UNIVERSITI TEKNIKAL MALAYSIA MELAKA

AN ENHANCEMENT OF THE SPECTRAL STATISTICAL TEST FOR RANDOMNESS

NUR AZMAN ABU
NANNA SURYANA
SHAHRIN SAHIB

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

AN ENHANCEMENT OF THE SPECTRAL STATISTICAL TEST FOR RANDOMNESS

NUR AZMAN ABU
NANNA SURYANA
SHAHRIN SA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

An Enhancement of the Spectral Statistical Test for Randomness

Nur Azman Abu, Nanna Suryana Herman and Shahrin Sahib
Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka (UTeM),
Durian Tunggal, 76109 Melaka, Malaysia
{nura, nsuryana, shahrinsahib}@utem.edu.my

Abstract—**Random numbers play essential roles in cryptography, modeling and simulation applications. NIST statistical test suite for randomness is the most comprehensive set of random tests. It has been popular and used as a benchmark test for randomness. One of the random tests is spectral test. There has been serious problem in spectral test as pointed out by few researchers. In this paper, further theoretical improvement shall be proposed on the spectral test based on computational observation being made on random noise. A recommendation on the spectral test setting for short cryptographic keys shall also be made.**

Keywords-random test; spectral test; random ambience;

I. INTRODUCTION

Random and pseudorandom number generators are used in many applications especially cryptography. They are utilised in the construction of encryption keys, private keys, session keys, master keys and every other cryptographic parameters.

True random numbers are believed to be generated only using hardware random number generators. Careful statistical analysis is still required to have any confidence in the process and apparatus which generates numbers that are sufficiently 'random' to suit the cryptographic use. This is where statistical test for randomness comes into picture.

NIST statistical test suite for randomness[1] is the most comprehensive set of random tests. It has been popular and used as a benchmark test for randomness. Statistical test suite for randomness is also being used as a tool to evaluate the output of symmetric encryption algorithm such as AES[2]. Ideally, the ciphertext should not provide any clues to distinguish them statistically from truly random source.

Spectral test is one of the set of random NIST test suite. As recommended in [1], it is only suitable test for long binary sequence. At the same time, the first author find it so difficult to produce a sample input that gives fail result on spectral test for short practical cryptographic keys.

This paper has been written to overcome such problem and propose a more accurate spectral test. Section 2 will briefly go through the theoretical setting of hypothesis test. Section 3 will touch on NIST test suite for long and short binary sequences. Section 4 will explain about spectral test for randomness. Section 5 will touch on the correction on spectral test made by Song-Ju Kim et al. Section 6 will give a counter example for short binary sequence which the original spectral test give a unintended result. Section 7 will give further analysis on the distribution of random variable used in spectral test. A suggestion on clear optional spectral test is given in Section 8. Section 9 details on the recommendation by the authors. Section 10 discuss on the consistent result of the enhanced spectral test before further concluded in Section 11.

II. A STATISTICAL HYPOTHESIS TEST

A statistical test is formulated to test a specific null hypothesis H_0. For the purpose of this study, the null hypothesis under test is that the binary sequence ε being tested is random against the alternative hypothesis H_1 for which the binary sequence ε is not random.

For each statistical test, a set of $P-$values (corresponding to the set of sequences) is produced. For a fixed significance level α, a certain percentage of $P-$values are expected to indicate failure. For example, if the significance level is chosen to be 0.01, then about 1% of the sequences are expected to fail. A sequence passes a statistical test whenever the $P-$value $\geq \alpha$ and fails otherwise. The parameter α denotes the significance level that determines the critical region of acceptance and rejection. Even though NIST recommends that α be in the range [0.001, 0.01],

III. NIST STATISTICAL TEST SUITE

The NIST statistical test suite is a statistical package consisting of 16 tests that were developed to test the randomness of arbitrary long and short binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators.

The 16 tests are decomposable into 2 groups based on its suitability for short or long binary sequence. Only 8 tests are particularly suitable for practical cryptographic keys size here. The selected NIST Test for short practical cryptographic key sizes are listed in the Table I below.

TABLE I THE LIST OF SUITABLE RANDOM TESTS FOR SHORT KEYS.

0	Statistical Test	Min key size n
1	Frequency Monobit	128 bits
2	Block Frequency (M = 8)	128 bits
3	Consecutive Runs	128 bits
4a	Cumulative Sums (Forward)	128 bits

978-1-4244-7578-0/$26.00 © 2010 IEEE

4b	Cumulative Sums (Backward)	128 bits
5	Longest Runs of Ones ($M = 8$)	128 bits
6	Spectral DFT	1024 bits
7	Approximate Entropy ($m = 7$)	128 bits
8a	Serial ($m = 7$) $P-$value1	128 bits
8b	Serial ($m = 7$) $P-$value2	128 bits

The first author is interested in using the random test for short cryptographic keys. Since the practical cryptographic keys are 128, 256, 1024-bit keys and so on, closer attention has been made on the spectral test. A recommendation in the NIST statistical test suite is only for 1024-bit and above for spectral test. A more accurate analysis on spectral test is required.

IV. Spectral Test

The focus of this test is the peak heights in the Discrete Fourier Transform(DFT) of the sequence. The purpose of this test is to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness. The intention is to detect whether the number of peaks exceeding the 95% threshold is significantly different than 5% based on binomial distribution.

The test described here is based on the discrete Fourier transform. It is a member of a class of procedures known as spectral methods. The Fourier test detects periodic features in the bit series that would indicate a deviation from the assumption of randomness.

Let $\boldsymbol{\varepsilon} = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ the binary random variables be identically independently distributed(iid). Then let $x_k = 2\varepsilon_k - 1 = \begin{cases} +1 \\ -1 \end{cases}$ be the k^{th} bit, where $k = 1, ..., n$. The coefficient of Fast Fourier Transform[3] shall be computed as

$$y_j = \sum_{k=1}^{n} x_k \cdot \exp\left\{\frac{2\pi i(k-1)}{n} j\right\} \quad \ldots\ldots (1)$$

where $j = 0, \ldots, n-1$, and $i = \sqrt{-1}$. Because of the symmetry of the real to complex-value transform, only the values from 0 to $(\frac{n}{2} - 1)$ are considered.

Let $|y_j|$ be the modulus of the complex number y_j. Under the assumption of the randomness of the series x_k, a confidence interval can be placed on the values of $|y_j|$. More specifically, 95 percent of the values of $|y_j|$ should be less than $h = \sqrt{2.995732274\, n}$ as corrected by Song-Ju Kim et al. in [4] instead of $h = \sqrt{3n}$ in the original NIST document[1].

V. Derivation of the Threshold in Spectral Test

Let us go through the derivation of the threshold $h = \sqrt{2.995732274n}$ according to Song-Ju Kim et al. in [4]. For a frequency j, DFT are defined by following equation.

$$\begin{aligned} y_j &= \sum_{k=1}^{n} x_k \cdot \exp\left\{\frac{2\pi i(k-1)}{n} j\right\} \\ &= \sum_{k=1}^{n} x_k \cdot \cos\left[\frac{2\pi j(k-1)}{n}\right] \\ &\quad + i\sum_{k=1}^{n} x_k \cdot \sin\left[\frac{2\pi j(k-1)}{n}\right] \quad \ldots\ldots (2) \end{aligned}$$

Let us consider the square of modulus of (2),

$$|y_j|^2 = c_j^2 + s_j^2 \quad \ldots\ldots (3)$$

where

$$c_j = \cos\left[\frac{2\pi j(k-1)}{n}\right] \text{ and } s_j = \sin\left[\frac{2\pi j(k-1)}{n}\right] \quad \ldots\ldots (4)$$

Assuming $x_k = 2\varepsilon_k - 1 = \begin{cases} +1 \\ -1 \end{cases}$ are random for $k = 1, 2, \ldots, n$, then c_j and s_j converge to the normal distribution with mean μ is zero and variance σ^2 is $n/2$.

Therefore,

$$Y = \left(\frac{c_j}{\sigma}\right)^2 + \left(\frac{s_j}{\sigma}\right)^2 \quad \ldots\ldots (5)$$

converges to χ^2 distribution with 2 degree of freedom with pdf

$$f_Y(y) = \frac{1}{2} e^{-\frac{y}{2}} \quad \ldots\ldots (6)$$

Let Z = Y/2, then Z shall have following distribution pdf,

$$f_Z(z) = e^{-z},\ Z > 0 \quad \ldots\ldots (7)$$

The threshold h is defined such that the number of peaks exceeding the threshold h should be 5% under the assumption of randomness. Let

$$\begin{aligned} \int_{z_0}^{+\infty} f_Z(z)dz &= \int_{z_0}^{+\infty} e^{-z} dz \\ &= -e^{-z}\Big|_{z_0}^{+\infty} = e^{-z_0} = 0.05 \quad \ldots\ldots (8) \end{aligned}$$

Then $z_0 = -\ln(0.05) = 2.995732274$.

From $|y_j| = \sqrt{nZ}$, it can be concluded that

$$h = \sqrt{2.995732274\, n} \quad \ldots\ldots (9)$$

A $P-value$ based on this threshold comes from the binomial distribution. Let N_1 be the number of peaks less than h. Only the first $n/2$ peaks are considered.

$$P-value = 2[1 - \phi(|d|)] \quad \ldots\ldots (10)$$

where $\phi(x)$ is the cumulative distribution function (cdf) of the standard normal distribution.

Let the significant level $\alpha = 0.01$. If the computed $P-value$ is < 0.01, then conclude that the sequence is non-

random. Otherwise, conclude that the sequence is random. A d value that is too low would indicate that there were too few peaks (< 95%) below T, and too many peaks (more than 5%) above T.

VI. Counter Example on Spectral Test

This spectral test is not suitable for short cryptographic keys of size 128 and 256-bit. It has been observed that spectral test may easily give a wrong result for short linear binary sequence. Here is a counter example for n = 128. It follows the step-by-step procedure.

i). Let $\boldsymbol{\varepsilon} = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ the binary sequence to be tested for randomness. Take $\boldsymbol{\varepsilon}$ = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F written in hexadecimals.

ii). Convert the input sequence $\boldsymbol{\varepsilon}$ to values of –1 and +1. Let the sequence $X = x_1, x_2, \ldots,$ xn, where $x_i = 2\varepsilon_i - 1$.

iii). Apply a Discrete Fourier transform (DFT) on X to produce: $S = DFT(X)$. A sequence of complex variables is produced which represents periodic components of the sequence of bits at different frequencies.

iv). Calculate $M = modulus(S') \equiv |S'|$, where S' is the substring consisting of the first $n/2$ elements in S.

v). Let $p = P(M < T)$, under the assumption that $p = 0.95$ then set the hypothesis testing as

$$H_0 : \mu = N_0 \text{ versus } H_1 : \mu \neq N_0$$

and compute the 95% peak height threshold value, $T = \sqrt{2.995732274n} = 19.5820$. Under the assumption of randomness, 95% of the values obtained from the test should not exceed T.

vii). Count N_1 as the actual observed percentage of number of coefficients in M that are less than L. $N_1 = 62$.

viii). Compute $N_0 = 0.95n/2 = 60.8$ where N_0 is the expected theoretical (5%) number peaks (under the assumption of randomness) that are larger than T.

$$d_1 = \frac{N_1 - N_0}{\sqrt{n \cdot (0.95)(0.05)/2}} = 0.6882.$$

ix) Compute P–value according to (10) shall give P–value = 0.4913 > 0.01 which concludes that the byte counter sequence is still random.

The counter example above has been extended for n = 256. Let Take $\boldsymbol{\varepsilon}$= 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F written in hexadecimals. The comparable result can be seen in Table 2 below. The results below show that this spectral test gives wrong conclusion with P–value > 0.01 for n = 128 and 512.

TABLE 2. THE UPPER RIGHT 0.05 TAIL PASSING RESULT ON RANDOMNESS FOR SHORT N-BIT BYTE COUNTER SEQUENCE

n	T	N_0	N_1	d_1	P–value
128	19.5820	60.8	62	0.6882	0.4193
256	27.6931	121.6	121	-0.2433	0.8077
512	39.1639	243.2	208	-10.0943	5.8552e-024
1024	55.3862	486.4	456	-0.0062	7.0745e-010

VII. Analysis on Spectral Test

Experimental result on random ambience noise starts from (4). Let $Y = C^2 + S^2$. Statistical distributions of random variables C and S has been investigated for n = 128, 256 and 1024-bit. They are consistently normally distributed with mean μ is zero and variance σ^2 is $n/2$.

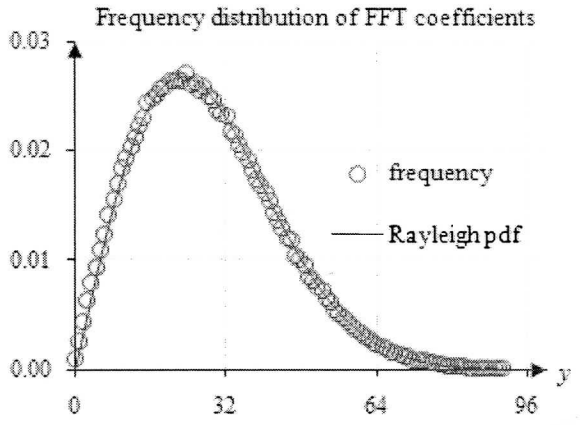

Figure 1. The magnitue of DFT coefficents follows Rayleigh distribution

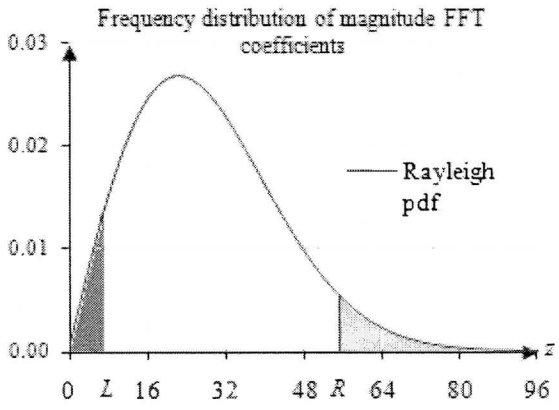

Figure 2. The lower and upper tails of Rayleigh distribution for n = 1024.

However, the random variable of interest is $Z = \sqrt{C^2 + S^2}$. Statistical distributions of random variables Z has been investigated for n = 128, 256 and 1024-bit. Theoretically, $\sigma^2 Y$ follows the χ^2 distribution with 2 degree of freedom. Whereas the random variable $Z = \sqrt{C^2 + S^2}$ itself follows the Rayleigh distribution as shown in Fig. 1

above. In Fig. 2, the distribution of the first $n/2$ of DFT coefficents follow Rayleigh distribution with pdf,

$$f_Z(z) = \frac{2z}{n} e^{-\frac{z^2}{n}}, z > 0 \quad \text{..... (11)}$$

Theoretically, this random variable has been pointed out in[5]. Moreover, in communications theory, if the component velocities of a particle in the x and y directions are two independent normal random variables with zero means and equal variances, then the distance the particle travels per unit time follows Rayleigh distribution.

VIII. Recommendation on Spectral Test

Since it is well known that the first $n/2$ of DFT coefficents follows Rayleigh distribution, the authors propose that the Spectral Test be divided into 2 subtests consists of left and right α-tails on both side as shown in Fig. 2 above.

First, let

$$P(Z < L) = \int_0^L f_Z(z)dz = \int_0^L \frac{2z}{n} e^{-\frac{z^2}{n}} dz = -e^{-\frac{z^2}{n}}\Big|_0^L$$

$$= 1 - e^{-\frac{L^2}{n}} = 0.05 \quad \text{..... (12)}$$

Then, $L = \sqrt{n(-\ln 0.95)} = 0.226480229573247\sqrt{n}$.

Second, let

$$P(Z > R) = \int_R^{+\infty} f_Z(z)dz = \int_R^{+\infty} \frac{2z}{n} e^{-\frac{z^2}{n}} dz$$

$$= -e^{-\frac{z^2}{n}}\Big|_R^{+\infty} = e^{-\frac{R^2}{2}} = 0.05 \quad \text{..... (13)}$$

Then, $R = \sqrt{n(-\ln 0.05)} = 1.73081838260229\sqrt{n}$.

The lower and upper 0.05 tails are displayed in Table 3 below.

TABLE 3. THE LOWER AND UPPER 0.05 TAILS FOR RESPECTIVE N-BIT CRYPTOGRAPHIC KEY

n	L	R
128	2.562331298175	19.581974645447
256	3.623683673172	27.693094121637
1024	7.247367346344	55.386188243273
2048	10.249325192699	78.327898581786

IX. Spectral Test Procedure

This spectral test is suitable for short cryptographic keys of size 128, 256, 1024-bit and so on. The step by step procedure is as follows;

i). Let $\boldsymbol{\varepsilon} = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ the binary sequence to be tested for randomness.

ii). Convert the input sequence $\boldsymbol{\varepsilon}$ to values of –1 and +1 to create the sequence $X = x_1, x_2, \ldots, x_n$, where $x_i = 2\varepsilon_i - 1$.

iii). Apply a Discrete Fourier transform (DFT) on X to produce: $S = DFT(X)$. A sequence of complex variables is produced which represents periodic components of the sequence of bits at different frequencies.

iv). Calculate $M = modulus(S') \equiv |S'|$, where S' is the substring consisting of the first $n/2$ elements in S, and the modulus function produces a sequence of peak heights.

v). Let $p_1 = P(M < L)$ and $p_2 = P(M > R)$ then set the hypothesis testing as

$H_0 : p_1 = 0.05$ versus $H_1 : p_1 \neq 0.05$

and $H_0 : p_2 = 0.05$ versus $H_2 : p_2 \neq 0.05$,

or equivalently let a random variable y follows Bernoulli distribution with probability p, then $\sum_{i=1}^{n} y_i$ shall follow Binomial distribution with mean $\mu = np$ and variance $\sigma^2 = np(1-p)$. Thus

$H_0 : \mu_1 = N_0$ versus $H_1 : \mu_1 \neq N_0$

and $H_0 : \mu_2 = N_0$ versus $H_2 : \mu_2 \neq N_0$

vi). Set the significant level $\alpha = 0.01$. Compute

$L = \sqrt{n(-\ln 0.95)} = 0.2264802296\sqrt{n}$ and

$R = \sqrt{n(-\ln 0.05)} = 1.7308183826\sqrt{n}$.

vii). Count N1 = the actual observed percentage of number of coefficients in M that are less than L and N2 = the actual observed percentage of number of coefficients in M that are larger than R.

viii). Compute $N_0 = 0.05n/2$. N_0 is the expected theoretical (5%) number of lows and peaks (under the assumption of randomness) that are less than L and of larger than R respectively.

$$d_1 = \frac{N_1 - N_0}{\sqrt{n \cdot (0.95)(0.05)/2}} \text{ and } d_2 = \frac{N_2 - N_0}{\sqrt{n \cdot (0.95)(0.05)/2}}$$

ix) Compute

$P-\text{value1} = 2[1 - \phi(|d_1|)]$ and

$P-\text{value2} = 2[1 - \phi(|d_2|)]$.

x). The null hypothesis shall be rejected if any one of the two $P-$values < 0.01.

X. Discussion

While the upper right-hand-side 0.05 tail is similar to the original test, the lower left-hand-side 0.05 tail makes full use of the Rayleigh distribution of the DFT coefficients. The result in Table 4 below shows that this test consistently give failing result on randomness for short n-bit byte counter sequence for as short as 128-bit numbers.

TABLE 4. THE LOWER LEFT 0.05 TAIL GIVES CONSISTENTLY FAILING RESULT ON RANDOMNESS FOR SHORT N-BIT BYTE COUNTER SEQUENCE.

n	L	N_0	N_1	d_1	$P-$value

128	2.5623	3.20	17	7.9148	2.4756e-015
256	3.6237	6.40	40	13.6266	2.7825e-042
512	5.1247	12.80	120	30.7417	1.5783e-207
1024	7.2474	25.60	288	53.2086	0

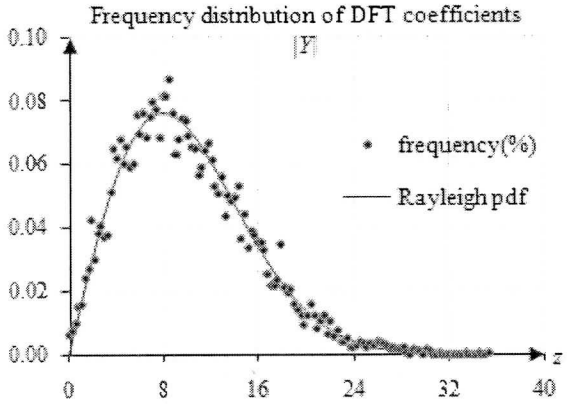

Figure 3. An experimental result on the frequency distribution of norm of DFT coefficients.

An experiment on 128 sets of 128-bit random ambience noise[6] has been conducted. The result in Fig. 3 shows that even short binary sequence give correct statistical result. The random variable on the spectral test, namely, the norm of DFT coefficients from random noise consistently approaches Rayleigh distribution.

XI. Conclusion

In this paper, clear statistical distribution of DFT coefficients has been explored. It is an important distribution for one of NIST random test suite, namely, spectral test. A recommendation on the spectral random test setting for short practical cryptographic keys has also been made. It has been observed based on computational experience being made on random noise. The DFT coefficients follow Rayleigh distribution. This paper proposed a more accurate spectral test based on the lower tail of the distribution. This test consistently gives failing result on randomness for short *n*-bit byte counter sequence for as short as 128-bit numbers.

References

[1] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo, A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications, NIST Special Publication 800-22, May 15, 2001.

[2] J. Soto and L. Bassham: Randomness Testing of the Advanced Encryption Standard Finalist Candidates, NIST (2000). http://csrc.nist.gov/aes/

[3] R. N. Bracewell, The Fourier Transform and Its Applications, McGraw-Hill, 1986.

[4] Song-Ju Kim, Ken Umeno, and Akio Hasegawa, Corrections of the NIST Statistical Test Suite for Randomness, 2004 http://eprint.iacr.org/2004/018.pdf,

[5] Athanasios Papoulis, Probability, Random Variable and Stochastic Processes, 3rd Edition, McGraw-Hill, 1991, p. 96.

[6] Nur Azman Abu and Zulkiflee Muslim, Random Room Noise for Cryptographic Key, Proceedings 2nd IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2008), Phitsanulok, Thailand, 27-29 February 2008, pp. 381-387.