Fast Spectral Tests for Measuring Nonrandomness and the DES

Frank A. Feldman
Department of Physics, Suffolk University
Boston, MA 02114

Abstract — Two spectral tests for detecting nonrandomness were proposed in 1977. One test, developed by J. Gait [1], considered properties of power spectra obtained from the discrete Fourier transform of finite binary strings. Gait tested the DES [10,11] in output-feedback mode, as a pseudorandom generator. Unfortunately, Gait's test was not properly developed [3,4], nor was his design for testing the DES adequate.

Another test, developed by C. Yuen [2], considered analogous properties for the Walsh transform. In estimating the variance of spectral bands, Yuen assumed the spectral components to be independent. Except for the special case of Gaussian random numbers, this assumption introduces a significant error into his estimate.

We recently [3,4] constructed a new test for detecting nonrandomness in finite binary strings, which extends and quantifies Gait's test. Our test is based on an evaluation of a statistic, which is a function of Fourier periodograms [5]. Binary strings produced using short-round versions of the DES in output-feedback mode were tested. By varying the number of DES rounds from 1 to 16, it was thought possible to gradually vary the degree of randomness of the resulting strings. However, we found that each of the short-round versions, consisting of 1, 2, 3, 5 and 7 rounds, generated ensembles for which at least 10% of the test strings were rejected as random, at a confidence level approaching certainty.

A new test, based on an evaluation of the Walsh spectrum, is presented here. This test extends the earlier test of C. Yuen. Testing of the DES, including short-round versions, has produced results consistent with those previously obtained in [3].

We prove that our measure of the Walsh spectrum is equivalent to a measure of the skirts of the logical autocorrelation function. It is clear that an analogous relationship exists between Fourier periodograms and the circular autocorrelation function.

1. Introduction

Kolmogorov [7] and Chaitan [8] have established a theory of the information content of strings, which has been used to define random strings. Particular tests to detect certain irregularities of pseudorandom strings are presented in Knuth [9]. Fast spectral tests, in this spirit, have since been proposed. These tests evaluate either the fast Fourier transform (FFT) [6], or the fast Walsh transform (FWT) [12], of a finite test string. Both of these kinds of spectral tests were first proposed in 1977. One, presented by

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 243-254, 1988.

J. Gait [1], examined the Fourier power spectra. The other, presented by C. Yuen [2], examined analogous properties for the Walsh transform. In the form presented, neither of these early tests can be compared directly with the output of the tests described by Knuth.

The purpose of Gait's paper was to test the DES, in output-feedback mode, as a pseudorandom generator. A significant part of his paper was devoted to the development of a power spectrum test; this test was applied to binary strings of length 2^{15} bits generated by the DES. Each test string can be specified by approximately 2^{14} spectral components. Nevertheless, on the basis of twenty-seven sample points taken from the power spectrum of one such sequence, the DES output was judged to be random. Actually, one can show that the graphic display presented by Gait is too flat, and thereby offers strong evidence for rejecting this test string as random [3,4].

The test proposed by C. Yuen considered analogous properties for the discrete Walsh transform. Yuen tested output from two kinds of pseudorandom generators: a Gaussian generator, and a generator of uniformly distributed "reals" ranging from 0 to 1. Yuen recognized — as Gait did not — that "... a spectrum estimate that looks too flat is as suspect as one not flat enough." Yuen also recognized that estimates for individual contributions to the Walsh power spectrum are not consistent. To circumvent this difficulty he chose to consider bands of spectral contributions. In his estimate of the variance for a band, Yuen assumed the spectral contributions to be statistically independent. This assumption is valid for the case of random numbers with a Gaussian distribution. However, in the general case, this assumption violates the *Parseval constraint* [5] on the spectrum and introduces a significant error into ones estimate of the variance.

We recently [3,4] proposed a new test for detecting nonrandomness in finite binary strings. Our test extends and quantifies Gait's test. We tested binary strings of length 2^{15} bits which were produced using short-round versions of the DES, in output-feedback mode. By varying the number of DES rounds from 1 to 16, it was thought possible to gradually vary the degree of randomness of the resulting strings. We found that for ensembles of test strings generated by short-round versions, consisting of 1, 2, 3, 5 and 7 rounds, each ensemble yielded test strings for which at least 10% were rejected as nonrandom at a confidence level approaching certainty.

We now propose a similar test based on an evaluation of the Walsh spectrum. This test is an extension of Yuen's test. We note that the fast Walsh transform (FWT) can be obtained from the fast Fourier transform (FFT) by setting all sines to 0 and all cosines to 1. It is usual to find a program block in the FFT which reorders the indices — by combining first a bit reversal, followed by Gray coding of the indices [12]. If one deletes this block, one obtains a particular representation of the Walsh transform which has the various designations: natural ordered Walsh transform, Walsh-Hadamard transform, and Hadamard transform. The FWT is at least four times faster than the FFT, and demands half the memory. We use the symmetry properties of the Hadamard transform to derive recursion relations which facilitate the computation of certain expectations: the expectations for estimating powers and products of Walsh periodograms. Thereby, the estimates of the mean and the variance called for in our test can be computed both easily and with precision.

2. Test for Nonrandomness

Our test computes a statistic, which is dependent on a finite length binary string. This statistic is compared with the value expected for a random string. The input string is interpreted as nonrandom if the computed value of the statistic differs too much from the expected value.

TEST (For the r^{th} moment; where $r = 4$, or $r = 6$)

INPUT: A string $x = x_0, \ldots, x_{n-1}$ of length $n = 2^k$.

PARAMETERS:

INTEGERS: $r = 4$, or $r = 6$. And $n = 2^k$, where n is sufficiently large [3,4].

REAL: t, the desired significance level, with $0 < t < 1$.

OUTPUT: "May be Random" or "Not Random."

STEP 1:

Representing the bits of x, with the values 1 and -1, the fast Walsh transform (FWT), $\hat{x}$, of x is computed. The algorithmic running time of the FWT is $O(nlogn)$. The space requirement is $O(n)$.

STEP 2:

The computation of the r^{th} power for each of the n Walsh transform components

$$\hat{x}^r = (\hat{x})^r,$$

where the input parameter r specifies that the r^{th} *moment* is being tested, and r is an *even* integer greater than 2.

STEP 3:

The computation of the statistic D_r, where

$$D_r = \sum_{k=0}^{n-1} (\hat{x}_k^r - m_r)/v_r. \qquad (2.1)$$

The values assigned to m_r and v_r are defined in Section 4, by eq. (4.2) and (4.3).

STEP 4.

The decision is made "Not Random" or "May be Random."

The null hypothesis H_0 — that the input $x_0 \ldots x_{n-1}$ is random — is rejected at a level of significance, determined by the input t, if the integral

$$\frac{1}{\sqrt{2\pi}} \int_{-D_r}^{D_r} \exp\left(-\frac{y^2}{2}\right) dy \qquad (2.2)$$

is less than $1 - t$.

3. Properties of the Walsh Transform

The Walsh transform is an orthogonal transformation of $n = 2^k$ variables. In *natural order* this transformation is effected through the use of a *Hadamard matrix.* For order 2, the symmetric Hadamard matrix is defined as

$$H[2] = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Higher order Hadamard matrices can be defined recursively as the direct product of lower order Hadamard matrices. Thus, for example

$$H[2n] = \begin{pmatrix} H[n] & H[n] \\ H[n] & -H[n] \end{pmatrix}$$

We prefer to define the Hadamard matrix, for order $n = 2^k$, in terms of its matrix elements. First, let the matrix indices s and t be represented in binary form as $(s_{k-1} \ldots s_0)_2$ and $(t_{k-1} \ldots t_0)_2$. Then

$$H_{s,t} = \prod_{p=0}^{k-1} (-1)^{s_p t_p}. \tag{2.1}$$

The Walsh transform of $x_0, \ldots, x_{n-1}$ is represented as

$$\hat{x}_s = \sum_{t=0}^{n-1} H_{s,t} x_t.$$

We show below that the *inverse* transformation is

$$x_s = \frac{1}{n} \sum_{t=0}^{n-1} H_{s,t} \hat{x}_t.$$

Five basic properties which follow from the above definitions are:

PROPERTY 1 (symmetry)

$$H_{s,t} = H_{t,s}$$

PROPERTY 2 (summation)

$$\sum_{s=0}^{n-1} H_{s,t} = n\delta(t),$$

where $\delta(s)$ is the *unit impulse* [5] function.

PROPERTY 3 (product)

$$H_{s,t}H_{s,p} = H_{s,t\oplus p},$$

where $t \oplus p \overset{\text{def}}{=} (t_{k-1} \oplus p_{k-1} \ldots t_0 \oplus p_0)_2$, and $\oplus$ is the "xor" operation (addition modulo 2). For example $t \oplus t = 0$.

Proof:

$$\begin{aligned} H_{s,t}H_{s,p} &= \prod_{q=0}^{k-1} (-1)^{s_q(t_q \oplus p_q)} \\ &= H_{s,t\oplus p}. \end{aligned}$$

PROPERTY 4 (orthogonality)

$$\begin{aligned} \frac{1}{n}\sum_{t=0}^{n-1} H_{s,t}H_{t,p} &= \delta(s \oplus p) \\ &= \delta(s-p). \end{aligned}$$

PROPERTY 5 (*logical* shift)

$$H_{s,t}\hat{x}_t = \sum_{p=0}^{n-1} H_{t,p}x_{p\oplus s}.$$

Proof: $H_{s,t}\hat{x}_t = \sum_{p=0}^{n-1} H_{s,t}H_{t,p}x_p = \sum_{p=0}^{n-1} H_{t,s\oplus p}x_p$, where PROPERTY 3 has been used. And then, since $s \oplus p$ is simply a permutation of the integers $(0, \ldots, n-1)$ over the range of the "dummy index" p, a relabelling of this index yields the sum $\sum_{p=0}^{n-1} H_{t,p}x_{p\oplus s}$.

We define Walsh periodograms as

$$I_s = (1/n)\hat{x}_s^2.$$

A sequence known as the *logical* autocorrelation function is defined as

$$\tilde{a}_s = \frac{1}{n}\sum_{t=0}^{n-1} x_t x_{t\oplus s}.$$

Theorem 1.

$\tilde{a}_0, \ldots, \tilde{a}_{n-1}$ and $I_0, \ldots, I_{n-1}$ are Walsh transform pairs [12]. That is

$$I_s = \sum_{t=0}^{n-1} H_{s,t}\tilde{a}_t,$$

and

$$n\tilde{a}_s = \sum_{t}^{n-1} H_{s,t}I_t.$$

Corollary (Parseval's theorem for the Walsh transform)

$$\sum_{s=0}^{n-1} I_s = n\tilde{a}_0\,, \text{ or equivalently } \sum_{s=0}^{n-1} \hat{x}_s^2 = n\sum_{s=0}^{n-1} x_s^2.$$

A degenerate case of Parseval's theorem occurs with the restriction $x_s \in [-1,1]$, in that it yields a *deterministic* value for the sum of the squared Walsh coefficients. And for this case

$$\sum_{s=0}^{n-1} \hat{x}_s^2 = n^2.$$

Consider the following important example. When testing n random bits, it is usual to map bit values from $[0,1]$ onto the values $[-1,1]$. And for this case, Parseval's theorem tells us that the summed value for the "power spectrum" is *identical* for all test strings. This result is referred to as *deterministic* for the following reasons: First, the summed value is n^2 for any test sequence, independent of its distribution. Second, assume the set $x_0,\ldots,x_{n-1}$ to be a set of random variables, whose values are either 1 or -1. Let this set be assigned an arbitrary joint probability distribution. Yet, not only is the ensemble average for the summed "power spectrum" equal to n^2, but in addition the variance of this sum is zero. Thus, the induced probability distribution for the summed "power spectrum" degenerates into a singular distribution known as a *Dirac delta function*.

Such is also the case for the FFT. One can choose the option of testing *spectral bands*, as in [2]. However, to be in the asymptotic region for which the central limit theorem holds [3], one may have to increase the length n of the test strings. An alternative approach will be developed in the next section. However, the groundwork will be developed below.

Our main contribution, in this section, is presented in the form of two theorems. These two theorems will be stated below in the context of the FWT and the logical autocorrelation function $\tilde{a}$. However, both of these theorems are also valid in the context of the FFT, with the replacement of the FWT by the FFT, the Walsh periodogram by the Fourier periodogram [5], and the logical autocorrelation function by the circular [5] (positively wrapped [6]) autocorrelation function. This last replacement is effected by changing $s \oplus t$ to $(s+t) \bmod n$. Both of these theorems can be proved by means of a straightforward application of the five basic transform PROPERTIES listed earlier in this section.

Theorem 2.

$$\sum_{t=0}^{n-1} H_{s,t} I_t^2 = n\sum_{t=0}^{n-1} \tilde{a}_t \tilde{a}_{t\oplus s}. \tag{3.1}$$

Corollary

$$\sum_{s=0}^{n-1} I_s^2 = n\sum_{s=0}^{n-1} \tilde{a}_s^2. \tag{3.2}$$

Theorem 3.

$$\sum_{t=0}^{n-1} H_{s,t} I_t^3 = n \sum_{t=0}^{n-1} \sum_{p=0}^{n-1} \tilde{a}_t \tilde{a}_{t \oplus s \oplus p} \tilde{a}_p . \tag{3.3}$$

Corollary

$$\sum_{s=0}^{n-1} I_s^3 = n \sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \tilde{a}_s \tilde{a}_{s \oplus t} \tilde{a}_t . \tag{3.4}$$

Discussion of these two theorems is postponed to the next section.

4. Ensemble Averages

In testing for randomness an *a priori* requirement is that the type of randomness be defined. This requirement is met by considering the string variables to be random variables and then assigning a joint probability distribution for these variables. The theorems presented in the previous section can be applied to these random variables. It is possible to interpret these theorems in terms of ensemble averages. Consider, for example, the corollary of theorem 2. We shall restrict our attention to *binary* test strings of length 2^k — where for convenience, bits will be represented as -1 and 1. Taking expectations, yields the relation

$$E[\sum_{s=0}^{n-1} \hat{x}_s^4] = n^3 + n^3 \sum_{s=0}^{n-1} E[\tilde{a}_s^2], \tag{4.1}$$

where use has been made of the relation $\tilde{a}_0 = 1$. Thus, the expected sum of the fourth power of the spectral components is related to the expected sum of the square of the terms making up the skirts of the logical autocorrelation function. It is clear that, for the FFT, a similar relation exists between the squared periodograms and the circular autocorrelation function.

We now restrict our attention to *symmetric Bernoulli sequences.* That is, sequences $x_0, \ldots, x_{n-1}$ which are independent and identically distributed with $Pr(x_k = 1) = \Pr(x_k = -1) = 1/2$, for $k = 0, \ldots, n-1$. Our goal is to numerically evaluate terms of the form

$$m_r = E[\sum_{s=0}^{n-1} \hat{x}_s^r] \tag{4.2}$$

and

$$v_r = E[(\sum_{s=0}^{n-1} \hat{x}_s^r)^2] - m_r^2 \tag{4.3}$$

for $r = 4$ and $r = 6$. These two expectations are called for as parameters in STEP 3 of our test for nonrandomness.

Combining ,the symmetry of the distribution with the structure of the Walsh transform yields the equivalences

$$m_r = nE[\hat{x}_0^r], \tag{4.4}$$

and

$$v_r = nE[\hat{x}_0^{2r}] + n(n-1)E[\hat{x}_0^r\hat{x}_1^r] - n^2(E[\hat{x}_0^r])^2. \tag{4.5}$$

Thus to complete the numerical evaluation of m_r and v_r it is necessary to compute expectations of the form $E[\hat{x}_0 s]$ and $E[\hat{x}_0^s\hat{x}_1^s]$, where s is an even integer. This can be accomplished by means of the two recursion relations which are presented below.

First note that $E[\hat{x}_k^s] = E[\hat{x}_0^s]$ for $k = 1 \ldots n-1$ and $E[\hat{x}_0^{2s+1}] = 0$. We now use the notation $\hat{x}_k(n)$ to indicate the k^{th} transform of a sequence of n bits and note that for the trivial case of $n = 1$

$$E[\hat{x}_0^s(1)] = 1. \tag{4.6}$$

One can then show that

Recursion Relation 1.

$$E\left[(\hat{x}_0(2n))^{2r}\right] = \sum_{s=0}^{r} \binom{2r}{2s} E\left[(\hat{x}_0(n))^{2(r-s)}\right] E\left[(\hat{x}_0(n))^{2s}\right] \tag{4.7}$$

Recursion Relation 2.

$$E\left[(\hat{x}_0(2n)\hat{x}_1(2n))^{2r}\right] = \sum_{s=0}^{2r} \binom{2r}{s}(-1)^s E\left[(\hat{x}_0(n))^{4r-2s}\right] E\left[(\hat{x}_0(n))^{2s}\right] \tag{4.8}$$

These two relations can be proved by representing $\hat{x}_0(2n) = \hat{y}_0(n) + \hat{z}_0(n)$ where $\hat{y}_0(n) = \sum_{s=0}^{n-1} x_s$ and $\hat{z}_0(n) = \sum_{s=n}^{2n-1} x_s$, and then using the binomial expansion prior to taking their expections. To derive recursion relation 2, a similar device is used to re-express $\hat{x}_1(2n)$ as the sum of two statistically independent terms.

We list the explicit solution to the first recursion relation for two terms:

$$E[\hat{x}_0(n)^2] = n, \quad \text{and} \quad E[\hat{x}_0(n)^4] = n + 3n(n-1).$$

5. Statistical Results

In this section we report the results obtained from a series of statistical tests which we performed on binary test strings of length 2^{13} bits. Both the DES, and short-round versions of the DES, run in output-feedback mode, were used to generate our test strings.

By thus varying the number of rounds from 1 to 16, it was thought possible to gradually vary the degree of randomness of the resulting strings. For each of these 16 gradations we generated an *ensemble* of 10 test strings.

Plaintext consisting of all zeroes was used to initiate generation of all the test strings. The same 10 keys were used for each ensemble. These keys were generated by using the DES, in output-feedbak mode, with a seed of all zeroes, and the key $FFFFFF00FF000000_{16}$. The k^{th} output block of ciphertext was subsequently used as the key for generating the k^{th} test string of each ensemble.

Three tests measuring nonrandomness were performed on the test strings. If any of these tests indicated the nonrandomness of a test string at the 5% level, then the test string was flagged and the characterizing parameters for all three tests were printed.

The first test measured uniformity of distribution with respect to bit values. Each test string was partitioned into 2^{11} ordered sets — each set consisting of four bits. To measure uniformity of distribution, the chi-square statistic was computed with respect to the 16 possible realizations of four bits. When the chi-square value is greater than 24.996 (for 15 degrees of freedom) the string distribution is significantly nonrandom at the 5% level.

The second, and third tests were our tests for evaluating the second, and third moments ($r = 4$ and $r = 6$). If the characterizing parameter, for either of these tests, is greater than 1.960, then the input string is significantly nonrandom with respect to that test, at the 5% level.

Our results are presented in Table 1 below.

For the one round truncation of the DES, a seed of all zeroes was used to generate the strings. As a consequence, its output is limited to a repetition of two 64 bit blocks. The first block necessarily contains zeroes in its 32 odd positions, and a mixture of zeroes and ones in its even positions. The second block, also by necessity, contains 64 zeroes. All the pairs of blocks which follow, are a repetition of the first two blocks. Thus, one expects the characterizing parameters for each nonrandom test to reach near maximum values. Table 1 satisfies this expectation for all of the test strings in this ensemble.

Every output block generated by the two-round version of the DES is uniquely encrypted. Yet, all but three of the ten test strings generated, were flagged at the 5% level of significance, with one string rejected as random by both of the spectral tests, but not by the chi-square test. However, the majority of test strings was found to be nonrandom at a level approaching certainty.

For the three-round version of the DES, all ten strings were flagged at the 5% level of significance by both of the spectral tests. For nine of the test strings, the random hypothesis was rejected at a level approaching certainty. Six of the strings were rejected at the 5% level by the chi-square (two of these were at a level approaching certainty).

Using four or more rounds, the number of strings flagged as nonrandom, at the 5% level, were within a range acceptable for random strings. However, the five round version generated a single test string which was found to be nonrandom by all three tests, at a

Table 1

String label	χ^2	$r = 4$	$r = 6$
1 Round			
1	7872.000	0.289E+05	0.560E+07
2	6720.000	0.196E+05	0.245E+07
3	6720.000	0.237E+05	0.380E+07
4	6720.000	0.199E+05	0.246E+07
5	7744.000	0.203E+05	0.261E+07
6	6784.000	0.202E+05	0.260E+07
7	6336.000	0.208E+05	0.278E+07
8	8256.000	0.251E+05	0.430E+07
9	6720.000	0.206E+05	0.278E+07
10	6976.000	0.199E+05	0.249E+07
2 Rounds			
2	143.906	144.	640.
4	688.000	1080.	7150.
6	116.984	139.	553.
7	45.078	67.3	243.
8	185.406	202.	894.
9	99.453	55.2	151.
10	12.891	12.7	21.7
3 Rounds			
1	30.406	18.3	33.9
2	28.047	23.7	66.3
3	19.609	12.8	24.8
4	25.047	32.7	77.7
5	25.187	46.3	116.
6	21.297	14.1	23.7
7	21.281	13.1	23.7
8	15.672	3.49	2.94
9	100.172	125.	527.
10	49.687	22.6	44.1
4 Rounds			
8	25.844	0.472	0.731
5 Rounds			
1	12.687	3.31	2.56
3	34.094	0.426	0.586
9	44.109	9.21	17.6
6 Rounds			
1	10.594	2.43	1.72
7 Rounds			
5	33.656	12.2	23.6
7	9.812	2.33	1.56
8 Rounds			
4	25.812	1.16	1.22
7	13.437	1.45	2.02

Table 1 (cont.)

String label	χ^2	$r = 4$	$r = 6$
9 Rounds		{ None flagged at 5% level}	
10 Rounds			
4	10.250	−2.18	−2.13
Rounds 11,12,13		{None flagged at 5% level}	
14 Rounds			
4	13.922	−2.17	−2.08
15 Rounds			
2	19.953	−2.46	−1.62
4	27.641	0.2537	−0.114
7	7.047	1.76	2.20
10	26.875	0.999	0.823
DES (16 Rounds)		{None flagged at 5% level}	

level approaching certainty. One test string generated by the seven-round version was found to be nonrandom by both the spectral tests at a level approaching certainty, while the chi-square test accepted this string as random at less than the 0.5% level. Thus, probabilistic considerations force one to conclude that the ensembles generated by the five and the seven round versions of the DES are not random. Ensembles generated by eight or more rounds, were found to have good statistical properties.

Our spectral test for $r = 4$ appears to be a good complement to the chi-square test. Looking at test strings generated by four or more rounds of the DES, one observes little overlap between the chi-square test and the spectral tests. Of the fifteen strings flagged at the 5% level, five were flagged by the chi-square test alone; and six which were not flagged by this test, were flagged by the $r = 4$, spectral test. The overlap between the two spectral tests — though not total — was high.

We note that when we previously used our spectral test based on the FFT [3] to test the DES round by round we used the same set of keys to generate our test ensembles. Our test strings, however, were of length 2^{15} bits. (This is the length originally chosen by Gait in his test [1].) When we compare the output of these tests with our new results, they are essentially the same string for string except that for the longer test strings, the significance level of the rejected strings is generally much higher. This indicates that tests based on the FWT, and the FFT, give similar results; and also that the "bad" strings are key dependent, since they remain nonrandom when the length of the test string is increased by a factor of four.

References

[1] J. Gait, "A New Nonlinear Pseudorandom Number Generator," IEEE Trans. on Software Eng., Vol. SE–3(5) pp. 359–363 (Sept. 1977)

[2] C. Yuen, "Testing Random Number Generators by Walsh Transform," IEEE Trans. on Computers, Vol. C–26(4) pp. 329–333 (April 1977)

[3] F. A. Feldman, "A New Spectral Test for Nonrandomness and the DES," submitted to IEEE Trans. on Software Engineering (July 1986)

[4] F. A. Feldman, "A New Spectral Measure of Nonrandomness," Suffolk University Technichal Report No. 5, (1987)

[5] A. V. Oppenheim and R. W. Schafer, *Digital Signal Processing.* Prentice-Hall, Inc., Englewood Cliffs. New Jersey, 1975.

[6] A. Aho, J. Hopcroft, J. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley Publishiing Company, Reading, Mass. 1974.

[7] A. Kolmogorov, "Three Approaches to the Quantitative Definition of Information," PROB. INFO. TRANSMISSION, Vol. 1, No. 1, Jan. 1965, 1–7.

[8] G. Chaitan, "On the Length of Programs for Computing Finite Binary Sequences," JACM (13), 1966, 547–569.

[9] D. Knuth, *The Art of Computer Programming; Vol. 2, Seminumerical Algorithms*, Addison-Wesley, Reading, Mass. 1969.

[10] "Data Encryption Standard," FIPS PUB 46, National Bureau of Standards, Washington, D.C., Jan. 1977.

[11] H. Katzan, *The Standard Data Encryption Algorithm*, Petrocelli Books, Inc., New York, 1977.

[12] K. G. Beauchamp, *Applications of Walsh and Related Functions*, Academic Press, 1984.