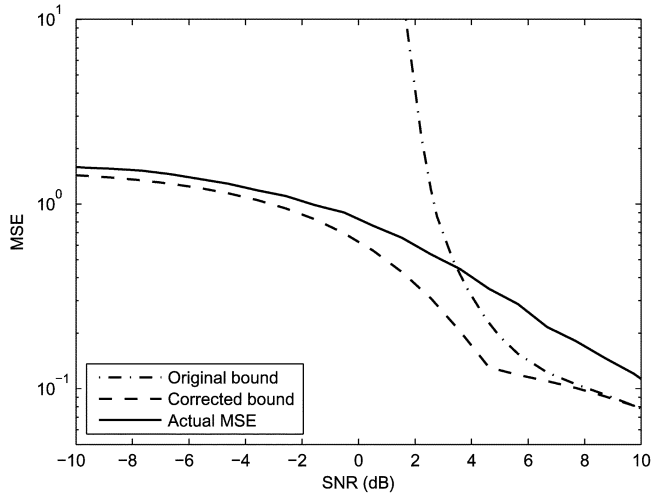

Fig. 1. Plot of the corrected WWB (24), the incorrect version (6), and the actual MSE, for a scalar estimation setting with a disjoint set Θ.

This problem is illustrated in Fig. 1, where the incorrect bound (6) is compared with the original WWB (4), which can be written as

$$\frac{h^2 e^{2\mu(s,h)}}{e^{\mu(2s,h)} + e^{\mu(2-2s,-h)} - 2\tilde{M}(s,h)}. \tag{24}$$

The actual MSE obtained by the optimal estimator can be calculated using Monte Carlo simulations, and is also plotted. In the figure, values of $a = 1/2$ and $b = 2$ were used. The variance σ^2 was modified to obtain various signal-to-noise ratios (SNRs), where $\mathrm{SNR} = \mathrm{Var}(\theta)/\sigma^2$.

It is evident from Fig. 1 that the value (6) becomes exceedingly high at low SNR. Indeed, for SNR values below approximately 0 dB, there always exist values of s and h such that the denominator of (6) is arbitrarily small, and thus the bound tends to infinity. For SNR values around 2–4 dB, (6) yields finite values which are larger than the actual MSE obtained by the optimal estimator. The original version (24), by contrast, closely follows the true MSE value.

ACKNOWLEDGMENT

The authors are grateful to Prof. A. J. Weiss and Prof. E. Weinstein for carefully reviewing an early version of this correspondence.

REFERENCES

[1] H. L. Van Trees, *Detection, Estimation, and Modulation Theory*. New York: Wiley, 1968, vol. 1.

[2] J. Ziv and M. Zakai, "Some lower bounds on signal parameter estimation," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 3, pp. 386–391, May 1969.

[3] A. J. Weiss and E. Weinstein, "A lower bound on the mean-square error in random parameter estimation," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 5, pp. 680–682, Sep. 1985.

[4] E. Weinstein and A. J. Weiss, "A general class of lower bounds in parameter estimation," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 338–342, Mar. 1988.

[5] T. J. Nohara and S. Haykin, "Application of the Weiss-Weinstein bound to a two-dimensional antenna array," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 36, no. 9, pp. 1533–1534, Sep. 1988.

[6] D. F. DeLong, Use of the Weiss-Weinstein Bound to Compare the Direction-Finding Performance of Sparse Arrays Lincoln Lab, Mass. Inst. Tech, Cambridge, MA, 1993, Tech. Rep. 982.

[7] K. L. Bell, "Performance Bounds in Parameter Estimation With Application to Bearing Estimation," Ph.D. dissertation, George Mason University, Fairfax, VA, 1995.

Results of the Enumeration of Costas Arrays of Order 27

Konstantinos Drakakis, *Member, IEEE*,
Scott Rickard, *Senior Member, IEEE*,
James K. Beard, *Life Senior Member, IEEE*, Rodrigo Caballero,
Francesco Iorio, Gareth O'Brien, and John Walsh

***Abstract*—This correspondence presents the results of the enumeration of Costas arrays of order 27: all arrays found, except for one, are accounted for by the Golomb and Welch construction methods.**

***Index Terms*—Costas arrays, enumeration, Golomb method, order 27, Welch method.**

I. INTRODUCTION

In this brief note we present the results of the enumeration of Costas arrays of order 27. This result comes approximately 2.5 years after the last major enumeration project of Costas arrays undertaken, namely that for order 26, completed independently and by two different groups led by J. K. Beard [1] and S. Rickard [2], respectively. Our project was run on various supercomputers in Ireland [GridIreland[1], which actually ran 68.75% of the project, and some clusters in University College Dublin (Halation[2], Meteorite[3], Rowan)] and Scotland [the University of Edinburgh's EPCC's BlueGene[4]], as well as on several other private machines. Taking a CPU running at 2.00GHz as a reference, the project required approximately 25 years of single

Manuscript received May 23, 2008; revised June 16, 2008. Current version published September 17, 2008. This material was supported by the Science Foundation Ireland under Grant 05/YI2/I677.

K. Drakakis is with the School of Mathematics, University College Dublin, Belfield, Dublin 4, Ireland. He is also now with the Claude Shannon Institute and University College Dublin, Belfield, Dublin 4, Ireland (e-mail: konstantinos.drakakis@ucd.ie).

S. Rickard is with the School of Electrical, Electronic and Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland. He is also with the Claude Shannon Institute and University College Dublin, Belfield, Dublin 4, Ireland (e-mail: scott.rickard@ucd.ie).

J. K. Beard is an independent consultant (e-mail: jkbeard@ieee.org).

R. Caballero and G. O'Brien are with the School of Mathematics, University College Dublin, Belfield, Dublin 4, Ireland (e-mail: rodrigo.caballero@ucd.ie, gareth.obrien@ucd.ie).

F. Iorio is with the IBM Systems and Technology Group, IBM Technology Campus, Damastown Industrial Park, Mulhuddart, Dublin 15, Ireland (e-mail: francesco_iorio@ie.ibm.com).

J. Walsh is with the Department of Computer Science, Trinity College Dublin, College Green, Dublin 2, Ireland (e-mail: John.Walsh@cs.tcd.ie).

Communicated by G. Gong, Associate Editor for Sequences.

Color version Figure 1 in this correspondence are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.928979

[1]http://www.grid-ireland.org

[2]http://www.ucd.ie/itservices/researchit/services/clusters

[3]Internal UCD clusters

[4]http://www.epcc.ed.ac.uk/

TABLE I
THE LEXICOGRAPHICALLY MINIMAL REPRESENTATIVES OF THE EQUIVALENCE CLASSES OF COSTAS ARRAYS OF ORDER 27, SHOWN ALONG WITH THE METHOD THAT PRODUCES THEM: ONE IS T_4 AND IS SYMMETRIC, 6 ARE W_2, 21 ARE G_2 (6 OF WHICH ARE SYMMETRIC), AND ONE IS SPORADIC. A/s NEXT TO THE METHOD SYMBOL INDICATES THAT THE EQUIVALENCE CLASS IS SYMMETRIC

1 3 7 15 2 5 11 23 18 8 17 6 13 27 26 24 20 12 25 22 16 4 9 19 10 21 14	W_2
1 3 19 12 23 5 25 20 10 16 13 27 11 15 2 9 14 8 21 22 18 17 26 6 4 7 24	G_2
1 8 22 18 16 5 23 17 14 19 12 20 26 25 7 10 11 27 3 15 2 21 13 24 9 4 6	G_2
1 25 19 5 4 12 10 16 26 7 18 6 23 27 24 8 21 11 3 22 17 20 13 15 2 9 14	G_2/s
2 3 14 12 21 5 18 20 26 16 4 27 24 15 1 9 19 8 23 22 25 17 10 6 13 7 11	G_2
2 8 26 22 10 3 11 6 20 4 14 15 18 27 25 19 1 5 17 24 16 21 7 23 13 12 9	W_2
2 17 14 12 7 19 18 20 26 16 4 13 24 1 15 23 5 8 9 22 11 3 10 6 27 21 25	G_2
2 20 3 8 23 7 10 5 1 9 13 22 21 27 18 16 4 25 14 15 17 11 24 6 26 12 19	G_2
2 20 17 8 9 21 10 19 15 23 27 22 7 13 18 16 4 11 14 1 3 25 24 6 26 12 5	G_2
2 24 16 4 14 7 5 13 12 1 6 18 27 3 22 8 19 9 15 11 26 23 25 10 17 20 21	G_2
2 24 16 4 14 21 19 27 12 15 6 18 13 17 22 8 5 23 1 25 26 9 11 10 3 20 7	G_2
2 25 8 13 3 23 12 5 19 20 18 22 14 1 27 4 21 16 26 6 17 24 10 9 11 7 15	W_2
3 9 1 8 13 15 19 4 2 20 11 25 5 17 6 27 14 24 7 10 26 23 22 18 12 21 16	G_2/s
3 15 6 10 18 8 9 2 13 19 21 26 11 25 12 7 5 27 16 23 22 4 24 20 1 17 14	W_2
3 17 6 19 18 16 22 26 20 27 11 12 5 23 14 2 10 7 9 24 1 4 15 25 21 13 8	G_2
3 24 10 26 20 15 13 23 14 1 8 4 22 19 21 2 5 25 9 17 6 7 11 16 27 12 18	G_2/s
4 3 7 23 25 16 11 12 15 21 26 22 14 1 27 20 9 17 24 6 18 8 2 13 10 19 5	G_2
4 7 24 22 2 25 10 6 21 20 14 5 26 27 3 15 1 12 18 8 17 9 19 16 23 11 13	G_2
4 17 21 9 11 16 25 12 1 7 26 22 14 15 13 20 23 3 24 6 18 8 2 27 10 5 19	G_2/s
5 13 11 25 20 4 22 24 18 7 6 2 3 23 8 12 21 27 15 26 1 16 9 19 10 17 14	G_2
5 15 11 4 3 25 13 16 22 24 9 23 27 19 10 17 14 12 21 26 6 1 18 2 20 7 8	G_2
5 21 11 18 2 23 19 10 13 24 1 27 3 17 16 25 12 20 22 4 26 15 7 8 14 9 6	G_2
5 25 10 26 2 4 15 22 3 13 7 6 9 23 20 21 27 17 8 1 18 16 12 24 11 19 14	W_2
6 10 23 13 16 1 11 20 15 2 7 26 4 27 9 5 19 25 17 8 24 22 3 21 18 12 14	T_4/s
6 16 20 12 14 7 1 25 8 17 18 26 11 23 10 24 15 13 3 19 22 27 5 2 9 4 21	G_2/s
6 16 20 12 14 21 15 11 8 3 18 26 25 9 10 24 1 27 17 5 22 13 19 2 23 4 7	G_2
6 23 14 8 21 1 26 4 22 20 12 11 16 3 17 13 15 24 27 10 5 9 2 18 25 7 19	G_2/s
7 5 18 6 26 12 16 19 14 3 2 23 17 27 20 22 9 21 1 15 11 8 13 24 25 4 10	W_2
11 10 4 24 7 23 3 18 21 9 26 16 5 1 15 27 2 25 17 22 19 6 8 12 20 13 14	

CPU time to complete (the memory and storage requirements of the code used were minimal).

II. BASICS

Let us begin with the definition of a Costas function/permutation [3]–[5].

Definition 1: Let $[n] := \{1, \ldots, n\}, n \in \mathbb{N}$ and consider a bijection $f : [n] \to [n]$; f is a Costas permutation if and only if

$$\forall\, i, j, k \text{ such that } 1 \leq i, j, i+k, j+k \leq n :$$
$$f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j \text{ or } k = 0.$$

Permutations correspond to permutation arrays by setting the elements of the permutation to denote the positions of the (unique) 1 in the corresponding column of the array, counting from top to bottom: $f(i) = j \Leftrightarrow a_{j,i} = 1$. For example, the array shown in Fig. 1 corresponds to the permutation $526\,134$. It is customary to represent the 1's of a permutation array as "dots" and the 0's as "blanks". The terms "array" and "permutation" will henceforth be used interchangeably.

The Costas property is invariant under rotations of the array by 90°, horizontal and vertical flips, and flips around the diagonals, hence a Costas array gives birth to an equivalence class that contains either 8 Costas arrays, or 4 if the array happens to be symmetric; in the latter case, we say the equivalence class is symmetric. When presenting the results of the enumeration, we will give the lexicographically minimal representative from each equivalence class for brevity.

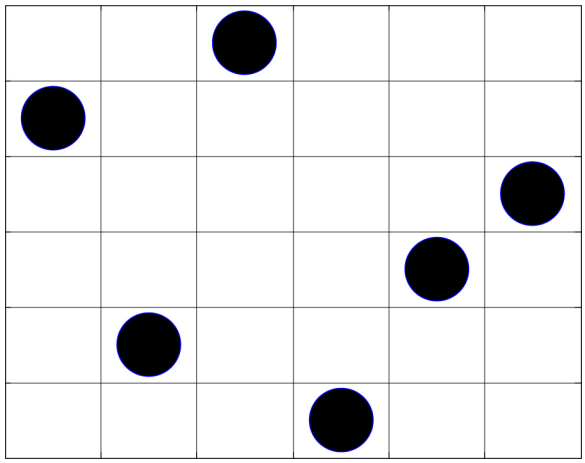

Fig. 1. The Costas array of order 6 corresponding to the permutation $526\,134$.

There exist two algebraic methods for the construction of Costas arrays, known as the Golomb and Welch methods [5]–[8].

Theorem 1 (Welch Construction $W_1(p, g, c)$): Let p be a prime, let g be a primitive root of the finite field $\mathbb{F}(p)$ of p elements, and let $c \in [p-1] - 1$ be a constant; then, the function $f : [p-1] \to [p-1]$ where $f(i) = g^{i-1+c} \bmod p$ is a bijection with the Costas property.

Note that W_1 arrays for $p > 5$ are never symmetric [9].

Theorem 2 (Welch Construction $W_2(p, g)$): Let p be a prime, and let g be a primitive root of the finite field $\mathbb{F}(p)$ of p elements; then,

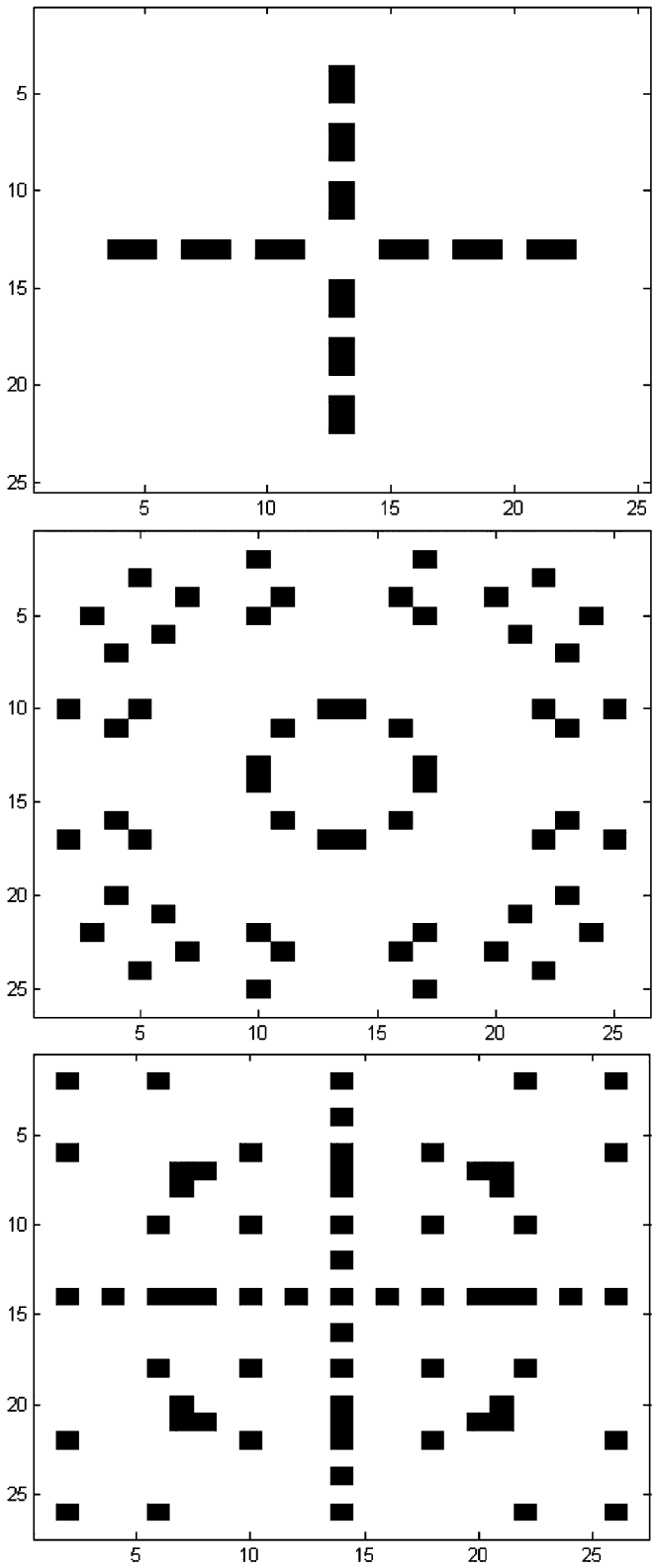

Fig. 2. Forbidden positions for a Costas array of order $25, 26$, and 27 (top to bottom).

the function $h : [p-1] \to [p-1]$ generated by $W_1(p, g, 0)$ is a bijection with the Costas property such that $h(1) = 1$. This implies that $f : [p-2] \to [p-2]$ where $f(i) = h(i+1) - 1, i \in [p-2]$ is a bijection with the Costas property.

In other words, $W_2(p, g)$ follows from $W_1(p, g, 0)$ by removing the left column and the top row, whose common element (the top left corner) is 1. This construction is always possible.

Theorem 3 (Golomb Construction $G_2(p, m, a, b)$): Let p be a prime, $m \in \mathbb{N}$, and let a, b be primitive roots of the finite field $\mathbb{F}(p^m)$ of $q = p^m$ elements; then, the function $f : [q-2] \to [q-2]$ where $a^{f(i)} + b^i = 1$ is a bijection with the Costas property.

If $m = 1$, G_2 arrays are symmetric iff $a = b$ [9]; this special case is known as the Lempel construction [5].

Theorem 4 (Golomb-Taylor Construction $T_4(p, m)$): Let p be a prime, $m \in \mathbb{N}$, and let a be a primitive root of the finite field $\mathbb{F}(p^m)$ of $q = p^m$ elements with the property that $a^2 + a = 1$; then, the corresponding $G_2(p, m, a, a)$ function $g : [q-2] \to [q-2]$ satisfies $g(1) = 2$ and $g(2) = 1$, and, consequently, the function $f : [q-4] \to [q-4]$ where $f(i) = g(i+2) - 2, i \in [q-4]$, is a bijection with the Costas property.

In other words, $T_4(p, m)$ follows from $G_2(p, m, a, a)$, when $a^2 + a = 1$, by removing the top two rows and left two columns, whose intersection, the top left corner 2×2 square has its nondiagonal elements equal to 1. This construction is not always possible as such a may not exist in the field [8].

Costas arrays not constructed by either of these two methods are commonly referred to as "sporadic."

III. Results and Analysis

The enumeration found in total 204 Costas arrays, divided into 29 equivalence classes: their lexicographically minimal members are shown in Table I. Out of those, we have the following.

- One is a $T_4(31, 1)$ and is symmetric.
- 6 are $W_2(29, g)$ for the various primitive roots of $\mathbb{F}(29)$. There are $\phi(28) = 12$ such primitive roots, and they produce 12 $W_1(29, g, 0)$ arrays, which correspond to equivalence classes in pairs related by a vertical flip, or, equivalently, generated by inverse primitive roots [9], hence there are 6 such equivalence classes. The removal of the corner dot shows that W_1-equivalence classes correspond bijectively to W_2-equivalence classes.
- 21 are $G_2(29, 1, a, b)$ for the various choices of primitive roots a and b: there are $\phi(28) = 12$ such primitive roots. Choosing them to be equal produces 12 symmetric arrays, which fall in equivalence classes in pairs, hence there are 6 symmetric classes. The remaining 15 classes contain 8 arrays each and are not symmetric.
- One is sporadic[5] and is not symmetric.

Out of the above, four are Costas arrays of order 26 extended by the addition of a corner dot (three G_2, one of which symmetric, and one W_2). Note that, in agreement with Section I, all symmetric Costas arrays are Lempel-constructed, with the exception of the T_4 array, which is produced by removing two corner dots from a Lempel-generated Costas array.

Efficiency improvement of the search methodology led to the consideration of forbidden positions for the dots of Costas arrays for different orders (an idea introduced in [11]). Fig. 2 shows the forbidden positions for Costas arrays of order 27: if a dot of a permutation array of order 27 corresponds to a black square, this array cannot be Costas. This figure is obtained by superposing all Costas arrays of order 27 and observing which elements host no dot. The corresponding results for orders 25 and 26 (first shown in [11]) are also offered for comparison purposes; for orders $n = 1, 2$ and $4 \leq n \leq 24$, there are no forbidden positions: for $n = 3$ the middle position $(2, 2)$ is forbidden.

[5]The existence of this array was first noted by J. K. Beard [10].

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