Statistical properties of chaotic binary sequences

Bogdan Cristea, Member, IEEE

Abstract—Mean value and cross-covariance function of chaotic binary sequences are evaluated for chaotic maps with specific properties. We also take into account the effect of fixed- and floating-point representations on statistical properties of chaotic generators. Thus, one is able to obtain possible candidates for pseudo-random binary sequences generation. Results of statistical tests applied to chaotic binary sequences are presented. The chaotic binary sequences thus obtained could be used for security improvement in IEEE 802.11 standard.

Index Terms—Chaos, Cryptography, Random number generation, Binary sequences

I. INTRODUCTION

Pseudo-random binary sequences have applications in several domains including information theory (informational sources), spread-spectrum systems (spreading sequences) and cryptography (stream ciphers, key generation, initialization vectors, etc.).

Chaotic generators were already studied for cryptographic applications [1], [2], [3] due to their specific properties: sensitivity to initial conditions, random-like behavior, nonlinear dynamics, etc. As already noticed in [1], the main difficulty when using chaotic generators in cryptography is the fact that chaotic generators take values from a continuous, infinite space, while classical encryption techniques operate on a discrete, finite space. However, since most chaotic generators are implemented using a finite precision (fixed- or floating-point), the conversion from the continuous space to the discrete space is realized implicitly [3]. Further conversion techniques allow to pass from the discrete space to a binary space thus obtaining chaotic binary sequences [4].

In order to obtain pseudo-random binary sequences, previously proposed approaches use a bit extraction technique so that one or several bits are extracted from each chaotic value. However, there are few studies related to the selection of chaotic maps with good statistical properties and how the bit extraction technique must be designed [3], [4]. These are the main topics aborded in our paper. The originality of our approach resides on the fact that we take into account the effect of fixed- and floating-point representations on statistical properties of chaotic generators.

The rest of the paper is organized as follows. In section II the theoretical background used in our developments is presented. The definitions for the mean value and cross-covariance function of chaotic binary sequences are given. Subsections II-A and II-B give simplified expressions of mean value and cross-covariance function, respectively, for chaotic maps with specific properties. Thus one is able to obtain possible candidates for pseudo-random binary sequences generation. Results of statistical tests applied to chaotic binary sequences are presented in section III. Finally some conclusions are given in section IV.

II. MEAN VALUE AND CROSS-COVARIANCE FUNCTION OF CHAOTIC BINARY SEQUENCES

We consider chaotic sequences \( \{x_n\} \) generated by a function (chaotic map) \( \tau : [0,1] \rightarrow [0,1] \):

\[
x_n = \tau(x_{n-1})
\]

where \( n \in \{1,2,\ldots\} \). Each chaotic value, \( x_n \), and the parameters of the chaotic map are represented using fixed- or floating-point representation.

Any chaotic map, defined on some interval \([a,b] \), \( f : [a,b] \rightarrow [a,b] \), can be redefined on the interval \([0,1] \), using the transformation:

\[
\tau(x) = \frac{f(a + (b-a)x) - a}{b-a}
\]

The choice of the \([0,1] \) interval allows the simplification of our mathematical developments.

Starting from a given value \( x \in [0,1] \) one can obtain the bits of the fractional part using a sum of threshold functions [4]:

\[
b_i(x) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \sigma \frac{x}{2^i} (x)
\]

\( i \in \{1,2,\ldots\} \). When a fixed-point representation is used for \( x \), the threshold function \( \sigma_i(x) \) has the expression:

\[
\sigma_i(x) = \begin{cases} 0 & , x < t \\ 1 & , x \geq t 
\end{cases}
\]

and, when a floating-point representation is used, the threshold function is:

\[
\sigma_i(x) = \begin{cases} 0 & , x < t \\ 1 & , e^x \geq t 
\end{cases}
\]

where \( e \) is the non-biased exponent of the floating-point value \( x \) [3].

The binary sequence obtained using \( b_i(x) \), \( i \in \{1,2,\ldots\} \) is called a chaotic binary sequence if \( x \) is obtained from a chaotic generator [1]. In the following we are interested to determine under which conditions the chaotic binary sequence is pseudo-random.

For this purpose, the following statistical measures of the chaotic binary sequence are defined [4]:

--Chaos, Cryptography, Random number generation.
1) mean value

\[ < b_i > = \int_0^1 b_i(x) f^*(x) dx \]  

(6)

2) cross-covariance function

\[ < \rho^{(2)}(l; b_i, b_j) > = \int_0^1 (b_i(x) - < b_i >) (b_j(x) - < b_j >) f^*(x) dx \]  

(7)

where \( f^*(x) \) is the density function of the chaotic map \( \tau \) [6] p. 8] and \( \tau^l(x) \) represents the output of the chaotic map after \( l \) iterations (1). Since a non-zero cross-covariance function will imply the statistical dependence of bits, we are interested to determine when the cross-covariance function is (close to) zero (5).

A. Mean value

Starting from the definition of the mean value (6) and using (3) the mean value can be rewritten as:

\[ < b_i > = \sum_{r=1}^{2^l-1} (-1)^{r-1} p_r \frac{r}{2^l} \]  

(10)

where

\[ p_r(t) = \int_0^1 \sigma_t(x) f^*(x) dx \]  

(11)

If the threshold function \( \sigma_t(x) \) is defined under fixed-point representation (4), then \( p_r(t) \) (11) can be written as:

\[ p_r(t) = \int_0^1 f^*(x) dx \]  

(12)

and if \( \sigma_t(x) \) is defined under floating-point representation, then:

\[ p_r(t) = \begin{cases} \int_{2^{e_{\min}}+1}^{2^{e_{\min}}+k} f^*(x) dx & t \leq 0.5 \\ \sum_{k=1}^{e_{\min}+k} \int_{2^{e_{\min}}+k}^{2^{e_{\min}}+k+1} f^*(x) dx & t > 0.5 \end{cases} \]  

(13)

where \( e_{\min} < 0 \) is the minimum value of the exponent \( e \) (for example, in floating-point double precision \( e_{\min} = -1022 \) (8)). In order to obtain (13) the interval \([0, 1]\) is divided into sub-intervals defined by a constant exponent \( e \) (5) and the definition of the threshold function \( \sigma_t(x) \) (5) is used.

Note that the expression of the mean value (10) depends only of the density function, \( f^*(x) \), and the representation used for the chaotic map, \( \sigma_t(x) \). Thus a whole class of chaotic maps having the same density function can be characterized using (10).

To further simplify the expression of the mean value (10) the density function \( f^*(x) \) must be specified. We have considered two examples of density functions:

\[ f^*(x) = 1 \]  

(14)

and

\[ f^*(x) = \frac{1}{\pi \sqrt{x(1-x)}} \]  

(15)

corresponding to Bernoulli map

\[ \tau(x) = \text{mod}(px, 1) \]  

(16)

where \( p \) is the parameter of Bernoulli map and logistic map

\[ \tau(x) = 4x(1-x) \]  

(17)

respectively [6].

Thus, it can be shown that when the density function is given by (14), under fixed-point representation, the mean value is:

\[ < b_{i,t} > = 0.5 \]  

(18)

\( i \in \{1, 2, \ldots\} \) and under floating-point representation:

\[ < b_{i,t} > = \begin{cases} 1 - 2^{e_{\min}} & , i = 1 \\ 0.5 & , i \in \{2, 3, \ldots\} \end{cases} \]  

(19)

So, conditions (5) and (9) can be used to select from all available chaotic maps potential candidates for pseudo-random binary sequences generation.

In the next two subsections analytical expressions for the mean value and cross-covariance function will be deduced for chaotic maps with specific properties.
In order to prove (18) and (19) see appendix.

The result given by (19) can be explained by the fact that, when a floating-point representation is used, the first bit $i = 1$ is the hidden bit of the fractionary part (significand) [5]. Since the probability to have this bit set (normalized numbers) is much greater than the probability to have this bit unset (denormalized numbers) we obtain: $< b_1 > \approx 1$.

Following (18) and (19) one can conclude that, when the density function is given by (14), all bits of the fractionary part (except the hidden bit) can be used to obtain balanced chaotic binary sequences.

When the density function is given by (15), under fixed-point representation, the mean value is:

$$< b_i > = 0.5 - \frac{1}{\pi} \sum_{r=1}^{2^{i-1}} (-1)^{r-1} \sin \left( \frac{\pi r}{2^{i-1}} - 1 \right)$$  

and under floating-point representation:

$$< b_i > = \begin{cases} 0.5 - \frac{1}{\pi} \sin \left( 2^e_{\min+1} - 1 \right), & i = 1 \\ - \frac{1}{\pi} \sum_{r=1}^{2^{i-1}} (-1)^{r-1} \sin \left( r 2^e_{\min+1} - 1 \right), & i > 1 \end{cases} \sum_{r=2^{i-1}+1}^{2^i-1} (-1)^{r-1} p_r \left( \frac{r}{2^i} \right)$$  

where

$$p_r(t) = \frac{1}{\pi} \sum_{k=1}^{e_{\min}} \left( \sin \left( 2^e_{\min+k} - 1 \right) \right) - \sin \left( t 2^e_{\min+k} - 1 \right) \quad \forall t > 0.5$$

In order to prove (20) and (21) see appendix.

Numerical evaluation of relations (20) and (21) shows that, when the density function is given by (15), under fixed-point representation, all bits of the fractionary part can be used to obtain balanced chaotic binary sequences (Fig. 1a). However, under floating-point representation, the mean value only converges to 0.5 as the bit index $i$ (21) increases (Fig. 1b). So, in this case, the first bits of the fractionary part must be discarded and thus a less efficient bit extraction technique must be used in order to obtain balanced chaotic binary sequences.

So, using the mean value of the chaotic binary sequence, one is able to determine the bits of the fractionary part needed to obtain chaotic binary sequences with an equal number of zeros and ones. In order to gain further insights into the statistical properties of chaotic binary sequences, higher order statistics must be used. In the following subsection the cross-covariance function is evaluated in order to characterize the correlations at the bit level in chaotic binary sequences.

### B. Cross-covariance function

In order to simplify the expression of the cross-covariance function (7), the chaotic map $\tau(x)$ is chosen so that [4]:

$$|g_i'(x)| f^*(g_i(x)) = \frac{1}{N_\tau} f^*(x) \forall 1 \leq i \leq N_\tau$$  

where $g_i(x) = \tau_i^{-1}(x)$, $g_i'(x)$ is the first derivative of $g_i(x)$, $\tau_i(x)$ is defined on a subinterval $[d_{i-1}, d_i] \subset [0, 1]$ so that $\tau_i(x)$ is invertible, $\tau_i(x) = \tau(x) \forall x \in [d_{i-1}, d_i]$ and $N_\tau$ is the number of subintervals in $[0, 1]$ on which $\tau(x)$ is invertible. Among the chaotic maps verifying (23) one can mention Bernoulli map, tent map, logistic map and Chebyshev polynomials [4].

Using (24) the cross-covariance function can be written as [4]:

$$< \rho^{(2)}(0; b_i, b_j) > = \sum_{r=1}^{2^i-1} \sum_{s=1}^{2^j-1} (-1)^{r+s} \left( p_r \left( \max \left( \frac{r}{2^i}, \frac{s}{2^j} \right) \right) - p_r \left( \frac{r}{2^i} \right) p_r \left( \frac{s}{2^j} \right) \right)$$  

$$< \rho^{(2)}(l; b_i, b_j) > = \frac{1}{N_\tau^l} \sum_{r=1}^{2^i-1} \sum_{s=1}^{2^j-1} (-1)^{r+s} \left( \Pi_{k=1}^l \left( \frac{r}{2^i} \right) \left( \frac{s}{2^j} \right) \right)$$  

$\forall l > 0$, where $p_r(t)$ has the expression given by (11).

The cross-covariance function, (24) and (25), depends not only of the density function, $f^*(x)$, and the representation used for the chaotic map, $\sigma_i(x)$, but also of the chaotic map itself, $\tau(x)$, and the sign of its derivative, sign ($\tau'(x)$). Note also that the cross-covariance function (25) is inverse proportional with the number of subintervals on which $\tau(x)$ is invertible, $N_\tau$. Thus, in order to have a cross-covariance function with values near to zero, the chaotic map must be chosen so that $N_\tau$ is large enough. For example, the Bernoulli map (16) with $p = 1.99$ has $N_\tau = 2$, but when $p = 3.99$ we have $N_\tau = 4$.

Numerical evaluation of (25) for Bernoulli map under floating-point representation is given in Fig. 2a and 2b. It can be seen that, when the number of iterations $l$ is fixed, the correlations between the bits of different chaotic values can be reduced by choosing the parameter of the Bernoulli map so that $N_\tau$ is large enough.

However, the expression of the cross-covariance function is too complex to provide insights into statistical properties of chaotic maps without full specification of the chaotic map. Since our goal is to find pseudo-random generators, we have found more useful to directly apply statistical tests (6) on chaotic binary sequences. The results of the application of statistical tests are given in the following section.

### III. Simulation results

In our simulations we use the chaotic maps defined by (16) and (17), the tent map

$$\tau(x) = p(1 - |1 - 2x|)$$  

where $p = 0.99$ and the Chebyshev polynomial of third order

$$\tau_p(x) = (2x - 1)(2\tau_p(x) - 1) + 1 - \tau_{p-2}(x)$$  

where $\tau_1(x) = x$, $\tau_0(x) = 1$ and $p = 3$. 
Since under a finite representation (fixed- or floating-point) the chaotic sequences are periodic, we use in our simulations initial conditions generating chaotic sequences with the longest period [9]. The parameters used in our simulations are synthesized in Table I. The fixed-point representation on 32 bits is defined by one bit for the sign, 3 bits for the integer part and 28 bits for the fractional part. The floating-point representation on 32 bits is the IEEE754 floating-point single-precision representation [8]. We use also the floating-point double-precision representation with the same initial conditions as for single-precision (this choice is due to the fact that in double-precision finding the longest period takes a much longer time than for single-precision). From each chaotic value, represented with finite precision, the bits of the fractional part (except the hidden bit when floating-point representation is used) are extracted and thus chaotic binary sequences are obtained.

Using chaotic sequences represented with floating-point double precision, we have numerically computed the probability density function for each chaotic map. Thus, we have found that Bernoulli map and tent map belong to the same class of chaotic maps having the density function given by (14). Logistic map and Chebyshev polynomial of third order have a density function close to (15). So, the results obtained for the mean value using (14) and (15) are applicable for tent map and Chebyshev polynomial of third order, respectively.

In Fig. III we have computed the number of zeros and

| Chaotic map       | Representation | Initial condition      | Period len. |
|-------------------|----------------|------------------------|-------------|
| Bernoulli map     | fixed (32 bits)| 0.58268645778298...   | 3050        |
|                   | float (32 bits)| 0.24101102352142...   | 3827        |
| Tent map          | fixed (32 bits)| 0.05443460385232...   | 583         |
|                   | float (32 bits)| 0.4090572135508...    | 4311        |
| Logistic map      | fixed (32 bits)| 0.0009547546505...    | 13404       |
|                   | float (32 bits)| 0.99998587869918...   | 930         |
| Chebyshev pol. of third order | fixed (32 bits) | 0.99994068592786... | 10014       |
|                   | float (32 bits) | 0.0544851856231...    | 1821        |

TABLE I
SIMULATION PARAMETERS
ones of chaotic binary sequences with $10^6$ bits. Thus, we have found that logistic map and Chebyshev polynomial of third order under single-precision floating-point representation generate chaotic binary sequences with a greater number of ones than zeros. This result is in agreement with the theoretical result obtained for the mean value (21) (Fig. 1b). Using the same representation, Bernoulli map and tent map have an almost equal number of zeros and ones (19). When the fixed-point representation is used, all considered chaotic maps generate balanced chaotic binary sequences. The differences with respect to theoretical results, (18), (19) and (20), are due to the fact that, in simulation, we use a finite precision, while in theory we have supposed that the number of bits of the fractionary part is infinite. However, if the number of bits of the fractionary part is large enough, we find a good agreement between theory and simulation.

We have also applied all 16 statistical tests described in [7] on chaotic binary sequences generated with the above described chaotic maps. We have used 100 binary sequences of $10^6$ bits each. The best results were obtained with Bernoulli map (Fig. 4a) and tent map (Fig. 4b) under floating-point double precision representation.

Thus, the theoretical results given in subsections II-A and II-B have allowed to select chaotic maps suitable for pseudo-random sequences generation. Further, one can select the bits to be extracted from each chaotic value for pseudo-random sequences generation. Bernoulli map and tent map were selected since chaotic maps with density function given by (14) generate balanced chaotic binary sequences using all bits of the fractionary part. Note that the parameter of Bernoulli map $p = 3.99$ was chosen based on the fact that the cross-covariance function has smaller values when $N_t = 4$.

By simulation, we have noticed that the period length of chaotic sequences has an impact on the results of statistical tests. The longer the period is, the better are the results of statistical tests. This observation could provide another explanation why the best results were obtained using double-precision floating-point representation (Fig. 4a and 4b).

Instead of selecting initial conditions generating chaotic sequences with the longest period, one can use arbitrary initial conditions and the perturbations technique [10]. Our simulations have shown that, with respect to our method, the perturbations technique brings little improvements of the results of statistical tests. However, the perturbations technique represents a practical approach for the implementation of chaotic pseudo-random generators e.g. in the Wired Equivalent Privacy (WEP) protocol of IEEE 802.11 standard [11].

The WEP protocol is particularly interesting for the application of chaotic generators since the initialization vector (initial condition) is often changed. Thus, short length periods or fixed points, specific for chaotic maps represented with finite precision, can be avoided. We expect that security improvements in IEEE 802.11 standard could be achieved by replacing the RC4 pseudo-random generator with chaotic binary generators.

IV. CONCLUSION

The mean value and cross-covariance function of chaotic binary sequences were analytically computed. The considered chaotic sequences were represented using fixed- and floating-point representations. We have shown that chaotic binary
sequences can produce binary sequences with an equal number of zeros and ones if the density function is \( f^*(x) = 1 \). Further, these chaotic binary sequences were obtained using all the bits of the fractionary part of the chaotic value. This bit extraction technique is highly efficient with respect to previously proposed methods. Improvements of correlation properties of chaotic binary sequences are possible by increasing the number of subintervals, \( N_\tau \), on which the chaotic map is invertible. Using these results, possible candidates (chaotic maps) for pseudo-random binary sequences generation can be selected. We have also evaluated, by means of statistical tests, chaotic binary sequences thus obtained.

Further research needs to be conducted for chaotic maps under fixed-point representation. We have considered a relatively short fixed-point representation on 32 bits, but we expect that increasing the precision in this case could provide also good pseudo-random binary sequences. Another interesting research direction is to find out how much precision is needed in order to obtain chaotic binary sequences with good statistical properties. Also, it should be interesting to develop statistical measures by taking into account the finite representation of chaotic values, that is by replacing in the definitions of the mean value and cross-covariance function the integral by a sum.

A possible application of chaotic binary sequences could be the WEP protocol of IEEE 802.11 standard by replacing the RC4 pseudo-random generator with chaotic binary generators. However, further cryptanalysis research should be done in order to prove the validity of this approach.

APPENDIX

i. **Mean value for** \( f^*(x) = 1 \)

Fixed-point representation
Knowing that (12):

\[
p_\tau(t) = 1 - t
\]

we get (10):

\[
< b_i > = \sum_{r=1}^{2^{i-1}} (-1)^{r-1} \left(1 - \frac{r}{2^i}\right)
\]

With

\[
\sum_{r=1}^{n} (-1)^{r-1} r = (-1)^{n-1} \frac{n+1}{2}
\]

and (29) we get (18).

Floating-point representation
Knowing that (13):

\[
p_\tau(t) = \begin{cases} 2^{\epsilon_{\text{min}}} (1 - 2t) + 1 - 2^{\epsilon_{\text{min}}}, & t \leq 0.5 \\ (2(1-t)(1-2^{\epsilon_{\text{min}}}), & t > 0.5 \end{cases}
\]

we get (10):

if \( i = 1 \)

\[
< b_i > = p_\tau \left( \frac{1}{2} \right) = 1 - 2^{\epsilon_{\text{min}}}
\]

if \( i > 1 \)

\[
< b_i > = \sum_{r=1}^{2^{i-1}} (-1)^{r-1} p_\tau \left( \frac{r}{2^i} \right) + \sum_{r=2^{i-1}+1}^{2^i} (-1)^{r-1} p_\tau \left( \frac{r}{2^i} \right) = \frac{1}{2}
\]

So we have completely proved (19).

ii. **Mean value for** \( f^*(x) = \frac{1}{\pi \sqrt{x(1-x)}} \)

The following result is used:

\[
\int_0^1 \frac{1}{\pi \sqrt{x(1-x)}} dx = \frac{1}{\pi} \text{asin} \left( 2x - 1 \right)
\]

Fixed-point representation
With (36) and (12) we get:

\[
p_\tau(t) = 0.5 - \frac{1}{\pi} \text{asin} \left( 2t - 1 \right)
\]
So (10):

\[
< b_i > = 0.5 - \frac{1}{\pi} \sum_{r=1}^{2^{i-1}-1} (-1)^{r-1} \arcsin \left( \frac{r}{2^{i-1}} - 1 \right)
\]  \hspace{1cm} (38)

Floating-point representation with (36) and (13) we get:

\[
p_{\tau}(t) = \begin{cases} 
0.5 - \frac{1}{\pi} \arcsin \left( 2^{e_{\text{min}}+2} - 1 \right), & t \leq 0.5 \\
\frac{1}{\pi} \sum_{k=1}^{-e_{\text{min}}} \left( \arcsin \left( 2^{e_{\text{min}}+k+1} - 1 \right) - \arcsin \left( 2^{e_{\text{min}}+k+1} - 1 \right) \right), & t > 0.5
\end{cases}
\]  \hspace{1cm} (39)

So (10):

If \( i = 1 \)

\[
< b_1 > = p_{\tau}(\frac{1}{2}) = 0.5 - \frac{1}{\pi} \arcsin (2^{e_{\text{min}}+1} - 1)
\]  \hspace{1cm} (40)

If \( i > 1 \)

\[
< b_i > = \sum_{r=1}^{2^{i-1}-1} (-1)^{r-1} p_{\tau}(\frac{r}{2^{i-1}}) + \sum_{r=2^{i-1}+1}^{2^{i-1}-1} (-1)^{r-1} p_{\tau}(\frac{r}{2^{i-1}})
\]  \hspace{1cm} (41)

\[
= -\frac{1}{\pi} \sum_{r=1}^{2^{i-1}-1} (-1)^{r-1} \arcsin \left( 2^{e_{\text{min}}-i+2} - 1 \right) \quad (42)
\]

\[+ \sum_{r=2^{i-1}+1}^{2^{i-1}-1} (-1)^{r-1} p_{\tau}(\frac{r}{2^{i-1}}) \quad (43)
\]

So we have completely proved (21).

REFERENCES

[1] L. Kocarev, “Chaos-based cryptography: a brief overview,” \textit{Circuits and Systems Magazine, IEEE}, vol. 1, no. 3, pp. 6–21, 2001.
[2] G. Alvarez, P. Montoya, G. Pastor, and M. Romera, “Chaotic cryptosystems,” in \textit{Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on}, pp. 332–338, 1999.
[3] S. Li, G. Chen, and X. Mou, “On the dynamical degradation of digital piecewise linear chaotic maps,” \textit{International Journal of Bifurcation and Chaos}, vol. 15, no. 10, pp. 3119–3151, 2005.
[4] T. Kohda and A. Tsuneda, “Statistics of chaotic binary sequences,” \textit{IEEE Trans. Inf. Theory}, vol. 43, pp. 104–112, Jan. 1997.
[5] D. Goldberg, “What every computer scientist should know about floating-point arithmetic.” Computing surveys, Mar. 1991.
[6] A. Lasota and M. C. Mackey, \textit{Chaos, fractals and noise}. New-York: Springer-Verlag, 1994.
[7] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, “A statistical test suite for pseudorandom number generators used in cryptographic applications,” tech. rep., National Institute of Standards and Technology, 2001.
[8] J. E. May, J. E. Riganati, and S. E. Sherr, “IEEE standard for binary floating-point arithmetic.” American National Standards Institute, July 1985.
[9] B. Cristea, P. Charge, D. Fournier-Prunaret, F. Peyrard, and J.-J. Mercier, “Behavior of chaotic sequences under a finite representation and its cryptographic applications,” \textit{IEEE Workshop on nonlinear maps and applications (NOMA’07)}, December 2007. Toulouse, France.
[10] H. Zhou and X.-T. Ling, “Realizing finite precision chaotic systems via perturbation of m-sequences.” Acta Electronica Sinica, 1997.
[11] M. Gast, \textit{802.11 Wireless networks. The definitive guide}. O’Reilly, 2005.