Physical-Layer Secrecy in AWGN via a Class of Chaotic DS/SS Systems: Analysis and Design

Yongsun Hwang, *Student Member, IEEE,* and Haralabos C. Papadopoulos, *Member, IEEE*

***Abstract*—We study a class of pseudo-chaotic spread spectrum systems for secure communication over additive white Gaussian noise (AWGN) channels, whereby a symbol stream is linearly modulated on a spreading sequence generated by iterating an initial condition through a suitably chosen chaotic map. We compare the uncoded probability of error ($\Pr(\epsilon)$) attainable by intended receivers that know the initial condition to the associated $\Pr(\epsilon)$ of unintended receivers that know the modulation scheme but not the initial condition. The sensitive dependence of chaotic sequences on initial conditions, together with the presence of channel noise, can be exploited to provide substantially lower $\Pr(\epsilon)$ to intended than to unintended receivers. We develop computationally efficient methods for obtaining tight bounds on the best $\Pr(\epsilon)$ performance of intended and unintended receivers. In the process, we identify chaotic map attributes that affect the relative $\Pr(\epsilon)$ advantages provided to intended receivers and develop methods for designing maps that achieve a target gap between the intended and unintended receiver $\Pr(\epsilon)$.**

***Index Terms*—Chaos, security, spread spectrum communication.**

I. Introduction

In this paper, we examine the physical-layer secrecy potential of a class of pseudo-chaotic direct sequence spread spectrum (DS/SS) systems for communication over additive white Gaussian noise (AWGN) channels. In particular, we consider linear modulation schemes on spreading sequences arising from a class of one-dimensional (1-D) piecewise-linear chaotic maps and investigate the relative probability of error ($\Pr(\epsilon)$) performance advantages these systems provide to intended receivers over unintended ones. In the process, we identify chaotic map properties that affect the $\Pr(\epsilon)$ gap between intended and unintended receivers and construct methods for designing maps that optimize these $\Pr(\epsilon)$ performance gaps.

The subject of communication based on chaotic systems has received considerable attention in the last decade. The first communication system employing chaos was reported by Cuomo *et al.* [1] and pertains to a chaotic signal-masking technique that employs chaotic systems decomposable into drive and response subsystems and exploits synchronization of the two (transmitter/receiver) subsystems to a common coupled signal [2]–[4]. Since chaotic sequences have broadband spectra and excellent auto- and cross-correlation properties, they are also well suited as spreading sequences in DS/SS and multiuser communication applications. Chaotic DS/SS systems were originally suggested by Heidari-Bateni and McGillem [5]. Since then, two main classes of methods for incorporating chaotic dynamics into DS/SS systems have emerged. The first class includes methods, whereby a continuous-time chaotic waveform is used as both modulating carrier and spreading signal [6], and where synchronization of two chaotic circuitries is exploited to reliably demodulate the information-bearing signal. The latter class employs spreading sequences based on trajectories from 1-D chaotic maps. Such spreading sequences can be multilevel sequences generated by quantizing the original chaotic sequences [5], [7]–[12], unstable periodic orbits [13], or binary sequences suitably obtained from underlying chaotic sequences, e.g., by exploiting the base-2 representation of numbers in the unit interval [14]. A lot of emphasis in the aforementioned works has been on the performance of legitimate communicating pairs in a multiuser environment. The statistics of chaotic sequences have been analyzed, and the correlation properties of some class of such sequences were found to outperform those of binary-valued pseudonoise (PN) sequences [7], [9], [12]. In particular, it was shown that code division multiple access (CDMA) systems employing time-varying pseudo-chaotic spreading sequences can provide improvements in (intended) user $\Pr(\epsilon)$ with respect to their conventional CDMA counterparts (employing binary-valued PN spreading sequences). Indeed, for many of these systems, cochannel interference characteristics and the associated bit error probabilities of intended receivers have been evaluated and found to compare favorably to those of existing CDMA systems [7], [10], [11]. One such attractive example involves CDMA systems where all users employ spreading sequences generated by the same map but from distinct initial conditions.

In this paper, we focus on single-user DS/SS systems with pseudochaotic spreading sequences and explore the $\Pr(\epsilon)$ benefits these systems can provide to intended receivers over their unintended counterparts that do not know the seed used to generate the chaotic spreading sequence. We develop computationally efficient approximations and associated bounds for the $\Pr(\epsilon)$ of intended and unintended receivers and obtain relationships between various system parameters and receiver performance. Such relationships are then exploited to design systems that optimize the relative $\Pr(\epsilon)$ advantages provided to intended users. As we show, these systems can be designed to provide substantially worse $\Pr(\epsilon)$ performance to unintended receivers, in contrast to conventional DS/SS (assuming the seed used to generate the binary-valued PN spreading sequence is

Manuscript received January 31, 2003; revised October 9, 2003. This work was supported by the DoD-ARO under Award DAAD19-01-1-0494. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Nicholas D. Sidiropoulos.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (email: yeongsun@eng.umd.edu; babis@eng.umd.edu)

Digital Object Identifier 10.1109/TSP.2004.832029

not made available to unintended receivers). Our single-user analysis also suggests the $\Pr(\epsilon)$ advantage trends available to intended users in multiuser chaotic DS/CDMA systems.

The discrete-time baseband model of the chaotic DS/SS transmitters of interest is shown in Fig. 1 and involves a symbol stream $b[n]$ that is modulated on a sequence $c[n]$, generated by iterating an initial condition $c[0]$ through a 1-D chaotic map. The inherent privacy potential of these systems is due to the combined effect of channel distortion and the sensitive dependence on initial conditions of chaotic trajectories. Due to the deterministic nature of chaotic dynamics, knowledge of the initial condition allows reconstruction of the spreading sequence, rendering the initial condition an ideal candidate for the key made available to intended users. The key allows the intended receiver to reconstruct the spreading sequence and form a (time-varying) matched-filter detector, in the same manner that intended receivers in conventional DS/SS systems use the initial seed to reconstruct, via a linear feedback shift-register (LFSR), the spreading PN sequence that is used in forming a matched-filter detector.

Although, for properly designed chaotic DS/SS systems with moderate/large spreading gains, the intended receiver $\Pr(\epsilon)$ performance is similar to that of their conventional DS/SS counterparts, as we show, chaotic DS/SS can result in substantially higher $\Pr(\epsilon)$ for unintended receivers that do not know the initial condition. Specifically, unintended receivers without the key face a composite detection problem, whereby, under each hypothesis, the unknown spreading sequence lies within an enormous set of valid chaotic trajectories. For the class of chaotic spreading sequences we consider, due to their sensitive dependence on initial conditions, consistent estimates of these spreading sequences cannot be formed from their noisy observations. Furthermore, not only these estimates are not efficient, but the ratio of the estimate error variance over the associated Cramér–Rao lower bound grows exponentially fast with the length of the observed sequence for chip energy-to-noise ratios ($\mathcal{E}_c/N_o$) below a certain high threshold [15]. These properties are consistent with the fact that the number of local maxima of the likelihood function increases exponentially with the length of the sequence. In contrast, the seed of conventional binary-valued PN spreading sequences from known LFSRs can be consistently estimated based on noisy observations; indeed, simple suboptimal estimators of the initial state of the LFSR can correctly identify the seed with very high probability based on just a fraction of the sequence period, even at very low $\mathcal{E}_c/N_o$ [16], [17].

Quantized chaotic system implementations are required to ensure that the number of bits needed to describe the key $c[0]$ is finite. Although such digital implementations inherently yield periodic pseudo-chaotic sequences, if properly designed, they can retain, in some sense, the sensitivity to initial conditions of the original systems while generating trajectories with enormous periods that, for all practical purposes, can be viewed as aperiodic. In particular, given a B-bit description for $c[0]$, digitized implementations can be constructed that generate spreading sequences with periods of order 2^{B-1}–2^B.

The outline of the paper is as follows. In Section II, we describe the chaotic DS/SS systems and the channel model of interest. In Section III, we present the class of chaotic maps of interest and properties of the associated sequences that affect the $\Pr(\epsilon)$ performance of intended and unintended receivers. In Section IV, we derive uncoded $\Pr(\epsilon)$ expressions and bounds for intended receivers and develop computationally efficient bounds on the unintended receiver $\Pr(\epsilon)$. Based on these performance characterizations, we deduce connections between chaotic map features and the associated $\Pr(\epsilon)$ performance. These connections are then exploited in Section V to develop algorithms for recursively constructing maps with monotonically increasing $\Pr(\epsilon)$ gaps between intended and unintended users. Finally, Section VI contains some concluding remarks.

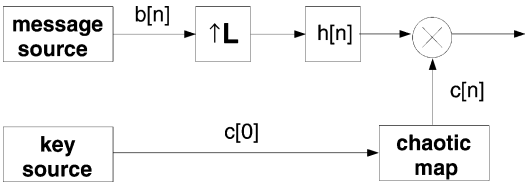

Fig. 1. Block diagram of a chaotic DS/SS modulator.

II. Pseudo-Chaotic Spread Spectrum Systems

In this section, we present the class of pseudo-chaotic DS/SS systems and channel models that are of interest in this paper.

A system model for the pseudochaotic transmitter is shown in Fig. 1, where the message stream $b[n] \in \{+\sqrt{\mathcal{E}_b}, -\sqrt{\mathcal{E}_b}\}$ is a sequence of independent and identically distributed (IID) binary-valued symbols with equally likely symbol values, and $c[n]$ is the spreading sequence obtained by iterating an initial condition $c[0]$ through an 1-D pseudochaotic map. Besides replacing binary-valued shift-register spreading sequences with chaotic sequences, the system in Fig. 1 is effectively identical to a conventional DS/SS system with spreading gain L. We consider an AWGN channel model, whereby the intended and unintended users' received signal at time n is of the form

$$y[n] = \frac{A}{\sqrt{L}}\, c[n]\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] + w[n] \tag{1}$$

where the normalization constant $A \triangleq 1/\sqrt{E\left[c^2[n]\right]}$ guarantees that $\mathcal{E}_b$ is the transmitted energy per bit, $w[n]$ is an IID zero-mean Gaussian sequence with power $N_o/2$ per dimension, and $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. While our analysis is confined to AWGN channels, it suggests, in some sense, the $\Pr(\epsilon)$ advantage trends these systems provide to intended users over flat fading channels.

III. Sequences from a Class of Piecewise-Linear Chaotic Maps

In this section, we define the chaotic maps and sequences of interest and present some of their properties and representations that are useful in the $\Pr(\epsilon)$ analysis of intended and unintended receivers. Methods for digital implementation of these chaotic sequences and their ramifications are briefly discussed in Appendix A.

The chaotic spreading sequences we exploit in this work are generated via the recursion

$$c[n] = F(c[n-1]) \tag{2}$$

initialized with some initial condition $c[0] \in I \triangleq [-1, 1]$. We assume that the map F belongs to the class of piecewise-linear $P \times Q$ equipartition maps defined as follows.

Definition 1: The map $F : I \to I$ is a piecewise-linear $P \times Q$ equipartition map if it satisfies the following conditions.

i) There exist partitions $-1 = a_0 < a_1 < \cdots < a_P = 1$ and $-1 = b_0 < b_1 < \cdots < b_Q = 1$ of I, where P and Q are positive integers with $P > Q$, such that, for each $i \in \{1, \ldots, P\}$, the restriction of F to $I_i = I_i^P \triangleq [a_{i-1}, a_i)$, $F|I_i$, is onto $[b_{j-1}, b_j)$, for some $j \in \{1, \ldots, Q\}$.
ii) $F(\cdot)$ is surjective, i.e., for any $j \in \{1, \ldots, Q\}$, there exists an $i \in \{1, \ldots, P\}$ for which $F|I_i$ is onto $[b_{j-1}, b_j)$.
iii) $F(\cdot)$ is piecewise linear, i.e., $F|I_i$ is affine for all i.
iv) $F(\cdot)$ is equipartitioned, i.e., the sets of numbers $\{a_0, \ldots, a_P\}$ and $\{b_0, \ldots, b_Q\}$ are both uniformly spaced on I.

For convenience, we refer to the class of maps of Definition 1 with fixed P and Q as $P \times Q$ partition maps and the subclass of Definition 1 corresponding to $Q = 1$ as P-partition maps.

The class of P-partition maps and the sequences they generate have a number of important properties. First, these maps have uniform invariant densities and are fully stretching, i.e., $F|I_i$ is onto for all i. Moreover, they are exact and ergodic transformations that possess the Markov property [18], [19]. Exactness ensures complete loss of memory of initial conditions with repeated iterations of the map and is directly related to the growth rate of sequence prediction error and the sensitive dependence on initial conditions. This sensitivity is captured by the Lyapunov exponent of the map $\lambda = \log(P) > 0$ and thus depends *only* on the numbers of partitions P. Remarkably, however, as we show in Section IV-B, distinct maps with the same P, possessing the same sensitivity to initial conditions, can provide vastly different uncoded $\Pr(\epsilon)$ advantages to intended receivers. As P-partition maps are especially amenable to analysis, we employ them to illustrate some of the key relationships between maps and the degree of secrecy of the associated chaotic spread spectrum systems. These relationships are then exploited to select maps from the richer class of maps of Definition 1 to achieve a required level of uncoded $\Pr(\epsilon)$ advantage offered to intended users. The subset of $P \times Q$ partition maps selected in the process also corresponds to exact Markov maps, with uniform invariant densities and Lyapunov exponents $\lambda = \log(P/Q) > 0$.

We next develop certain important representations for L-point sequences

$$\mathbf{c}^L \triangleq [\, c[0] \quad c[1] \quad \cdots \quad c[L-1] \,]^{\mathrm{T}} \tag{3}$$

generated by a given $P \times Q$ partition map. First, we note that $\mathbf{c}^L$ is fully determined by the initial condition $c[0]$, or, alternatively, by $c[L-1]$ and the set of partition indexes within which the iterates $\{c[n]; 0 \le n < L\}$ fall; given this information, one can reconstruct $\mathbf{c}^L$. Furthermore, we note that given any $c \in [-1, 1]$, we have $c \in I_i$ and $F(c) \in [b_{j-1}, b_j)$ for a unique $i \in \{1, 2, \ldots, P\}$ and a unique $j \in \{1, \ldots, Q\}$. For future convenience, we may define

$$s = s(c) \triangleq 2i - P - 1 \tag{4a}$$

and

$$q_s = q_s(s(c)) \triangleq 2j - Q - 1. \tag{4b}$$

The identifier functions in (4) are odd-symmetric, e.g.,

$$s(-c) = -s(c),\ c \in I. \tag{5}$$

Using (4), the mapping $F(\cdot)$ can be described as

$$y = F_s(x) = \frac{\zeta_s}{Q}\left(P \cdot x + \zeta_s \cdot q_s - s\right) \tag{6}$$

where ζ_s denotes the sign of the slope of the piecewise-linear map on its restriction to the partition associated with the index $s = s(x)$. Similarly, the inverse map is given by

$$x = F_s^{-1}(y) = \zeta_s \left(\frac{Q \cdot y - q_s + \zeta_s \cdot s}{P}\right). \tag{7}$$

Letting $s[n] = s(c[n])$, we have

$$c[n+1] = F(c[n]) = F_{s[n]}(c[n]) \Leftrightarrow c[n] = F_{s[n]}^{-1}(c[n+1]) \tag{8}$$

and, hence, the following equivalent representations for $\mathbf{c}^L$:

$$\mathbf{c}^L \Leftrightarrow c[0] \Leftrightarrow \{\mathbf{s}^{L-1},\, c[L-1]\} \tag{9}$$

where $\mathbf{s}^n \triangleq [\, s[0] \quad s[1] \quad \cdots \quad s[n-1] \,]^{\mathrm{T}}$ is often referred to as the n-point itinerary of $c[0]$.

The pair of vectors

$$\boldsymbol{\zeta} = \boldsymbol{\zeta}^P \triangleq [\, \zeta_{-P+1} \quad \zeta_{-P+3} \quad \cdots \quad \zeta_{P-1} \,]^{\mathrm{T}} \tag{10}$$

comprising the ordered signs of the slopes of $F(\cdot)$ over the P partitions, and

$$\mathbf{q} = \mathbf{q}^P \triangleq [\, q_{-P+1} \quad q_{-P+3} \quad \cdots \quad q_{P-1} \,]^{\mathrm{T}}$$

comprising the ordered range intervals associated with the P partitions, completely characterize a $P \times Q$ partition map. For instance, the case $(P = 2, Q = 1)$ with $\boldsymbol{\zeta} = [\, 1 \quad -1 \,]^{\mathrm{T}}$ and $\mathbf{q} = [\, 0 \quad 0 \,]^{\mathrm{T}}$ corresponds to the tent map

$$F_{\mathrm{T}}(c) = 1 - 2|c| \tag{11}$$

while the case $\{\zeta_s = 1, \forall s\}, \{q_s = 0, \forall s\}$ results in the class of r-adic maps, with $(P = 2, Q = 1)$ corresponding to the dyadic map

$$F_{\mathrm{D}}(c) = 2(c+1) \mod 2 - 1. \tag{12}$$

We remark that this characterization is not unique; any $P_0 \times Q_0$ partition map can be also viewed as a $(M \cdot P_0) \times (M \cdot Q_0)$ partition map for any positive integer M by appropriately expanding the pair $\left(\boldsymbol{\zeta}^{P_0}, \mathbf{q}^{P_0}\right)$ to $\left(\boldsymbol{\zeta}^{M \cdot P_0}, \mathbf{q}^{M \cdot P_0}\right)$. For example,

the tent map (11) can be also viewed as a 4×2 partition map with $\boldsymbol{\zeta} = [\,1 \quad 1 \quad -1 \quad -1\,]^{\mathrm{T}}$ and $\mathbf{q} = [\,-1 \quad 1 \quad 1 \quad -1\,]^{\mathrm{T}}$.

Any P-partition map $F(\cdot)$ and its inverse have the following concise descriptions:

$$y = F_s(x) = \zeta_s(P \cdot x - s) \tag{13a}$$

and

$$x = F_s^{-1}(y) = \frac{\zeta_s \cdot y + s}{P}. \tag{13b}$$

As (13) reveals, any map within this class is fully characterized by the vector (10).

We next focus on the probability density function (PDF) of the power of length-L sequences, and, in particular, its relation to features of the chaotic map. These PDFs play a key role in the probability of error performance of intended receivers. Due to (9), the power of a length-L chaotic vector $\mathbf{c}^L$ can be viewed as a function of the vector $\mathbf{c}^L$, the initial condition $c[0]$, or, alternatively, $\{\mathbf{s}^{L-1},\, c[L-1]\}$. Hence, with a slight abuse of notation, we have

$$\mathcal{E}\left(\mathbf{c}^L\right) = \mathcal{E}\left(c[0]\right) = \mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right) = \frac{1}{L}\sum_{n=0}^{L-1} c^2[n]. \tag{14}$$

Fig. 2 shows the dyadic map, its $(L-1)$-fold composition $F^{L-1}(c)$, and the power of $\mathbf{c}^L$, first versus $c[0]$ in Fig. 2(b) and then versus $c[L-1]$ for all possible $\mathbf{s}^{L-1}$ in Fig. 2(c). Each quadratic segment of $\mathcal{E}\left(c[0]\right)$ and $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ corresponds to a unique itinerary vector $\mathbf{s}^{L-1}$. We remark that the curvatures of the $\mathcal{E}\left(c[0]\right)$ curves grow exponentially with L, whereas those of $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ remain bounded as $L \to \infty$.

All P-partition maps with the same number of partitions P have the same power PDF. For any pair of distinct P-partition maps $F(\cdot)$ and $G(\cdot)$ with the same P, using (13a), we can readily verify that[1]

$$F_{s(c)}(c) = \pm G_{s(c)}(c)\,.$$

Moreover, using (5), we can readily show that

$$F_{s(-c)}(-c) = \pm F_{s(c)}(c).$$

Consequently, for any pair of sequences generated by propagating the same initial condition through two distinct P-partition maps $F(\cdot)$ and $G(\cdot)$ with the same P, we have

$$\begin{aligned}[\,c \quad F(c) \quad F^2(c) \quad \cdots \quad F^{L-1}(c)\,]^{\mathrm{T}} \\ = [\,c \quad \pm G(c) \quad \pm G^2(c) \quad \cdots \quad \pm G^{L-1}(c)\,]^{\mathrm{T}}\end{aligned} \tag{15}$$

showing, indeed, that the PDF of $\mathcal{E}\left(\mathbf{c}^L\right)$ depends only on the number of partitions P and not on the sign vector $\boldsymbol{\zeta}$ associated with the particular map. In addition, all P-partition maps have the same average sequence power $E\left[\mathcal{E}\left(\mathbf{c}^L\right)\right] = 1/3$, where $E[\cdot]$ denotes expectation. Thus, for the sequences from these maps, $A = \sqrt{3}$ in (1).

[1]We employ the notation $y = \pm x$ to denote $y = +x$ or $-x$.

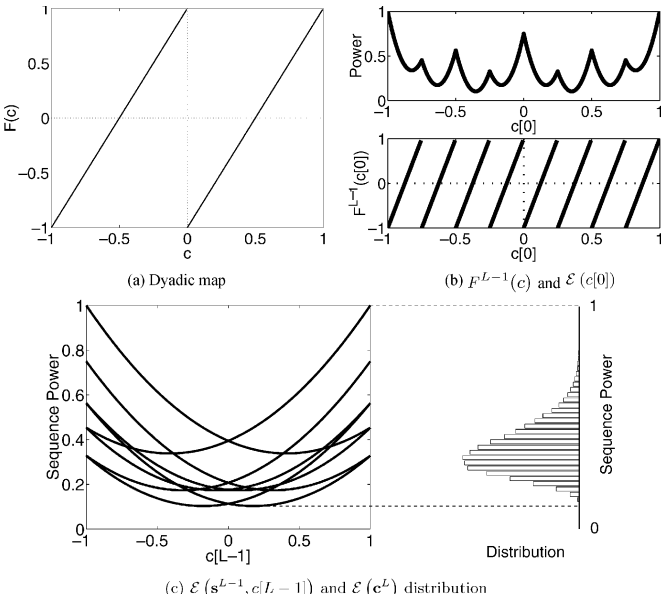

Fig. 2. Dyadic map and its sequence power characteristics for $L = 4$. (a) Dyadic map. (b) $F^{L-1}(c)$ and $\mathcal{E}\left(c[0]\right)$. (c) $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ and $\mathcal{E}\left(\mathbf{c}^L\right)$ distribution.

Finally, the minimum sequence power $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$ is also of interest as it greatly affects the intended receiver $\Pr(\epsilon)$. Since $\mathcal{E}\left(\mathbf{c}^L\right) = \left\|\mathbf{c}^L\right\|^2/L = \left\|\mathbf{c}^L - \mathbf{0}\right\|^2/L$, $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$ is attained by sequences that are closest to the origin. Since P-partition maps with odd P pass through the origin, $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right) = 0$ for these maps. P-partition maps with even P do not pass through the origin and, hence, exhibit a nonzero $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$. As $L \to \infty$, these $\min \left\|\mathbf{c}^L\right\|$ sequences approach fixed or period-2 trajectories with sample values from $\{+1/(P+1), -1/(P+1)\}$. Consequently

$$\lim_{L\to\infty} \min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right) = \left(\frac{1}{P+1}\right)^2, \quad P \text{ even}\,. \tag{16}$$

As a result, over all P-partition maps, $\min \mathcal{E}\left(\mathbf{c}^L\right)$ is maximum for $P = 2$, corresponding to the tent map and the dyadic map.

IV. Receiver Performance for DS/SS with P-Partition Map Sequences

In this section, we analyze the $\Pr(\epsilon)$ performance of intended and unintended receivers for DS/SS systems with spreading sequences from P-partition maps. We then exploit our analysis to deduce connections between chaotic map attributes and the $\Pr(\epsilon)$ advantages provided to intended users.

A. Intended Receiver Performance

In the following, we develop numerically efficient methods for evaluating the $\Pr(\epsilon)$ performance of intended receivers for DS/SS communication with P-partition maps in AWGN and determine the relationship between system and map parameters and the $\Pr(\epsilon)$ of these receivers.

From the viewpoint of intended receivers that know the initial condition, chaotic spreading is equivalent to linearly modulating the message bit stream on a *known* time-varying

shaping waveform. Consequently, the minimum $\Pr(\epsilon)$ receiver is a symbol-by-symbol detector consisting of a time-varying matched filter followed by sampling and a threshold detector. The (instantaneous) received bit signal-to-noise ratio (SNR) associated with a specific spreading vector $\mathbf{c}^L$ is given by

$$\gamma_b = \frac{A^2\mathcal{E}_b}{N_o}\mathcal{E}\left(\mathbf{c}^L\right) = \frac{3}{L}\cdot\frac{\mathcal{E}_b}{N_o}\sum_{n=0}^{L-1} c^2[n]. \tag{17}$$

As $c[n]$ is an ergodic sequence for almost all initial conditions [19],

$$\Pr(\epsilon) = E\left[\mathcal{Q}\left(\sqrt{2\gamma_b}\right)\right] = \int \mathcal{Q}\left(\sqrt{\frac{6\mathcal{E}_b\mathcal{E}\left(c\right)}{N_o}}\right) p_{c[0]}(c)\,dc \tag{18}$$

where $\mathcal{Q}(\nu) = 1 - \mathcal{F}(\nu)$, and where $\mathcal{F}(\cdot)$ denotes the cumulative distribution function of the standard Gaussian PDF, i.e.,

$$\mathcal{Q}(\nu) = \frac{1}{\sqrt{2\pi}}\int_{\nu}^{\infty} e^{-t^2/2}dt \tag{19}$$

and where $p_{c[0]}(\cdot)$ denotes the invariant density, which, for any P-partition map, is uniform in $[-1,\ 1]$. We remark that the integral (18) has no closed-form solution. Furthermore, the number of intervals required for numerical integration grows exponentially with L, as Fig. 2(b) suggests. These integrals are characterized by exponentially decreasing widths and integrands with curvatures exponentially increasing in L, leading to numerically sensitive computation algorithms of (18).

An alternative expression to (18) is obtained by replacing $\mathcal{E}\left(c[0]\right)$ with $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ and using the fact that $c[L-1]$ is uniformly distributed on I

$$\begin{aligned}\Pr(\epsilon) &= E\left[E\left[\mathcal{Q}\left(\sqrt{\frac{6\mathcal{E}_b\,\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)}{N_o}}\right)\middle|\,\mathbf{s}^{L-1}\right]\right] \\ &= \frac{1}{2P^{L-1}}\sum_{i=1}^{P^{L-1}}\int_{-1}^{+1}\mathcal{Q}\left(\sqrt{\frac{6\mathcal{E}_b\,\mathcal{E}\left(\mathbf{s}_i, c\right)}{N_o}}\right)dc. \end{aligned}\tag{20}$$

Although (20) requires computation of a number of integrals that grows exponentially with L, unlike (18), it suggests well-behaved algorithms for numerical computation of the intended receiver $\Pr(\epsilon)$, as each $\mathcal{E}\left(\mathbf{s}^{L-1} = \mathbf{s}_i, c[L-1]\right)$ curve in (20) has bounded curvature for all L. Furthermore, (20) suggests computationally efficient approximations based on equivalence classes of itineraries with similar $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$s.

Upper and lower bounds that are independent of L can serve as figures of merit for assessing the asymptotic $\Pr(\epsilon)$ characteristics of intended receivers. Specifically, we have

$$\mathcal{Q}\left(\sqrt{2\overline{\gamma}_b}\right) \le \Pr(\epsilon) \le \mathcal{Q}\left(\sqrt{\frac{6\mathcal{E}_b \min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)}{N_o}}\right) \tag{21}$$

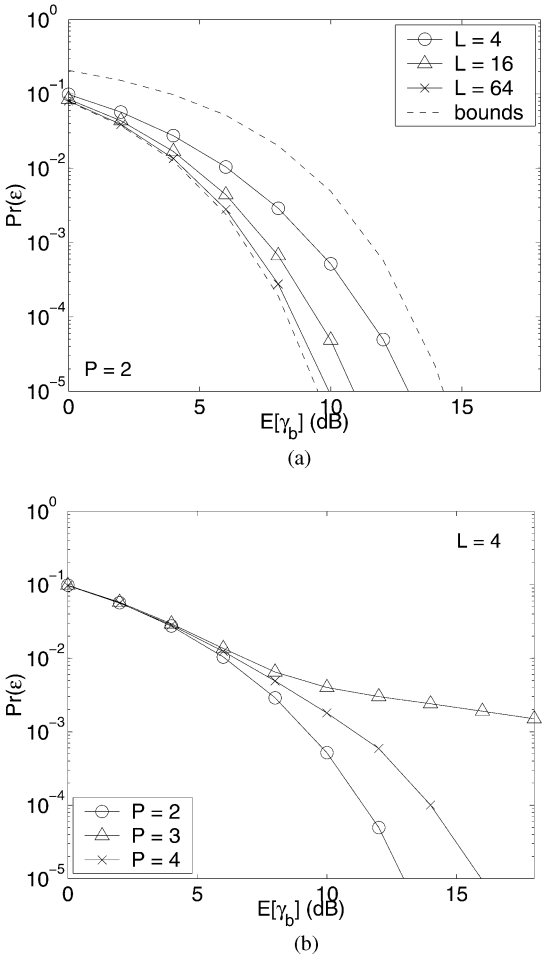

Fig. 3. Intended receiver $\Pr(\epsilon)$ performance. Solid curves indicate analytically computed $\Pr(\epsilon)$s and dashed curves indicate the lower and upper bounds for a given number of partitions. (a) $\Pr(\epsilon)$ versus SNR for various spreading gain L. (b) $\Pr(\epsilon)$ versus SNR for various number of partitions P.

where $\overline{\gamma}_b = E\left[\gamma_b\right] = \mathcal{E}_b/N_o$ is the average bit SNR. The lower bound in (21) is obtained using Jensen's inequality and the fact that $\mathcal{Q}(\cdot)$ is convex and corresponds to the optimum $\Pr(\epsilon)$ for antipodal signaling using binary-valued PN spreading sequences in AWGN, whereas the upper bound is due to $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right) \le \mathcal{E}\left(\mathbf{c}^L\right)$. For DS/SS systems using P-partition maps with odd P, the upper bound in (21) reduces to 1/2 since $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right) = 0$. For DS/SS systems using maps with even P, $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)$ rapidly converges to its limiting value (16) as L increases. Consequently, over a wide range of spreading gains, the upper bound in (21) is well approximated by its limiting value

$$\lim_{L\to\infty}\Pr(\epsilon) \le \mathcal{Q}\left(\frac{\sqrt{6\overline{\gamma}_b}}{P+1}\right), \quad P \text{ even}. \tag{22}$$

The spreading gain L and the number of map partitions P are the only parameters affecting the intended receiver $\Pr(\epsilon)$, as, due to (15), the codeword power PDF is independent of the sign vector $\boldsymbol{\zeta}$. Fig. 3 shows typical $\Pr(\epsilon)$ curves versus SNR as a function of L and P. As Fig. 3(a) reveals, the $\Pr(\epsilon)$ is a decreasing function of L, converging to the lower bound in

(21) as $L \to \infty$. The curves on Fig. 3(b) are consistent with upper bound in (21). Specifically, the $\Pr(\epsilon)$ for any odd-P map does not decay exponentially with SNR, as $\min \mathcal{E}\left(\mathbf{c}^L\right) = 0$.[2] In contrast, the intended receiver $\Pr(\epsilon)$ for any even-P map decays exponentially with SNR, as $\min \mathcal{E}\left(\mathbf{c}^L\right) > 0$. Furthermore, the tent and dyadic map-based systems ($P = 2$) have the best $\Pr(\epsilon)$ performance, which is consistent with the fact that they provide the spreading sequences with the largest $\min \mathcal{E}\left(\mathbf{c}^L\right)$. However, this property does not necessarily render these maps the most attractive for achieving secrecy, as it does not take into account the $\Pr(\epsilon)$ trends of unintended receivers.

B. Unintended Receiver Performance

In this section, we develop computationally efficient methods for evaluating the unintended receiver $\Pr(\epsilon)$ for DS/SS signaling with P-partition maps and determine system attributes that affect the unintended receiver $\Pr(\epsilon)$. We assume that the unintended receiver has complete knowledge of the modulation scheme including the chaotic map but does not know the initial condition $c[0]$.

As the unintended receiver does not know the key $c[0]$, it faces a composite hypothesis testing problem; under each (message sequence) hypothesis, the observed sequence is a signal term in AWGN, whereby the signal term is a random vector with statistical characterization determined by the message hypothesis and the set of valid chaotic spreading sequences. In particular, assuming

$$\mathbf{y} = \begin{bmatrix} y[0] & y[1] & \cdots & y[NL-1] \end{bmatrix}^{\mathrm{T}} \tag{23}$$

is observed, corresponding to a sequence of N transmitted bits in (1), represented as

$$\mathbf{b} \triangleq \begin{bmatrix} b[0] & b[1] & \cdots & b[N-1] \end{bmatrix}^{\mathrm{T}}, \tag{24}$$

the maximum likelihood (ML) detector is given by (25), shown at the bottom of the page.

One can readily verify that if F is an odd map, $\mathbf{y}$ from (23) has the same statistical characterization under hypotheses $\mathbf{b} = \mathbf{b}_o$ and $\mathbf{b} = -\mathbf{b}_o$, and hence, $p_{\mathbf{y}|\mathbf{b}}(\mathbf{y}|\mathbf{b}_o) = p_{\mathbf{y}|\mathbf{b}}(\mathbf{y}|-\mathbf{b}_o)$. As a result, even as $\overline{\gamma}_b \to \infty$, the optimal detector is unable to distinguish between the correct hypothesis and its antipodal. We therefore assume that there are only $N-1$ information bits to be distinguished, i.e., each pair $\pm\mathbf{b}_o$ are merged into a single hypothesis, resulting in 2^{N-1} possible hypotheses, carrying $N-1$ information bits. For consistency, we apply this approach to intended and unintended receivers and all chaotic DS/SS systems, regardless of the chaotic map symmetry.

Direct implementation of (25) is impractical except for small values of N, P, and L, as each of the 2^{N-1} likelihoods requires P^{NL} integral computations. As an alternative to exact $\Pr(\epsilon)$ evaluation, we develop lower and upper bounds that reflect the $\Pr(\epsilon)$ trends as a function of SNR and spreading gain. First, a numerically computable lower bound is obtained by simulating the optimum receiver in the case that, in addition to $\mathbf{y}$, the receiver has side information available in the form of the set $\{+c[NL-1], -c[NL-1]\}$. Associated with each member of this set is a finite set of possible initial conditions $\{c_m[0], m = 1, 2, \ldots, P^{NL-1}\}$, effectively transforming the uniform PDF of $c[0]$ to a posterior PMF of $2P^{NL-1}$ impulses. The associated ML detector is given by (26), shown at the bottom of the page. A useful upper bound on the unintended receiver $\Pr(\epsilon)$ can be obtained by considering the performance of the following suboptimal generalized likelihood ratio test (GLRT) detector:

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{GLRT}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \max_{c[0]|\mathbf{b}} p_{\mathbf{y}|\mathbf{b},c[0]}(\mathbf{y}|\mathbf{b}, c) \\ &= \arg\min_{\mathbf{b}} \sum_{n=0}^{NL-1} \left(y[n] - \frac{b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \hat{c}\,[n|NL-1, \mathbf{b}]}{\sqrt{\frac{L}{3}}} \right)^2 \end{aligned} \tag{27}$$

where $\hat{c}[n|k, \mathbf{b}_o]$ denotes the ML estimate of $c[n]$ based on $y[0], y[1], \ldots, y[k]$, given $\mathbf{b} = \mathbf{b}_o$. Accurate approximations of these estimates can be computed via extensions of the linear-complexity algorithm in [20], as elaborated in Appendix B. As Fig. 4 demonstrates for a typical P-partition map, the gap between the $\Pr(\epsilon)$ bounds based on (26) and (27) remains small over a wide SNR range, revealing that these bounds can predict the $\Pr(\epsilon)$ trends of unintended receivers.

Unlike the intended receiver case, in addition to the spreading gain and the number of map partitions, the unintended receiver $\Pr(\epsilon)$ is greatly affected by the map slope signs $\boldsymbol{\zeta}$ in (10). This can be illustrated by considering a vector $\mathbf{b}$ with $N = 2$, where it is known that $b[0] = \sqrt{\mathcal{E}_b}$. For convenience, we denote by $x[n]$ the signal-component samples that are obtained by letting $w[n] = 0$ in (1), and consider the pairwise relation between successive

[2]Using an argument similar to the one used in Appendix C, we can show that the intended receiver $\Pr(\epsilon)$ for any DS/SS with spreading sequences from P-partition maps with odd P decays at best as $1/\sqrt{\overline{\gamma}_b}$.

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \int p_{\mathbf{y}|\mathbf{b},c}(\mathbf{y}|\mathbf{b}, c) p_{c[0]}(c)\, dc \\ &= \arg\max_{\mathbf{b}} \int \exp\left\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \left(2\sqrt{\frac{3}{L}} y[n] F^n(c)\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] - \frac{3\mathcal{E}_b}{L} \left(F^n(c)\right)^2 \right) \right\} p_{c[0]}(c)\, dc. \end{aligned} \tag{25}$$

$$\hat{\mathbf{b}}_{\mathrm{LB}}(\mathbf{y}) = \arg\max_{\mathbf{b}} \sum_{m=1}^{2P^{NL-1}} \exp\left\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \left(\frac{y[n] F^n(c_{(m)}[0])}{\sqrt{\frac{L}{12}}}\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] - \frac{3\mathcal{E}_b}{L} \left(F^n(c_{(m)}[0])\right)^2 \right) \right\}. \tag{26}$$

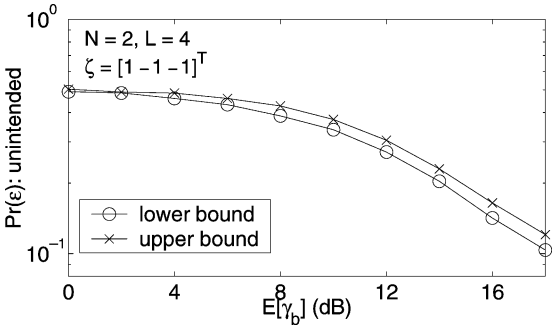

Fig. 4. Upper and lower bounds for the unintended receiver performance.

signal samples for tent and dyadic map-based SS systems. Fig. 5 shows the associated signal pair trajectories when $b[1] = \sqrt{\mathcal{E}_b}$ (solid) and $b[1] = -\sqrt{\mathcal{E}_b}$ (dashed). As the figure reveals, unlike the tent map case, where the two hypotheses are distinguishable throughout transmission of $b[1]$, in the dyadic map case, only the boundary pair $\{x[L-1],\ x[L]\}$ provides information for distinguishing between the two hypotheses. This effect is readily seen to be true for any odd map, regardless of the number of partitions, making, in general, odd maps more attractive in terms of secrecy potential than maps of even or no symmetry.

The optimal unintended receiver $\Pr(\epsilon)$ can vary among distinct odd P-partition maps. Since the optimal decision rules for systems utilizing odd maps are dominated by the pairs of observations at the bit transitions, insight can be gained by studying the decision regions of simplified rules that are solely based on such observation pairs. Such decision regions for two four-partition odd maps are shown in Fig. 6. As the figure reveals, the r-adic map leads to a finer partition of strips of alternating decision regions and, thus, lower noise immunity, suggesting a higher unintended receiver $\Pr(\epsilon)$ than the other odd map in the figure. It is straightforward to verify that, among all odd P-partition maps, the r-adic map yields the finest partitioning of decision regions. Furthermore, between any two r-adic maps, the one with larger P results in a larger number of thinner strips of alternating decision regions and, hence, a higher unintended receiver $\Pr(\epsilon)$.

Fig. 7 depicts the unintended receiver $\Pr(\epsilon)$ as a function of the spreading gain L for several four-partition maps. As the figure reveals, for all maps, $\Pr(\epsilon)$ is an eventually increasing function of L, with $\lim_{L\to\infty} \Pr(\epsilon) = 0.5$. For the odd maps in the figure, the unintended receiver $\Pr(\epsilon)$ is a strictly increasing function of the spreading gain; this is expected, as, for these maps, discrimination is effectively based on boundary signal pairs, and the energy per signal pair decreases with increasing L. On the other hand, for the asymmetric and the even map in the figure, there is an L–range for which the $\Pr(\epsilon)$ performance improves with L. This is due to the fact that for these maps, discrimination is based on *all* signal pairs throughout the interval (see Fig. 5) and is thus affected by both the chip and the codeword energy. In particular, as L increases, the variance in $\mathcal{E}\left(\mathbf{c}^L\right)$ becomes smaller, and thus, the probability of transmitting a low-power codeword, which dictates the $\Pr(\epsilon)$, decreases. As, however, higher spreading gains also imply lower energy per chip, the unintended receiver performance eventually degrades with increasing L. The figure also shows that odd maps outperform even and nonsymmetric maps in terms of $\Pr(\epsilon)$. Among all P-partition odd maps, r-adic maps are the most attractive as they result in the worst-case $\Pr(\epsilon)$ performance for unintended receivers. These observations are consistent with our preceding analysis, revealing that odd maps lead, in general, to higher unintended receiver $\Pr(\epsilon)$ and that, among odd maps with the same number of partitions, r-adic maps yield the least favorable decision regions. Thus, among all P-partition maps, r-adic maps provide the highest $\Pr(\epsilon)$ advantages to intended users. Interestingly, r-adic maps have been extensively studied in the context of intended receiver performance in multiuser DS/CDMA systems and have been shown to possess attractive auto- and cross-correlation properties and broadband spectra [7]–[9].

Fig. 8 depicts the $\Pr(\epsilon)$ of intended and unintended receivers versus SNR for various r-adic maps. Also shown in the figure is the lower bound on $\Pr(\epsilon)$ from (21). As the number of partitions P is increased, the $\Pr(\epsilon)$ attainable by intended receivers increases with respect to the lower bound from (21), as discussed in Section IV-A. This degradation is offset, however, by greater increase in the unintended receiver $\Pr(\epsilon)$, as higher P implies higher sensitivity to initial conditions and lower quality chaotic sequence estimates. At higher spreading gains, the $\Pr(\epsilon)$ gap becomes even larger as the intended receiver $\Pr(\epsilon)$ converges to the lower bound in (21), whereas the unintended receiver $\Pr(\epsilon)$ degrades with L.

As we show in Appendix C, the unintended receiver $\Pr(\epsilon)$ for DS/SS with odd P-partition maps cannot not decay faster than $1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$. In contrast, the intended receiver $\Pr(\epsilon)$ for these systems (with P even) decays exponentially with $\overline{\gamma}_b$. This is also verified in Fig. 8, showing that the simulated unintended receiver $\Pr(\epsilon)$ curves eventually exhibit the same slope as the dash-dot line $1/2\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$. Thus, knowledge of the initial seed in the chaotic DS/SS systems we consider yields significant uncoded $\Pr(\epsilon)$ advantages to intended users. This is in contrast to conventional DS/SS employing binary-valued spreading sequences (generated via LFSR's), where an unintended receiver without knowledge of the initial seed can obtain a consistent estimate, provided a long enough segment of the sequence is observed even at very low SNR [16], [17].

V. Iterative Constructions of $P \times Q$ Partition Map-Based DS/SS

Based on the analysis in Section IV-B, suggesting that odd symmetry and fine decision-region partitioning are attractive attributes, we can construct recursive algorithms for generating sequences of maps from the richer class of $P \times Q$ partition maps with monotonically increasing unintended receiver $\Pr(\epsilon)$ while keeping the intended receiver $\Pr(\epsilon)$ unaffected. Such an algorithm that preserves the ratio P/Q and, hence, the Lyapunov exponent, is illustrated in Fig. 9. The algorithm is initialized with a P-partition map, e.g., the dyadic map. At each step of the recursion, a new $P \times Q$ partition map is constructed via modifications of the map constructed in the preceding recursion step. In particular, segments of a given set of valid trajectories are swapped with their counterparts corresponding to the antipodal hypothesis to create a map that is twice as large as P and Q, whereby odd symmetry is preserved, and the partitioning of the unintended-receiver decision regions is made finer. Specifically,

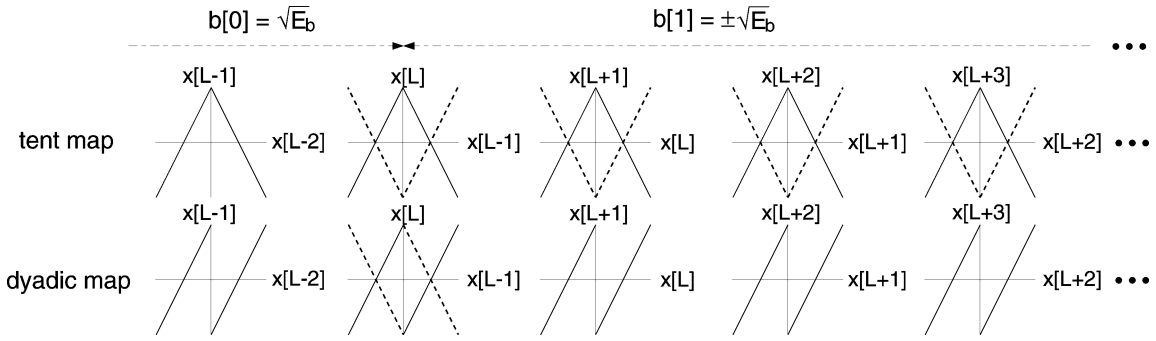

Fig. 5. Pairwise signal trajectories for tent and dyadic map-based SS systems in the cases $b[1] = b[0] = \sqrt{\mathcal{E}_b}$ (solid) and $b[1] = -b[0] = -\sqrt{\mathcal{E}_b}$ (dashed).

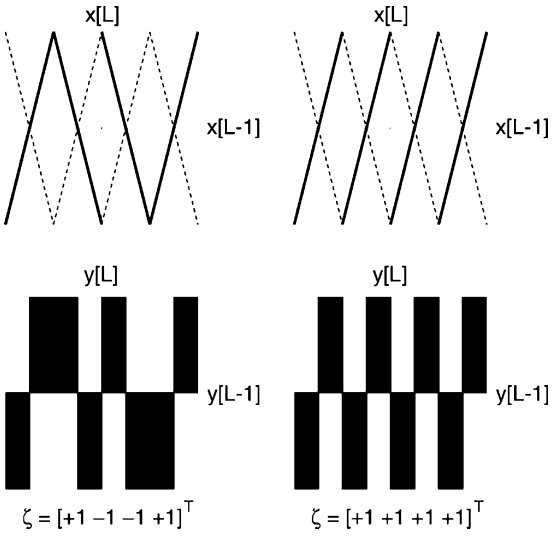

Fig. 6. Upper graphs: Valid signal trajectories $(x[L-1],\ x[L])$ for two odd four-partition maps, under hypotheses $b[0] = b[1]$ (solid) and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions based on $(y[L-1],\ y[L])$.

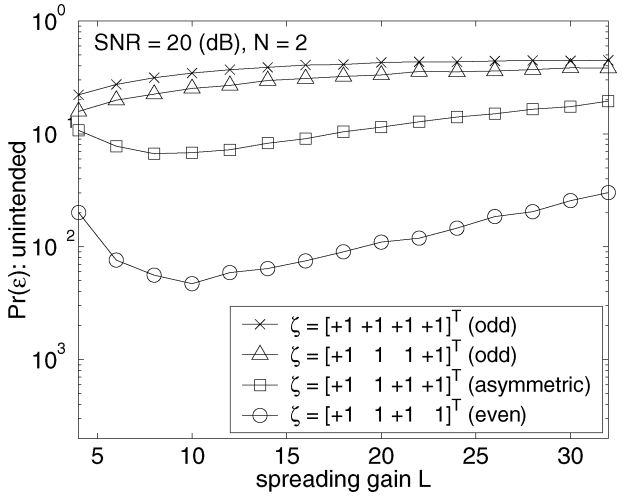

Fig. 7. Numerically computed upper bounds on the unintended receiver $\Pr(\epsilon)$ versus spreading gain for several SS systems employing four-partition maps.

the algorithm results in a sequence of $P_n \times Q_n$ partition maps $F_n(\cdot)$ by means of the following steps:

1) *Initialization*: Initialize the recursion with a P_0-partition map $F_0(\cdot)$ (i.e., $Q_0 = 1$). Let $n = 1$.

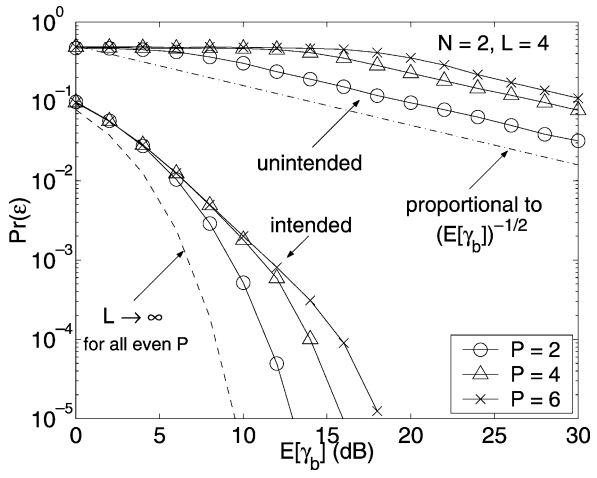

Fig. 8. Analytically computed intended receiver $\Pr(\epsilon)$s versus numerically computed upper bounds on $\Pr(\epsilon)$s of unintended receivers for r-adic map-based SS systems.

2) *nth Step Recursion*: Construct a $P_n \times Q_n$ partition map $F_n(\cdot)$ via modifications of the $P_{n-1} \times Q_{n-1}$ partition map $F_{n-1}(\cdot)$, as follows:

2a) Set $P_n = 2 \cdot P_{n-1}$ and $Q_n = 2 \cdot Q_{n-1}$;

2b) View $F_{n-1}(\cdot)$ as a $P_n \times Q_n$ partition map with (equi-spaced in I) partitions points $\{a_1^{(n)}, a_2^{(n)}, \ldots, a_{P_n}^{(n)}\}$ and $\{b_1^{(n)}, b_2^{(n)}, \ldots, b_{Q_n}^{(n)}\}$;

2c) Letting $m_i^{(n)}$ denote the mid-point of $I_i^{(n)} = \left[a_{i-1}^{(n)}, a_i^{(n)}\right)$, i.e., $m_i^{(n)} \triangleq (a_{i-1}^{(n)} + a_i^{(n)})/2$, $i \in \{1, \ldots, P_n\}$, sequentially define $F_n(\cdot)$ on $I = \cup_{1 \le i \le P_n} I_i^{(n)}$ as follows:

2c-i) *Initialization*: $F_n|I_1^{(n)} \triangleq F_{n-1}|I_1^{(n)}$; set $i = 2$;

2c-ii) *ith Interval*: For all $c \in I_i^{(n)}$, if $\left|F_n(m_{i-1}^{(n)}) + F_{n-1}(m_i^{(n)})\right| > \left|F_n(m_{i-1}^{(n)}) - F_{n-1}(m_i^{(n)})\right|$, then $F_n \triangleq -F_{n-1}$, else $F_n \triangleq F_{n-1}$;

2c-iii) If $i \le P_n$, increment i by 1, and go to step 2c-ii); else, go to step 3);

3) Increment n by 1, and go to step 2).

The nested maps designed by this algorithm have several important properties. First, it can be readily verified that the algorithm generates odd mappings in the cases of interest, involving initializing P-partition maps with an even number of partitions.

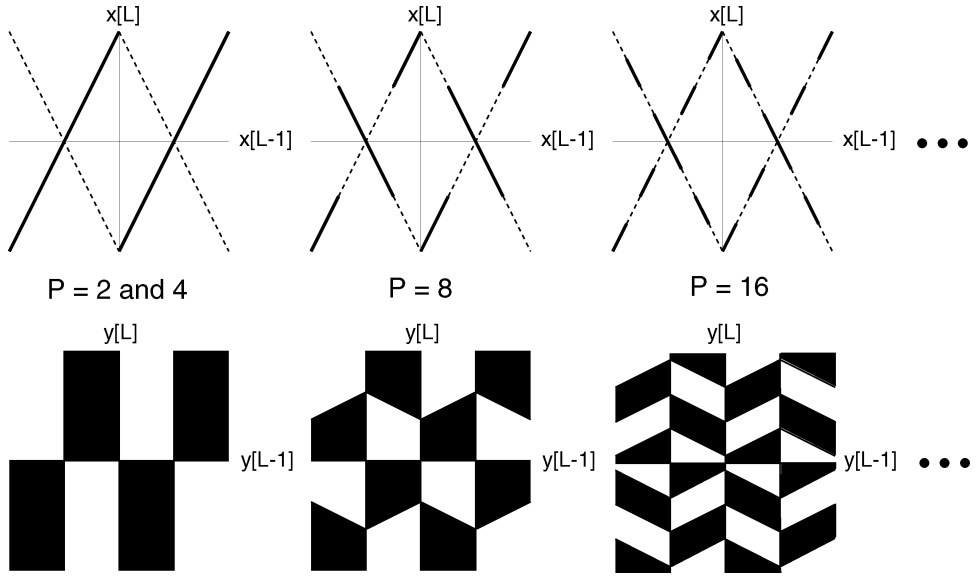

Fig. 9. Upper graphs: Signal trajectories for nested maps based on dyadic map, under hypotheses $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: Associated decision regions.

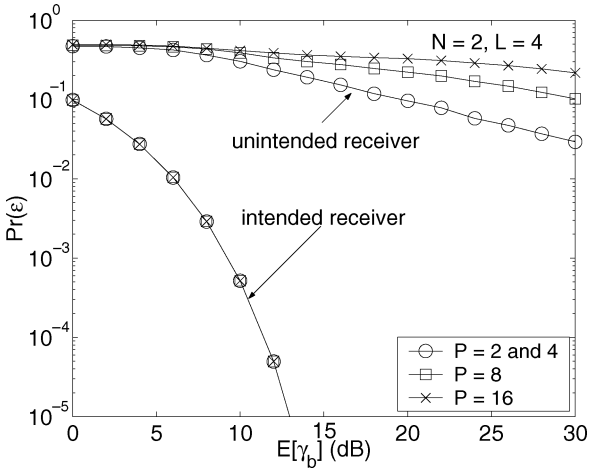

Fig. 10. Intended receiver $\Pr(\epsilon)$ versus numerically computed upper bounds on unintended receiver $\Pr(\epsilon)$ for nested maps based on dyadic map.

Since $|F_n^k(c[0])| = |F_n^{k-1}(c[0])|$ for all n, k and $c[0]$, the recursion preserves the PDF of $\mathcal{E}\left(\mathbf{c}^L\right)$ and, hence, the intended receiver $\Pr(\epsilon)$. Furthermore, all constructed maps have (unique) uniform invariant densities, possess the same sensitive dependence on initial conditions as $F_0(\cdot)$, and can be made exact with suitable realizations. These trends are readily reflected in Fig. 10, showing that the unintended receiver $\Pr(\epsilon)$ degrades monotonically with the number of recursion steps, whereas the intended receiver $\Pr(\epsilon)$ is unaffected. The physical-layer secrecy potential of these chaotic DS/SS systems is readily apparent from the figure, in terms of the $\Pr(\epsilon)$ gap between intended and unintended receivers.

VI. Concluding Remarks

In this paper, we have investigated the $\Pr(\epsilon)$ advantages provided to intended receivers by a class of chaotic DS/SS systems over AWGN channels. We have developed computationally efficient evaluation methods and useful bounds on the $\Pr(\epsilon)$ of optimal intended and unintended receivers and have demonstrated that by proper choice of the chaotic map, a required level of intended receiver performance can be met while satisfying a constraint on the unintended receiver $\Pr(\epsilon)$ performance. In particular, we have shown that for a subclass of these systems, the unintended receiver $\Pr(\epsilon)$ improves only as $1/\sqrt{\text{SNR}}$. We have also identified relationships between chaotic map features and intended and unintended receiver $\Pr(\epsilon)$ and exploited them to design maps that achieve a desired level of $\Pr(\epsilon)$ advantages provided to intended receivers, showing in the process that these chaotic DS/SS systems are indeed viable candidates for providing secrecy to intended receivers.

This work suggests several important directions for further investigation. A natural extension is to analyze the uncoded $\Pr(\epsilon)$ advantages available via chaotic DS/SS over fading channels of the type that arise in a range of wireless communication systems. These systems are potentially even more attractive candidates in these settings, as wireless transmissions are more vulnerable to unwanted interception and manipulation than their wireline counterparts. It is also important to analyze and optimize the uncoded $\Pr(\epsilon)$ advantages available in the context of multiuser generalizations of the chaotic DS/SS considered in this work. In general, the uncoded $\Pr(\epsilon)$ advantages in the multiuser setting also depend on the spectra of chaotic spreading sequences, as well as the amount of information available to intended and unintended users regarding the initial conditions of the spreading sequences of other users. Finally, developing digital implementations for these systems and assessing the effects of finite precision depth on the $\Pr(\epsilon)$ advantages provided to intended receivers is also a subject worthy of further investigation.

Appendix A
Digital Realization of Sequences from $P \times Q$ Partition Maps

In this Appendix, we briefly examine some of the issues that arise in digital realizations of sequences from $P \times Q$ parti-

TABLE I
LARGEST PRIME q, $q < 2^B$, SUCH THAT NONZERO SEQUENCES FROM (29) HAVE PERIOD $q-1$, FOR $r=2$ (DYADIC MAP) AND $r=3$ (3-ADIC MAP)

B	dyadic map	3-adic map	2^B
8	227	233	256
12	4093	4073	4096
16	65371	65419	65536
24	16776989	16777183	16777216
32	4294967291	4294967188	4294967296
48	281474976710597	281474976710597	281474976710656
64	18446744073709551557	18446744073709551557	18446744073709551616

tion maps. These digital implementations are dynamical systems over finite domains and can thus be viewed as finite state machine realizations of $P \times Q$ partition maps. As each digitized sequence from such a dynamical system is equivalent to a series of output states from a finite state machine, it is inherently periodic (thereby not chaotic), and hence, it cannot, in a strict sense, exhibit sensitive dependence on initial conditions in the long term [21]. If properly designed, however, digitized sequences with enormous periods can be generated that retain, in some sense, many of the important properties of the chaotic trajectories of interest.

Brute-force digital realizations of piecewise-linear chaotic maps can yield systems with undesirable dynamics. This can be illustrated by considering digital realizations of r-adic maps

$$\tilde{F}(x) = r\,x \mod 1\,,\ x \in [0,1]$$

where $x \bmod a$ denotes the non-negative remainder of x/a. Given a numerical precision depth of B bits, a straightforward realization method exploiting the maximum number of quantization levels can be effectively viewed as a mapping of the form

$$G(x) \triangleq r\,x \mod 2^B \tag{28}$$

where $x \in \{0,1,2,\ldots,2^B-1\}$. Propagating any initial condition x through (28) yields a fixed point of the map after a finite number of iterations. For instance, in the case $r=2$, the maximum possible number of iterations before reaching a fixed point is $B+1$. Evidently, this type of brute-force realization does not preserve the invariant density, exactness, broadband characteristics, and sensitivity to initial conditions of the original map.

Certain key properties of chaotic sequences can, in some sense, be preserved via properly constructed digitized realizations. In particular, consider r-adic map implementations of the form

$$G(x) = r\,x \mod q \tag{29}$$

where $x \in \{0,\,1,\,\ldots,\,q-1\}$, and q is a suitably chosen prime such that $q < 2^B$. An attractive attribute of implementations of the type (29) is that, under modulo q addition and multiplication, the integer set $\{0,\,1,\,\ldots,\,q-1\}$ forms a Galois field of order q, GF(q). As a result, if the prime q is chosen such that r is a primitive element in GF(q), then (29) yields $q-1$ maximal-length sequences $G^{(n)}(x)$ with period $q-1$ for all initial conditions, except for $x=0$ [22].

Implementations of the form (29), where r is a primitive element of GF(q), have several attractive properties. First, the sequences arising from nonzero initial conditions are exact and ergodic and possess uniform invariant densities on their restriction on $\{1,\,2,\,\ldots,\,q-1\}$. Furthermore, from the unintended receiver's point of view, these sequences can retain the sensitive dependence on initial conditions of the original chaotic map in the sense that the combined effect of sufficient quantization depth and channel noise can render the space spanned by these digitized sequences effectively indistinguishable from the space spanned by the real-valued chaotic trajectories. Consequently, the performance of intended and unintended receivers in the context of DS/SS systems exploiting such pseudochaotic sequences can be evaluated via analysis techniques that are developed for their chaotic counterparts.

Table I shows the largest prime q such that r is a primitive element of GF(q), as a function of the precision depth B for r-adic maps with $r=2,\,3$. As the table reveals, q is very close to 2^B for all B values in the figure. We note that although empirical methods for finding a suitable q may be sufficient, as one such q may suffice in designing a chaotic DS/SS system, algorithms for systematically generating such q's as a function of the precision depth are important in their own right and warrant further investigation, especially in the context of digitized implementations for other target maps (including all nested maps of Section V). For instance, although P-partition map realizations can be readily developed by systematic modifications of digital realizations of their r-adic counterparts (same P), in general, different q's are required to yield maximal-length sequences for different P-partition maps with the same number of partitions.

APPENDIX B
APPROXIMATE ML SEQUENCE ESTIMATION FOR NESTED MAPS

In this appendix we present extensions of ML estimation algorithms in [20] for the class of nested maps in Section V that includes the class of P-partition maps. These extensions are exploited in the construction of the GLRT detector presented in Section IV-B.

We denote by $\hat{c}_{\mathrm{ML}}[n|k,\mathbf{b}_o]$ the ML estimate of $c[n]$ given $y[m]$ for $m \le k$ and assuming

$$\mathbf{b} = \mathbf{b}_o \triangleq [\,b_o[0] \quad b_o[1] \quad \cdots \quad b_o[N-1]\,]^{\mathrm{T}}$$

is transmitted. The filtered ML estimates $\hat{c}_{\mathrm{ML}}[n|n,\mathbf{b}_o]$, for $n = 0,1,\ldots,NL-1$, can be readily obtained via a straightforward extension of the algorithm in [20] by exploiting the identity

$$\left|a - F_s^{-1}(b)\right| = \frac{|F_s(a)-b|}{\beta}$$

where $\beta = |P/Q|$, and which holds for any $a,b \in I$ and any admissible s in a nested map $F(\cdot)$. Given $\tilde{y}[n] = y[n]/A$, the

recursion for the intermediate sequence of estimates $\hat{c}[n|n,\mathbf{b}_o]$ is given by

$$\hat{c}[n|n,\mathbf{b}_o]=\frac{\left(\beta^2-1\right)\beta^{2n}\tilde{y}[n]b_o\left[\left\lfloor\frac{n}{L}\right\rfloor\right]+\left(\beta^{2n}-1\right)\hat{c}[n|n-1,\mathbf{b}_o]}{\beta^{2(n+1)}-1} \tag{30}$$

where

$$\hat{c}[n|n-1,\mathbf{b}_o]=F\left(\hat{c}[n-1|n-1,\mathbf{b}_o]\right)$$

and where the recursion is initialized via $\hat{c}[0|0,\mathbf{b}_o]=\tilde{y}[0]b_o[0]$. The ML estimate is then obtained by amplitude-limiting this intermediate estimate according to

$$\hat{c}_{\mathrm{ML}}[n|n,\mathbf{b}_o]=\mathcal{I}\left(\hat{c}[n|n,\mathbf{b}_o]\right)$$
$$\text{where } \mathcal{I}(x)=\begin{cases}x, & |x|\le 1\\ \mathrm{sgn}(x), & |x|\ge 1\end{cases}$$

and where $\mathrm{sgn}(x)$ denotes the sign of x. The smoothed ML estimates $\hat{c}_{\mathrm{ML}}[n|NL-1,\mathbf{b}_o]$, in contrast, cannot be readily obtained for nested maps, because the ML estimate of an itinerary point $\hat{s}[n|N]$, in general, cannot be expressed in terms of $\hat{c}_{\mathrm{ML}}[n|n,\mathbf{b}_o]$. However, computationally efficient algorithmic extensions yielding smoothed estimates can be used to approximate the performance characteristics of the smoothed ML estimates. Specifically, we consider the estimates formed via

$$\hat{c}\left[n|NL-1,\mathbf{b}_o\right]=F_{\hat{s}[n]}^{-1}\left(\hat{c}\left[n+1|NL-1,\mathbf{b}_o\right]\right) \tag{31}$$

initialized with $\hat{c}[NL-1|NL-1,\mathbf{b}_o]=\hat{c}_{\mathrm{ML}}[NL-1|NL-1,\mathbf{b}_o]$, where

$$\tilde{s}[n]=\underset{s[n]\in\mathcal{S}_n}{\arg\min}\left\{\tilde{y}[n]\,b_o\left[\left\lfloor\frac{n}{L}\right\rfloor\right]-F_{s[n]}^{-1}\left(\hat{c}\left[n+1|NL-1,\mathbf{b}_o\right]\right)\right\}^2 \tag{32}$$

and where $\mathcal{S}_n$ denotes the set of admissible $s[n]$ for the given map. As illustrated in Section IV-B, (32) results in estimates $\hat{c}\left[n|NL-1,\mathbf{b}_o\right]$, which, when used in the context of the GLRT-type detector (27), yield $\Pr(\epsilon)$ performance close to that predicted by the lower bound provided by the detector defined in (26).

Appendix C
Unintended Receiver $\Pr(\epsilon)$ Asymptotic Decaying Rate

In this Appendix, we show that the unintended receiver $\Pr(\epsilon)$ for DS/SS with spreading sequences generated by odd P-partition maps can be bounded from below by a function that decays at a rate of $1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$. Since for any nested map there exists a corresponding initializing P-partition map with lower unintended receiver $\Pr(\epsilon)$, the $1/\sqrt{\overline{\gamma}_b}$ bound also holds for all nested maps of Section V that are initialized by odd P-partition maps.

We develop a lower bound on the $\Pr(\epsilon)$ of detecting a fixed but arbitrary differentially encoded symbol given observation of $y[n]$ in (1). In particular, we assume that an IID sequence $i[n]=\pm 1$ is differentially encoded into the sequence $b[n]=i[n]\,b[n-1]$ used in (1). We focus on detection of $i[D]$, for some $1\le D\le N-1$, based on observation of $\mathbf{y}$ in (23). We denote via $\mathbf{x}(c,\mathbf{b})$ the NL-dimensional signal vector that is transmitted, given an initial condition c and a vector $\mathbf{b}$ in (24), viz.,

$$\mathbf{x}(c,\mathbf{b})\triangleq\left[\,x[0]\quad x[1]\quad\cdots\quad x[NL-1]\,\right]^{\mathrm{T}} \tag{33}$$

where

$$x[n]=x[n;c,\mathbf{b}]\triangleq\frac{A}{\sqrt{L}}F^n(c)\;b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]$$

and where $\mathbf{b}$ and $b[n]$ are related via (24). Letting $\mathcal{S}_k^{(D)}=\{\mathbf{b};\quad b[D]b[D-1]/\mathcal{E}_b=k\}$, for $k=\pm 1$, the optimal detector for the Dth symbol sets $\hat{i}[D]=\arg\max_{k\in\{-1,1\}}\Pr\left(\mathbf{b}\in\mathcal{S}_k^{(D)}|\mathbf{y}\right)$.

To obtain a lower bound on the $\Pr(\epsilon)$, we consider a detector that is provided with the remaining $N-2$ information symbols

$$\tilde{\mathbf{i}}\triangleq\left[\,i[1]\quad\cdots\quad i[D-1]\quad i[D+1]\quad\cdots\quad i[N-1]\,\right]^{\mathrm{T}} \tag{34}$$

as well as some additional side information that depends on whether or not $c[0]$ belongs in the set

$$I_o\triangleq\bigcup_{c\in\mathcal{C}^{(D)}}I(c)$$

where $I(c)\triangleq(c,c+\Delta)$, $\Delta\triangleq 2\,P^{-(NL-1)}$, and $\mathcal{C}^{(D)}$ is the preimage of $\{0\}$ under F^{DL-1}, i.e.,

$$\mathcal{C}^{(D)}\triangleq F^{-(DL-1)}(0)=\left\{c\in I;\quad F^{DL-1}(c)=0\right\}. \tag{35}$$

Specifically, if $c[0]\notin I_o$, the receiver is provided with the value of $i[D]$. If $c[0]\in I_o$, the receiver is only told that the initial condition is from the set $\{\pm\underline{c}[0]+\delta\}$, where $\underline{c}[0]$ denotes the unique $c\in\mathcal{C}^{(D)}$ for which $c[0]\in I(c)$, and $\delta\triangleq\delta(c[0])=c[0]-\underline{c}[0]$. Note that since F is odd, $\underline{c}[0]\in\mathcal{C}^{(D)}$ implies that $-\underline{c}[0]\in\mathcal{C}^{(D)}$. In addition,[3] since $|\mathcal{C}^{(D)}|=P^{DL-1}$, $\Pr(c[0]\in I_o)=P^{(D-N)L}$.

The availability of (34) limits the possible $\mathbf{b}$ candidates under hypothesis $i[D]=k$ at the receiver to $\tilde{\mathcal{S}}_k^{(D)}=\{\bar{\mathbf{b}}_k,-\bar{\mathbf{b}}_k\}$, where

$$\bar{\mathbf{b}}_k\triangleq\left[\,\bar{b}[0]\quad\bar{b}[1]\quad\cdots\quad\bar{b}[D]\quad k\,\bar{b}[D+1]\quad\cdots\quad k\,\bar{b}[N-1]\,\right]^{\mathrm{T}}$$

and where the nth entry of $\bar{\mathbf{b}}_k$ denotes the nth differentially encoded symbol in the case that $i[D]=k$, $\tilde{\mathbf{i}}$ is as in (34) and given $\bar{b}[0]=\sqrt{\mathcal{E}_b}$. Hence, when $c[0]\in I_o$, the optimal detector is given by $\hat{i}_1[D]=\arg\max_{k\in\pm 1}\Pr\left(\mathbf{x}\in\mathcal{X}_k^{(D)}|\mathbf{y}\right)$, where the signal set under hypothesis $i[D]=k$ is given by

$$\mathcal{X}_k^{(D)}=\left\{\mathbf{x}(c,\mathbf{b});\quad c\in\{\pm\underline{c}[0]+\delta\},\mathbf{b}=\tilde{\mathcal{S}}_k^{(D)}\right\}. \tag{36}$$

Letting ϵ_1 denote the error event of this receiver, we have

$$\Pr(\epsilon)\ge\Pr(c[0]\in I_o)\;\Pr(\epsilon_1|c[0]\in I_o). \tag{37}$$

[3]The set I_o could be made larger, e.g., by also including all sets of the form $(c-\Delta,c)$ with $c\in\mathcal{C}^{(D)}$. Although this would yield a somewhat tighter lower bound, its rate of decay cannot be made lower than $1/\sqrt{\overline{\gamma}_b}$.

$$\mathbf{u} = [\, x[DL; c[0], \bar{\mathbf{b}}_1] \quad x[DL+1; c[0], \bar{\mathbf{b}}_1] \quad \cdots \quad x[NL-1; c[0], \bar{\mathbf{b}}_1] \,]^{\mathrm{T}}$$

We next lower bound $\Pr(\epsilon_1 | c[0] \in I_o)$. First, when $c[0] \in I_o$ and $\mathbf{b} = \bar{\mathbf{b}}_1$, the signal term is given by

$$x[n; c[0], \bar{\mathbf{b}}_1] = \underline{\mathrm{x}}[n] + r[n] \tag{38a}$$

for all $0 \le n \le NL-1$, where

$$\underline{\mathrm{x}}[n] = \lim_{u \to 0^+} x[n; \underline{\mathrm{c}}[0] + u, \bar{\mathbf{b}}_1] \tag{38b}$$

$$r[n] = \frac{A}{\sqrt{L}} s[n]\, \bar{b} \left[\left\lfloor \frac{n}{L} \right\rfloor \right] P^n \delta \tag{38c}$$

and where $s[n]$ is defined via the recursion

$$s[n] = s[n-1]\, \mathrm{sgn}\underline{\mathrm{c}}[n]$$

with $\underline{\mathrm{c}}[n] \triangleq \lim_{u \to 0^+} F^n(\underline{\mathrm{c}}[0]+u)$ and initialized with $s[0] = 1$. Consequently, $x[n; c[0], \bar{\mathbf{b}}_1]$ varies *linearly* with $c[0]$ (or, rather $\delta = c[0] - \underline{\mathrm{c}}[0]$). The significance of (38) is that, as the reader can readily verify, the sets $\mathcal{X}_k^{(D)}$ from (36) can be expressed in the following convenient form:

$$\mathcal{X}_k^{(D)} = \left\{ \mathbf{x}; \quad \mathbf{x} = \ell \begin{bmatrix} \mathbf{p} + m\, k\, \mathbf{r} \\ m\, \mathbf{u} \end{bmatrix}, \quad \ell, m \in \{-1, 1\} \right\} \tag{39}$$

where $\mathbf{p} = [\underline{\mathrm{x}}[0] \underline{\mathrm{x}}[1] \underline{\mathrm{x}}[2] \cdots \quad \underline{\mathrm{x}}[DL-1]\,]^{\mathrm{T}}$, $\mathbf{r} = [r[0] r[1] \cdots r[DL-1]]^{\mathrm{T}}$, $\mathbf{u}$ is shown in the equation at the top of the page, and where $\underline{\mathrm{x}}[n]$, $x[n; c[0], \bar{\mathbf{b}}_1]$, and $r[n]$ are given by (38). Finally, given a fixed $c[0] \in I_o$, $\Pr(\epsilon_1 | c[0])$ is lower bounded by the probability of error of a detector that must decide between $\tilde{\mathbf{x}} = \mathbf{x}_1$ and $\tilde{\mathbf{x}} = \mathbf{x}_{-1}$, based on $\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \mathbf{w}$, where $\mathbf{x}_k = [\mathbf{p}^{\mathrm{T}} + k\mathbf{r}^{\mathrm{T}} \quad \mathbf{u}^{\mathrm{T}}]^{\mathrm{T}}$, and $\mathbf{w}$ is defined as $\mathbf{y}$ in (23) with $y[n]$ replaced by $w[n]$. Indeed, $\mathbf{x}$ from (39) can be viewed as the output of a channel with input $\tilde{\mathbf{x}}$: Given $\tilde{\mathbf{x}} = [\mathbf{p}^{\mathrm{T}} + k\mathbf{r}^{\mathrm{T}} \quad \mathbf{u}^{\mathrm{T}}]^{\mathrm{T}}$, the channel outputs $\mathbf{x} = \ell[\mathbf{p}^{\mathrm{T}} + km\mathbf{r}^{\mathrm{T}} \quad m\mathbf{u}^{\mathrm{T}}]^{\mathrm{T}}$, where $m, \ell = \pm 1$ are random variables with equally likely values and statistically independent of one another and $\tilde{\mathbf{x}}$. Hence, due to the data processing inequality [23], the optimal receiver based on (39) cannot outperform the one that detects $\tilde{\mathbf{x}}$ based on $\tilde{\mathbf{y}}$, i.e.,

$$\Pr(\epsilon_1 | c = \underline{\mathrm{c}}[0] + \delta) \ge \mathcal{Q}\left(\sqrt{\tilde{\gamma}(\delta)} \right) \tag{40}$$

where

$$\tilde{\gamma}(\delta) = \frac{\|\mathbf{x}_1 - \mathbf{x}_{-1}\|^2}{2N_o} = \frac{2\,\|\mathbf{r}\|^2}{N_o}$$

$$= \delta^2 \frac{6\,\mathcal{E}_b (P^{2DL} - 1)}{L(P^2-1)\, N_o} = C \overline{\gamma}_b \delta^2 \tag{41}$$

with $C = 6(P^{2DL}-1)/L(P^2-1)$. Conditioned on $c[0] \in I(\underline{\mathrm{c}}[0])$ (and thus on $c[0] \in I_o$), δ is uniformly distributed $(0, \Delta)$, which, using (41), also implies that $0 < \tilde{\gamma}(\delta) < \gamma_{\max} = C\Delta^2 \overline{\gamma}_b$. To show that $\Pr(\epsilon)$ cannot decay faster than $1/\sqrt{\overline{\gamma}_b}$, we pick an arbitrary $\gamma_o \in \left(0,\ C\,\Delta^2\,\overline{\gamma}_b\right)$; we remark that γ_o *can* remain fixed as $\overline{\gamma}_b$ increases. Hence, using (37) and (40), we have

$$\Pr(\epsilon) \ge \Pr\left(c[0] \in I_o\right) \int_0^\infty \mathcal{Q}\left(\sqrt{\gamma}\right)\, p_{\tilde{\gamma}}(\gamma)\, d\gamma$$

$$\ge P^{(D-N)L}\, \mathcal{Q}\left(\sqrt{\gamma_o}\right) \int_0^{\gamma_o} p_{\tilde{\gamma}}(\gamma)\, d\gamma \tag{42a}$$

$$= P^{(D-N)L}\, \mathcal{Q}(\sqrt{\gamma_o})\, \Pr\left(\delta < \sqrt{\frac{\gamma_0}{\overline{\gamma}_b\, C}} \;\middle|\; c[0] \in I_o \right)$$

$$= P^{(D-N)L}\, \mathcal{Q}(\sqrt{\gamma_o})\, \frac{P^{NL-1} \sqrt{\gamma_o L (P^2-1)}}{2\sqrt{6(P^{2DL}-1)}} \frac{1}{\sqrt{\overline{\gamma}_b}} \tag{42b}$$

where (42a) is due to the fact the $\mathcal{Q}\left(\sqrt{\gamma}\right)$ is a non-negative decreasing function of γ, and where (42b) is the desired bound.

ACKNOWLEDGMENT

The authors would like to thank the associate editor and the anonymous reviewers whose constructive comments improved the quality of the manuscript.

REFERENCES

[1] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 626–633, Oct. 1993.

[2] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb. 1990.

[3] ——, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, no. 4, pp. 2374–2383, Aug. 1991.

[4] E. Ott, *Chaos in Dynamical Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2002.

[5] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Commun.*, vol. 42, pp. 1524–1527, Feb./Mar./Apr. 1994.

[6] T. Yang and L. O. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *Intl. J. Bifurcation Chaos*, vol. 7, no. 12, pp. 2789–2805, Dec. 1997.

[7] C.-C. Chen, K. Yao, K. Umeno, and E. Biglieri, "Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory," *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 1110–1114, Sept. 2001.

[8] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA – Part I: System modeling and results," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 937–947, Oct. 1997.

[9] R. Rovatti, G. Setti, and G. Mazzini, "Chaotic complex spreading sequences for asynchronous CDMA – Part II: Some theoretical performance bounds," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 496–506, Apr. 1998.

[10] R. Rovatti, G. Mazzini, and G. Setti, "Interference bounds for DS-CDMA systems based on chaotic piecewise-affine Markov maps," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 885–896, June 2000.

[11] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete-time chaotic processes – Basic finite-dimensional tools and applications," *Proc. IEEE*, vol. 90, pp. 662–690, May 2002.

[12] D. León, S. Balkir, M. Hoffman, and L. C. Pérez, "Fully programmable, scalable chaos-based PN sequence generation," *Electron. Lett.*, vol. 36, no. 16, pp. 1371–1372, Aug. 2000.

[13] T. L. Carroll, "Spread-spectrum sequences from unstable periodic orbits," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 443–447, Apr. 2000.

[14] T. Kohda, "Information sources using chaotic dynamics," *Proc. IEEE*, vol. 90, pp. 641–661, May 2002.
[15] I. Hen and N. Merhav, "On the threshold effect in the estimation of chaotic sequences," in *Proc. 22nd Conv. Electr. Electron. Eng. Israel*, Dec. 2002, pp. 29–31.
[16] M. J. Mihaljević and J. D. Golić, "A comparison of cryptanalytic principles based on iterative error-correction," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1991, vol. 547, pp. 527–531.
[17] ——, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1993, vol. 658, pp. 124–137.
[18] S. H. Isabelle and G. W. Wornell, "Statistical analysis and spectrum estimation techniques for one-dimensional chaotic signals," *IEEE Trans. Signal Processing*, vol. 45, pp. 1495–1506, June 1997.
[19] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise*, 2nd ed. New York: Springer-Verlag, 1994.
[20] H. C. Papadopoulos and G. W. Wornell, "Maximum-likelihood estimation of a class of chaotic signals," *IEEE Trans. Inform. Theory*, vol. 41, pp. 312–317, Jan. 1995.
[21] C. Grebogi, E. Ott, and J. A. Yorke, "Roundoff-induced periodicty and the correlation dimension of chaotic attractors," *Phys. Rev. A*, vol. 38, no. 7, pp. 3688–3692, Oct. 1988.
[22] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Upper Saddle River, NJ: Prentice-Hall, 1995.
[23] T. C. Cover and J. Thomas, *Elements of Information Theory*. New York, NY: John Wiley & Sons, Inc., 1991.

Yongsun Hwang (S'97) was born in Seoul, Korea on November 14, 1974. He received the B.S. and M.S. degrees from the Yonsei University, Seoul, in radio communications engineering, in 1997 and 1999, respectively. Since 1999, he has been a Research Assistant with the Department of Electrical and Computer Engineering, University of Maryland, College Park, where he is currently pursuing the Ph.D. degree.

His research interests are in the areas of communications and signal processing, with emphasis on spread spectrum, communication security, and distributed designs of wireless communication networks.

Mr. Hwang received a Graduate School Fellowship from the University of Maryland in 1999.

Haralabos C. Papadopoulos (S'92–M'98) was born in Serres, Greece, on September 9, 1968. He received the S.B., S.M., and Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, all in electrical engineering and computer science, in 1990, 1993, and 1998, respectively.

Since 1998, he has been on the faculty of the Department of Electrical and Computer Engineering, University of Maryland, College Park, as an Assistant Professor. He also holds a joint appointment with the Institute of Systems Research. During his summer visits at AT&T Bell Laboratories, Murray Hill, NJ, between 1993 and 1995, he worked on shared time-division duplexing systems and digital audio broadcasting. His research interests are in the areas of signal processing and communications, with emphasis on nonlinear signal processing, digital audio broadcasting, and physical-layer algorithms for distributed computation and fusion in wireless sensor networks. He is active in industry and an inventor on several issued and pending patents.

Dr. Papadopoulos received an NSF CAREER Award in 2000, the G. Corcoran Award, given by the University of Maryland, in 2000, and the 1994 F. C. Hennie Award, given by the MIT EECS department. He is a member of Eta Kappa Nu and Tau Beta Pi.