}h_M \mathrm{d}h_E + n\delta_n \\ &= \int\int I(X;Y|Z,h_M,h_E) N(h_M,h_E) \mathrm{d}h_M \mathrm{d}h_E + n\delta_n \\ &\leq \int\int N(h_M,h_E) \left[\log(1 + h_M P^n(h_M)) - \log(1 + h_E P^n(h_M))\right]^+ \mathrm{d}h_M \mathrm{d}h_E + n\delta_n. \end{aligned}$$

$$R_e \leq \int\int \left[\log(1 + h_M P(h_M)) - \log(1 + h_E P(h_M))\right]^+ f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E + \delta_n, \tag{29}$$

Theorem 1, we have that there does not exist a code with finite length $n$ that can achieve a larger perfect secrecy rate than (8). The proof is complete.

## REFERENCES


[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, 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] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 356–360.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[7] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1468–1489, May 1999.

[8] Z. Li, R. Yates, and W. Trappe, "Secure communication over wireless channels," in *Proc. Information Theory and Application Workshop*, La Jolla, CA, Jan. 2007.

[9] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep. 2006.

[10] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[11] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep. 2001, pp. 87–89.

[12] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[13] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, to be published.

[14] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, submitted for publication.

[15] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep. 2006.

[16] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[17] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[18] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[19] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, submitted for publication.

[20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, submitted for publication.

[21] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. Advances in Cryptology-EUROCRYPT*, Bruges, Brugge, Belgium, May 2000, pp. 356–373.

[22] S. Boyd and L. Vandenberghe, *Convex Optimization*. London, U.K.: Cambridge Univ. Press, 2004.

[23] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[24] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.


# Capacity Achieving LDPC Codes Through Puncturing


Chun-Hao Hsu, *Student Member, IEEE*, and Achilleas Anastasopoulos, *Member, IEEE*



***Abstract*—The performance of punctured low-definition parity-check (LDPC) codes under maximum-likelihood (ML) decoding is studied in this correspondence via deriving and analyzing their average weight distributions (AWDs) and the corresponding asymptotic growth rate of the AWDs. In particular, it is proved that capacity-achieving codes of any rate and for any memoryless binary-input output-symmetric (MBIOS) channel under ML decoding can be constructed by puncturing some original LDPC code with small enough rate. Moreover, it is shown that the gap to capacity of all the punctured codes can be the same as the original code with a small enough rate. Conditions under which puncturing results in no rate loss with asymptotically high probability are also given in the process. These results show high potential for puncturing to be used in designing capacity-achieving codes, and in rate-compatible coding under any MBIOS channel.**



***Index Terms*—Asymptotic growth rate, average weight distribution, capacity-achieving codes, low-density parity-check (LDPC) codes, maximum-likelihood (ML) decoding, punctured codes, rate-adaptable codes.**


## I. INTRODUCTION

Low-density parity-check codes (LDPC), originally introduced by Gallager in the early 1960s [1], were the first successful example of capacity-achieving codes with linear decoding complexity. In particular, LDPC codes were shown in [2]–[4] to achieve the capacity of the binary erasure channel (BEC) using iterative decoding with linear decoding complexity with respect to the codeword length. A necessary condition for these LDPC codes to be capacity-achieving as proved in [5] is that their parity-check matrix density (normalized to the number of information bits) diverges to infinity as capacity is approached. Specifically, the density grows at least as $\log(1/\epsilon)$ with respect to the multiplicative gap to capacity $\epsilon$ [5]. Recently, a family of turbo-like codes, namely, irregular repeat–accumulate (IRA) codes were shown in [6] to be capacity achieving for the BEC with constant complexity with respect to $\epsilon$.

Regarding non-BEC channels, there are several examples of capacity-achieving codes for memoryless binary-input output-symmetric (MBIOS) channels. For instance, Forney's concatenated codes [7] are provably capacity achieving, but require a polynomial decoding complexity in the codeword length. Similarly, expander codes were shown to be capacity achieving for the binary symmetric channel (BSC) in [8]. Although the decoding complexity of expander codes is linear in the codeword length, it grows as $\exp(1/\epsilon)$. LDPC codes were shown in [5] to achieve the capacity of any MBIOS channel using maximum-likelihood (ML) decoding, the necessary condition


Manuscript received November 26, 2006; revised March 21, 2008. Current version published September 17, 2008. This work was supported in part by the National Science Foundation under Grant CAREER-CCF-0346977. The material in this correspondence was presented in part at the International Conference on Wireless Networks, Communications, and Mobile Computing, Maui, HI, June 2005.



Ch.-H. Hsu is with Qualcomm, Inc., Santa Clara, CA 95054 USA (e-mail: chhsu@umich.edu).

A. Anastasopoulos is with the Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109-2122 USA (e-mail: anastas@umich.edu).



Communicated by T. J. Richardson, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2008.928274