PRIVATE COMMUNICATION OVER FADING CHANNELS WITH CHAOTIC DS/SS

Yongsun Hwang and Haralabos C. Papadopoulos

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742 USA

ABSTRACT

We consider chaotic spread spectrum (DS/SS) systems for secure communication over fading channels, whereby a symbol stream is linearly modulated on a spreading sequence generated by iterating an initial condition through a suitably chosen chaotic map. For a class of these systems we develop methods for quantifying the uncoded probability of error ($\Pr(\epsilon)$) of unintended receivers that do not know the initial condition. We show that the $\Pr(\epsilon)$ of unintended receivers exploiting K degrees of diversity decays as $1/\sqrt{\text{SNR}}$, in contrast to the intended receiver $\Pr(\epsilon)$ that decays as $1/(\text{SNR})^K$, demonstrating that these systems can provide reliable and private communication over fading channels.

1. INTRODUCTION

In this paper we evaluate the privacy potential of a class of chaotic DS/SS systems for communication over Rayleigh fading channels. We consider linear modulation schemes on spreading sequences arising from a class of one-dimensional (1D) piecewise-linear chaotic maps, and investigate how diversity techniques affect the relative $\Pr(\epsilon)$ performance advantages these systems provide to intended receivers over unintended ones. For the systems considered, we establish a lower bound on the asymptotic decaying rate of unintended receiver $\Pr(\epsilon)$ vs. SNR and develop metrics that predict the $\Pr(\epsilon)$. Based on this analysis, we then show that unintended receivers cannot fully exploit available degrees of diversity.

CDMA systems with spreading sequences generated via 1D chaotic maps have received attention in recent years. These systems were found to possess attractive cochannel interference characteristics and intended user performance [1, 2]. As shown in [3], many of these systems can provide privacy at the physical layer, arising from the combined effect of channel distortion and the sensitive dependence on initial conditions of chaotic sequences. The privacy benefits are in the form of $\Pr(\epsilon)$ performance advantages granted to intended receivers over their unintended counterparts that do not know the seed used to generate the chaotic spreading sequence. In particular, sequences of chaotic DS/SS systems were constructed that yield monotonically increasing unintended receiver $\Pr(\epsilon)$ while preserving the intended user $\Pr(\epsilon)$. For these systems, the unintended receiver $\Pr(\epsilon)$ over AWGN channels decays at a rate of $1/\sqrt{\text{SNR}}$ at high SNR, in sharp contrast to the exponential decay rate exhibited by the intended receiver $\Pr(\epsilon)$ [3].

This work was supported by the DoD-ARO under Award No. DAAD19-01-1-0494.

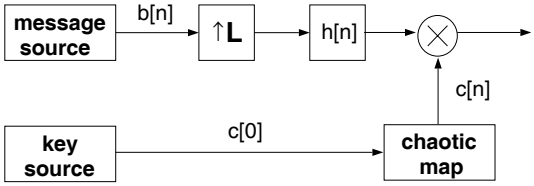

Fig. 1. Block diagram of a chaotic DS/SS modulator.

In this paper we quantify the $\Pr(\epsilon)$ advantages the chaotic DS/SS systems in [3] provide to intended users over Rayleigh fading channels. In particular, for these systems we show that, at high SNR, the unintended receiver $\Pr(\epsilon)$ over channels with K degrees of diversity decays as $1/\sqrt{\text{SNR}}$, in contrast to the $1/(\text{SNR})^K$ decay rate exhibited by the intended receiver $\Pr(\epsilon)$. We develop computationally efficient simulation-based metrics for characterizing the unintended user $\Pr(\epsilon)$. Based on our analysis, we demonstrate that the $\Pr(\epsilon)$ improvements due to diversity techniques are substantial for intended users but only marginal for unintended users.

The outline of the paper is as follows. In Sec. 2 we describe the chaotic DS/SS systems and the channel models of interest. In Sec. 3 we develop a lower bound on the asymptotic decaying rate of the unintended receiver $\Pr(\epsilon)$, and develop metrics for predicting the unintended receiver $\Pr(\epsilon)$. These metrics are then exploited in Sec. 4 to demonstrate the $\Pr(\epsilon)$ advantages provided to intended receivers over fading channels with temporal, spectral or receiver antenna diversity. Finally, Sec. 5 contains concluding remarks.

2. SYSTEM MODEL

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

A system model for the chaotic transmitter is shown in Fig. 1. The message stream $b[n] \in \left\{+\sqrt{\mathcal{E}_b}, -\sqrt{\mathcal{E}_b}\right\}$ 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 1D chaotic map. Besides replacing binary-valued shift-register spreading sequences

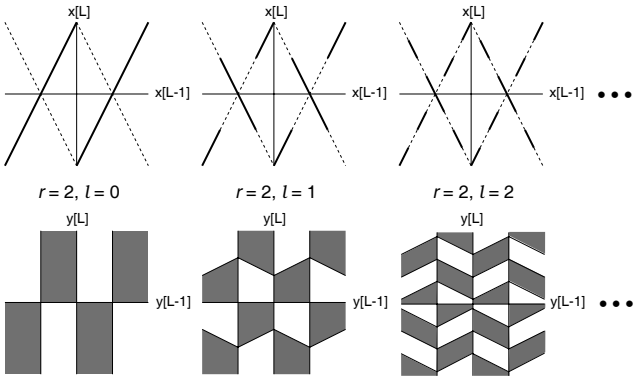

Fig. 2. Upper graphs: signal trajectories for nested maps based on dyadic map, given $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions for unintended receivers.

with chaotic sequences, the system in Fig. 1 is effectively identical to a conventional DS/SS system with spreading gain L. We consider a general fading channel model, where the intended and unintended users' received signal is

$$y_k[n] = \frac{A}{\sqrt{L}}\alpha_k[n]c[n]b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] + w_k[n]\,,\ 1 \le k \le K\,, \quad (1)$$

where the channel gains $\alpha_k[n]$ are independent in k, the $w_k[n]$'s are independent IID zero-mean Gaussian sequences with power $N_o/2$ per dimension, $A \stackrel{\triangle}{=} 1/\sqrt{E\left[c^2[n]\right]}$ guarantees that $\mathcal{E}_b$ equals the transmitted energy per bit, and $\lfloor x \rfloor$ denotes the largest integer not greater than x. We assume that, apart from $c[0]$, the unintended receiver has the same information as the intended receiver, including knowledge of $\alpha_k[n]$.

The model (1) captures many channels of interest for proper choice of the characterization of $\alpha_k[n]$. With $K = 1$, and $\alpha[n] = \alpha_1[n]$ an IID process, it captures time-selective flat fading channels (with n denoting the time index). The index n may also be associated with subcarriers in orthogonal frequency division multiplexing schemes for obtaining spectral diversity over frequency-selective channels. Also, with $K \ge 1$, the model (1) naturally incorporates multiple receiver antenna scenarios with slow/fast fading. We first characterize the unintended receiver $\Pr(\epsilon)$ for slow flat fading with $K = 1$, where $\alpha = \alpha_1[n]$ has a Rayleigh PDF normalized so that $E\left[\alpha^2\right] = 1$;

$$p_\alpha(\alpha) = 2\alpha e^{-\alpha^2}\,,\ \alpha \ge 0\,.$$

We then exploit our findings to deduce the $\Pr(\epsilon)$ trends of unintended users over channels with diversity.

2.1. Sequences from Piecewise-Linear Chaotic Maps

In this section we briefly review the chaotic DS/SS systems introduced in [3]. The chaotic spreading sequences used in this work are generated via the recursion

$$c[n] = F(c[n-1])\,, \quad (2)$$

initialized with an initial condition $c[0] \in [-1,\,1]$. The map F belongs to the class of piecewise-linear maps that are generated via recursive "nesting" algorithms in [3], initialized with an r-adic map, as illustrated in Fig. 2. For any nested map, $E\left[c^2[n]\right] = 1/3$, thus $A = \sqrt{3}$ in (1). These nested maps have several important properties [3]. First, increasing the recursion step ℓ monotonically increases the associated unintended receiver $\Pr(\epsilon)$ while preserving the intended receiver $\Pr(\epsilon)$. Also, the observation pairs $\{y[DL-1], y[DL]\}$, $D = 1, 2, \cdots$ dominate the optimal decision rules for unintended receivers. In particular, only a small number of observations at the boundary between two modulated codewords affect the unintended receiver $\Pr(\epsilon)$, and this number does not grow with the spreading gain. Moreover, the recursion steps monotonically degrade the unintended user $\Pr(\epsilon)$ in both AWGN and fading channels. This is because fading amounts to scaling the axes of decision regions in Fig. 2, and, hence, increasing ℓ implies finer partitioning of regions regardless of the channel.

3. UNINTENDED RECEIVER $\Pr(\epsilon)$ ANALYSIS

In this section we show that the unintended receiver $\Pr(\epsilon)$ curves for DS/SS over slow flat Rayleigh fading channels with spreading sequences generated by the maps of Sec. 2.1 exhibit a constant decaying rate at high average bit SNR $\overline{\gamma}_b$. We also develop computationally viable simulation-based approximations on the unintended receiver $\Pr(\epsilon)$.

3.1. Asymptotic Decaying Rate of $\Pr(\epsilon)$

In the following we sketch a proof of the fact that the unintended receiver $\Pr(\epsilon)$ for r-adic map based DS/SS is lower bounded by a function that decays as $1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$. Since for any nested map there exists a corresponding initializing r-adic map with lower unintended receiver $\Pr(\epsilon)$, the $1/\sqrt{\overline{\gamma}_b}$ bound also holds for all nested maps.

We develop a lower bound on the $\Pr(\epsilon)$ of detecting an arbitrary, but fixed, 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), and focus on detection of $i[D]$, for some $1 \le D \le N-1$, based on

$$\mathbf{y} \stackrel{\triangle}{=} [y[0] \quad y[1] \quad \cdots \quad y[NL-1]]^{\mathrm{T}}\,. \quad (3)$$

To obtain a lower bound on the $\Pr(\epsilon)$, we consider a detector that is provided with the remaining information symbols $\{i[n];\, 1 \le n \le N-1,\, i \ne D\}$ as well as some additional side information that depends on whether or not $c[0]$ belongs in the set $I_o \stackrel{\triangle}{=} \bigcup_{c \in \mathcal{C}^{(D)}} I(c)$, where $I(c) \stackrel{\triangle}{=} (c, c+\Delta)$, $\Delta \stackrel{\triangle}{=} 2\,r^{-(NL-1)}$, and $\mathcal{C}^{(D)}$ is the preimage of $\{0\}$ under F^{DL-1}. Specifically, when $c[0] \notin I_o$, $i[D]$ is declared to the receiver; when $c[0] \in I_o$, the receiver is only

told that $c[0]$ is from the set $\{\pm\underline{c}[0]+\delta\}$, where $\underline{c}[0]$ denotes the unique $c\in\mathcal{C}^{(D)}$ for which $c[0]\in(c,c+\Delta)$, and $\delta\stackrel{\Delta}{=}\delta(c[0])=c[0]-\underline{c}[0]$. It can be shown [3] that the optimal receiver with this side information (and knowing α) is inferior to the optimal detector in the context of binary signaling with codewords $\mathbf{x}_{i[D]}$ and $\mathbf{x}_{-i[D]}$, where $\mathbf{x}_{i[D]}$ is the transmitted vector, defined as $\mathbf{y}$ in (3) with $y[n]$ replaced by $\frac{A}{\sqrt{L}}\alpha c[n]\,b[\lfloor n/L\rfloor]$, and where $\mathbf{x}_{-i[D]}$ is the vector closest in Euclidean distance to $\mathbf{x}_{i[D]}$ among those associated with the antipodal hypothesis, and corresponds to using $c[n]$ generated from $c[0]=-\underline{c}[0]+\delta$. Thus,

$$\Pr(\epsilon|c=\underline{c}[0]+\delta,\alpha)\geq\mathcal{Q}\left(\sqrt{\tilde{\gamma}(\delta,\alpha)}\right) \tag{4}$$

where

$$\tilde{\gamma}(\delta,\alpha)=\frac{\|\mathbf{x}_1-\mathbf{x}_{-1}\|^2}{2N_o}=\delta^2\frac{6\alpha^2\mathcal{E}_b(r^{2DL}-1)}{(r^2-1)\,N_o}=C\overline{\gamma}_b\alpha^2\delta^2\,, \tag{5}$$

with $C=\frac{6(r^{2DL}-1)}{r^2-1}$. Conditioned on α and $c[0]\in I(\underline{c}[0])$, δ is uniformly distributed in $(0,\Delta)$ and, hence, the PDF of $\tilde{\gamma}$ in (5) is

$$p_{\tilde{\gamma}}(\gamma)=\frac{1}{2\Delta}\sqrt{\frac{\pi}{\gamma C\overline{\gamma}_b}}\left(1-\mathrm{erf}\left(\sqrt{\frac{\gamma}{\Delta^2C\overline{\gamma}_b}}\right)\right)\,.$$

We next pick an arbitrary but fixed γ_o (independent of $\overline{\gamma}_b$). Using (4), we have

$$\begin{aligned}\Pr(\epsilon)&\geq\Pr\left(c[0]\in I_o\right)\int_0^\infty\mathcal{Q}\left(\sqrt{\gamma}\right)\,p_{\tilde{\gamma}}\left(\gamma\right)d\gamma\\&\geq P^{(D-N)L}\mathcal{Q}(\sqrt{\gamma_o})\int_0^{\gamma_o}p_{\tilde{\gamma}}\left(\gamma\right)d\gamma\\&=P^{(D-N)L}\mathcal{Q}(\sqrt{\gamma_o})\left\{\sqrt{\frac{\pi\gamma_o}{\Delta^2C\overline{\gamma}_b}}\left(1-\mathrm{erf}\left(\sqrt{\frac{\gamma_o}{\Delta^2C\overline{\gamma}_b}}\right)\right)\right.\\&\qquad\left.+1-\exp\left\{-\frac{\gamma_o}{\Delta^2\overline{\gamma}_bC}\right\}\right\}\,.\end{aligned} \tag{6}$$

As $\overline{\gamma}_b$ increases, (6) converges to the following bound:

$$\Pr(\epsilon)\geq\mathcal{Q}\left(\sqrt{\gamma_o}\right)\,\frac{1}{\sqrt{\overline{\gamma}_b}}\frac{r^{NL-1}}{2}\sqrt{\frac{\pi\gamma_or^2-1}{6(r^{2DL}-1)}}\,. \tag{7}$$

3.2. $\Pr(\epsilon)$ Performance Evaluation

In this section we develop computationally viable methods for evaluating the unintended receiver $\Pr(\epsilon)$ in slow Rayleigh fading for DS/SS signaling with the nested maps of Sec. 2.1. The methods we present can be readily extended to all the fading channel models described in Sec. 2.

A lower bound on $\Pr(\epsilon)$ is obtained by assuming that the unintended receiver knows that the initial condition is from the set $\{c[m]\}_{m=1}^M$ for some M significantly larger than the observation interval NL. In particular, the unintended receiver $\Pr(\epsilon)$ is bounded by that of the optimum receiver in the case that, in addition to the observation $\mathbf{y}$ in (3), the receiver is given $b[0]$, $\{i[n];\,1\leq n\leq N-1,\,n\neq D\}$, and $c[0]\in\{c[m]\}_{m=1}^M$. This effectively transforms the uniform PDF of $c[0]$ to a posterior PMF of M impulses. The associated ML detector for $i[D]$ is given by

$$\hat{i}_{\mathrm{LB}}(\mathbf{y})=\arg\max_{i\in\pm1}\sum_{m=1}^M\exp\left\{\frac{1}{N_o}\sum_{n=0}^{NL-1}\left(\frac{y[n]\alpha F^n(c[m])}{\sqrt{L/12}}b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\right.\right.\\\left.\left.-\,\frac{3\mathcal{E}_b}{L}\left(\alpha F^n(c[m])\right)^2\right)\right\}\,. \tag{8}$$

Computationally viable approximations to $\Pr(\epsilon)$ are obtained by simulating (8) with $\mathbf{y}$ replaced by a windowed version $\mathbf{y}_w\stackrel{\Delta}{=}[y[DL-w]\;\;y[DL-w+1]\;\;\cdots\;\;y[DL+w]]^{\mathrm{T}}$, for $1\leq w\leq\lfloor NL/2\rfloor$. These approximations can prove accurate even when $w=1$, due to the dominance of the pairs of observations at the codeword transitions on the $\Pr(\epsilon)$ [3], and the sensitive dependence of the chaotic map on initial conditions. Upper bounds can be similarly obtained by considering the optimum detector of $i[D]$ given the windowed observation $\mathbf{y}_2$. This detector is also the minimum distance detector for the simpler binary-signaling-in-slow-fading problem, with sets of constellation points

$$\hat{\mathbf{c}}_{i,k}\stackrel{\Delta}{=}\left[-\tfrac{(P-1)+2(k-1)}{P}\quad\tfrac{i(-1)^k(Q-2k+1)}{Q}\right]^{\mathrm{T}}\,,$$

where $i\in\pm1$ and $k=1,2,\ldots,Q/2$. Consequently,

$$\hat{i}_{\mathrm{UB}}(\mathbf{y})=\arg\min_i\min_k\left\|\mathbf{y}_2-\alpha\sqrt{3\mathcal{E}_b/L}\,\hat{\mathbf{c}}_{i,k}\right\|^2\,. \tag{9}$$

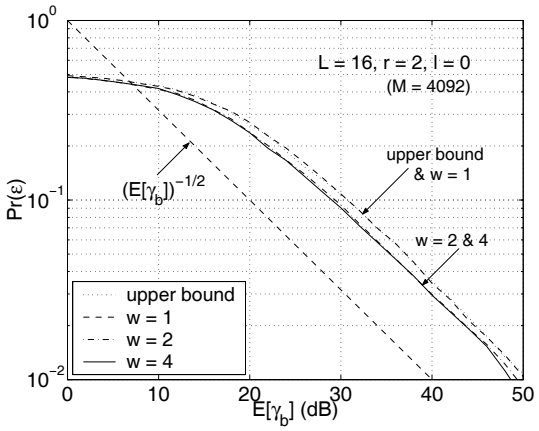

Fig. 3. Simulated upper bound and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ for various w.

Fig. 3 shows that, for the dyadic map ($r=2,\ell=0$), the approximation with $w=2$ nearly coincides with the upper bound and rapidly converges as w increases, revealing that the approximations to (8) and the upper bound based on (9) predict the $\Pr(\epsilon)$ trends of unintended receivers. The same trends are empirically observed with nested map DS/SS.

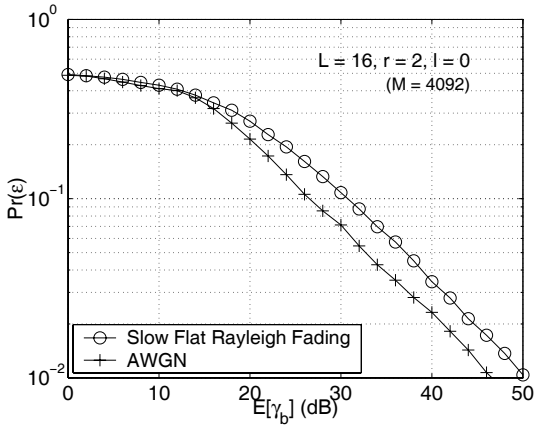

Fig. 4. Approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ in slow flat Rayleigh fading and AWGN.

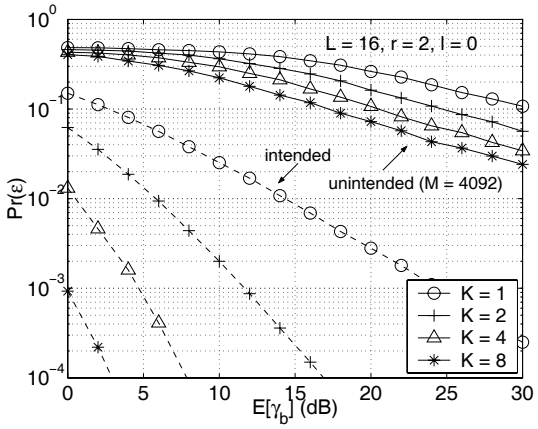

Fig. 5. Intended receiver $\Pr(\epsilon)$ (dashed) and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ (solid) for K degrees of spatial diversity in slow flat Rayleigh fading.

Fig. 3 also verifies that the unintended receiver $\Pr(\epsilon)$ curves at high $\overline{\gamma}_b$ indeed decay at the rate of $1/\sqrt{\overline{\gamma}_b}$.

4. DIVERSITY GAINS WITH CHAOTIC DS/SS

In this section we show that the unintended receivers for nested map-based chaotic DS/SS cannot fully exploit the available degrees of diversity in Rayleigh fading channels.

For the nested maps, the time- and frequency-selectivity of channel and the available degrees of diversity K do not affect the asymptotic decaying rate of unintended receiver $\Pr(\epsilon)$. Specifically, the decaying rate of $1/\sqrt{\overline{\gamma}_b}$ in slow flat fading, the worst case channel, is also the decaying rate in AWGN [3]. This is illustrated in Fig. 4 for the dyadic map. The unintended user $\Pr(\epsilon)$ in AWGN provides a lower bound on the unintended user $\Pr(\epsilon)$ over any fading channel with the same average received SNR, regardless of the available degrees of diversity. This lack of dependence of the decaying rate on the degrees of diversity in the channel is due to chaotic spreading. Indeed, from the perspective of unintended users, chaotic spreading can be viewed as additional fading process with uniform PDF, dominating the channel fading process and, hence, the decaying rate.

Fig. 4 also shows that the gap between the $\Pr(\epsilon)$ in slow flat fading and the $\Pr(\epsilon)$ in AWGN is less than 4 dB. As a result, in the presence of K degrees of spectral or temporal diversity, the unintended receiver $\Pr(\epsilon)$ gap in $\overline{\gamma}_b$ between $K = 1$ and $K = \infty$ is at most 4 dB. This small gap is due to the dominant effect of the fading process $c[n]$ on the $\Pr(\epsilon)$.

K-receiver antenna diversity, yielding K-fold average output SNR gains, cannot be fully exploited by unintended receivers. As Fig. 5 demonstrates, the $\Pr(\epsilon)$ improvements due to increasing the number of antenna elements are only substantial for intended users. This is a direct consequence of the difference in the asymptotic decay rates between the intended and unintended receiver $\Pr(\epsilon)$. Even for scenarios where the unintended receiver can exploit larger number of antennas, the additional number of antennas required for unintended receiver to outperform intended receivers at a target $\Pr(\epsilon)$ is substantial. For instance, $K \approx 256$ antennas are needed by the unintended user to outperform a single-antenna intended receiver at a target $\Pr(\epsilon)$ of 0.1 for a dyadic map DS/SS with $L = 16$, and even higher K's for systems with higher r, ℓ, and L.

5. CONCLUSION

In this paper we investigated the $\Pr(\epsilon)$ advantages provided to intended users by a class of chaotic DS/SS systems over fading channels. For these systems, we showed that the $\Pr(\epsilon)$ of unintended receivers with K independent fading channels improves only as $1/\sqrt{\mathrm{SNR}}$, unlike the intended receiver $\Pr(\epsilon)$, which decays as $1/(\mathrm{SNR})^K$. We also developed methods for quantifying the unintended receiver $\Pr(\epsilon)$, and demonstrated that unintended receivers cannot fully realize temporal, spectral, or receiver antenna diversity gains, showing that chaotic DS/SS can provide reliable and private communication over fading channels.

6. REFERENCES

[1] 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, no. 9, pp. 1110–1114, Sept. 2001.

[2] 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, no. 5, pp. 662–690, May 2002.

[3] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design," accepted for publication in *IEEE Trans. Signal Processing*.