A note on the QFT randomness spectral test a new approach of DST

Emil SIMION\textsuperscript{1,2), Elena Corina CIPU\textsuperscript{2,3)}, Vasile – Laurențiu DOSAN\textsuperscript{4)}, Andrei-Voicu TOMUȚ\textsuperscript{5)}

1) Department of Mathematical Models and Methods, University POLITEHNICA of Bucharest,
2) Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering “Traian Lalescu”, University POLITEHNICA of Bucharest,
3) Department of Applied Mathematics, University POLITEHNICA of Bucharest,
4) Faculty of Applied Sciences, University POLITEHNICA of Bucharest

Abstract.

Quantum computers provide a new way of solving problems even in cryptography in which digital signature make an important role. In this paper, we describe a comparison between the spectral test in classical mode and quantum mode through Fourier Transform. A comparison of the results in the two cases was made. Applications of the proposed techniques are from the field of statistical testing of the pseudorandom bit generators used for cryptographic applications. The proposed statistical test is an extension of the Discrete Fourier Transform statistical test proposed in NIST SP 800-22.

Key words: quantum Fourier transform, quantum computation, spectral test

1. Introduction

Random numbers are an essential resource in science and engineering with important applications, especially in cryptography, scientific simulations, gambling and lotteries. There are two types of random number generators: (i) pseudo-random number generators (PRNGs), based on mathematical algorithms which approximate the behavior of randomness and (ii) true random number generators (TRNGs), which use the behavior of a physical process. [5]

The binary "truly" random sequence is defined as the sequence in which each element has a probability of exactly 50\% of being "0" or "1" and in which the elements are statistically independent of each other. It is also difficult to ascertain if the sequence is truly random; therefore, the randomness of the sequences is evaluated statistically. [6]

The customary approach to randomness testing is using a series of statistical tests. The main suites available to perform these statistical tests are the NIST, TestU01, DieHard and DieHarder suites. Most tests apply statistical analyses similar to the standard chi-squared test. The result is a p-value that indicates how likely it is for a purely random number generator to produce the tested sequence. Each test suite has different threshold values to determine if a given p-value is compatible with randomness or not. NIST SP 800-22 consists of fifteen tests, and every test is hypothesis testing, where the hypothesis is that the input sequence is truly random; if the hypothesis is not rejected in all the tests, it is implied that the input sequences are random. Among the tests included in NIST SP 800-22, the DFT test is of the greatest concern to us. This test detects
periodic features of a random number sequence; input sequences are discrete Fourier transformed, and the test statistic is composed of the Fourier coefficients. [7]

Spectral is a statistical test. A statistical test is formulated to test a specific null hypothesis (H0). For the purpose of this document, the null hypothesis under test is that the sequence being tested is random. Associated with this null hypothesis is the alternative hypothesis (Ha), which, for this document, is that the sequence is not random. [8]

In this work, we studied the consequences of replacing the classical (discrete) Fourier transform with the Quantum Fourier Transform (QFT) in the Spectral test. Quantum Fourier Transform is a linear transformation on qubits and is the quantum analogue of the inverse Discrete Fourier Transform (DFT). We define DFT of a signal x, the vector y with the following components:

\[ y_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i k n}{N}}, k = 0, \ldots, N-1 \]

Using notation \( \omega = e^{-\frac{2\pi i}{N}} \), equation becomes:

\[ y_k = \sum_{n=0}^{N-1} x_n \omega^{kn}, k = 0, \ldots, N-1 \]

with \( |\omega| = 1 \). We introduce the matrix W,

\[
W = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\
1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)}
\end{bmatrix}
\]

W is a symmetric matrix, and we can compute the product

\[ W \cdot W = \overline{W} \cdot W = N \cdot I_N \]

The discrete Fourier transform can be written as follows:

\[ Y = WX. \]

As we can see in the book by Nielsen and Chuang (2010) and in the book by Nakahara and Ohmi (2008), the Quantum Fourier Transform (QFT) is based on essentially the same idea with the difference that the vectors x and y are state vectors, \( |x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \), \( |y\rangle = \sum_{j=0}^{N-1} y_j |j\rangle \), where \( |j\rangle \) is a basis vector in the \( \mathcal{H}_N \) Hilbert space of dimension \( N = 2^n \) with the inner product \( \langle \cdot | \cdot \rangle \)

\[ \langle \phi | \psi \rangle = [\phi_1, \phi_2, \ldots, \phi_n] \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{bmatrix} = \sum_{k=1}^{n} \phi_k \psi_k \]
in which \( \langle \psi | = | \psi \rangle^\dagger \) is the Hermitian conjugation of a ket vector and \( | i \rangle \langle j | = I_N \). In other words, QFT is a linear operator whose action on any of the computational basis vectors \( |0\rangle, |1\rangle, \ldots, |2^n - 1\rangle \) associated with an n-qubit register is described by the transformation:

\[
|j\rangle \mapsto W|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j}{2^n}} |k\rangle, 0 \leq j \leq 2^n - 1
\]

We observe that \( W \) for \( N = 2 \) is the Hadamard gate (H). Hadamard gates are used for preparing states. It creates an input state with constant amplitudes. Other gates used for describing QFT algorithm are \( R_k \) phase gate and SWAP gate. Phase gate leaves the basis state \( |0\rangle \) unchanged and map \( |1\rangle \) to \( e^{2\pi i/2^k} |1\rangle \). The SWAP gate swaps two qubits:

\[
SWAP = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

To encode a bit string with length \( n \) in the qubit statevector we need \( m = \log_2 n \) qubits. To realize QFT, \( \frac{m(m+1)}{2} \) operations are made. It means that the complexity of the algorithm becomes \( O((\log_2 n)^2) \equiv O(m^2) \) which leads to the conclusion that QFT algorithm is more efficient than the classical Fast Fourier Transform (FFT), for FFT we have \( O(n \cdot \log_2 n) \).

Assuming that we use only native quantum gates, and all the m qubits are interconnected, to realize QFT it is necessary a QPU having the Quantum Volume bigger than \( m(m - 1) = m^2 - \)
Unfortunately, this is an unusual situation on superconducting processors. Consequently, a few SWAP gates must be added, and the Quantum Volume will increase.

**Remark:** The states of a system can be pure or mixed. Pure states are of two types:

- **Product or separable states** - if it can be described as a tensor product of two subsystems: 
  \[ |\psi\rangle = |\varphi\rangle \otimes |\theta\rangle \]  
  in case \(|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2, |\varphi\rangle \in \mathcal{H}_1, |\theta\rangle \in \mathcal{H}_2\]

  Such a state describes a situation like a classical one meaning that the state of the system expresses exactly the information contained in the states of the subsystem. A change in status caused by a measurement made on one subsystem has no effect on the state of the other subsystem. This means that the measurement results on different subsystems are uncorrelated (or independent).

- **Bipartite states**, indestructible states, or (mixed) **entangled** states. These are correlated states that cannot be written as a product of subsystem states. In this case, a local measurement reduces the state of the whole and changes the probabilities for potential future measurements on any subsystem. For mixed states the product and separable states are not synonymous.

Another method of representing a quantum system is to use the notion of density matrix \([1,3]\). This form is especially useful in situations where complete information about that system is not known. For a system in the states \(|\psi_i\rangle\) with the associated probabilities \(p_i, i = 1 \ldots n\), we can associate the density matrix:

\[
\rho = \sum_{i=1}^{n} p_i \cdot |\psi_i\rangle \langle \psi_i |
\]

With the help of these density matrices, we can characterize quantum states. Thus, we have:

(i) **separable states** when \(\rho^2 = \rho\) and \(Tr(\rho^2) = 1\). Pure states occupy points located on the surface of the Bloch sphere.

(ii) **entangled** states when \(\rho^2 \neq \rho\) and \(Tr(\rho^2) < 1\). Mixed states are combinations of pure states, occupying points inside the Bloch sphere. The completely mixed state for a system of \(n\) qubits is described by the density matrix \(\rho = \frac{1}{2^n} I_n\), located right at the origin of the Bloch sphere. The density matrix also proves to be useful in calculating the average values of certain operators \([4]\). The average value of the operator \(\hat{A}\) computed on state \(\rho\) is:

\[
<\hat{A}> = Tr(\rho \hat{A})
\]

A density matrix \(\rho \in \mathcal{B}(\mathcal{H})\) is a Hermitian matrix \(n \times n\), \((\rho = \rho^\dagger)\) with \(Tr(\rho) = 1\) and positively defined \( |\psi\rangle \rho \langle \psi | \geq 0, \forall \psi \in \mathcal{H} \). Let be \(\mathcal{B}(\mathcal{H})\) the set of bounded operators defined in \(\mathcal{H}\).

**Examples**

The simplest quantum state for \(N=2\) can be written \(|\phi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i \varphi} \sin \frac{\theta}{2} |1\rangle\).

If \(A\) represents the preparation for polarization of a photon both vertically and horizontally:

\[
\frac{1}{2} |0\rangle \langle 0 | + \frac{1}{2} |1\rangle \langle 1 | = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}
\]

The same matrix density is obtained if \(A\) represents the preparation for an equal mixture of left and right polarized photons or any two pure orthogonal states. □
If the qubit state is codified by means of one photon and two optical modes, associating the mode 1 to the horizontal polarization $|H⟩$ and the mode 2 to the vertical one $|V⟩$, then $|ψ⟩ = α|H⟩ + β|V⟩$ and the singlet polarization-entangled state of two photons $A$ and $B$ is expressed by

$$|ψ^−⟩_{AB} = \frac{1}{\sqrt{2}} (|H⟩_A |V⟩_B - |V⟩_A |H⟩_B),$$

that have the property of being rotationally invariant. The density matrix $ρ_{AB}$ for the two particle entangled singlet state is expressed by

$$ρ_{AB} = \begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 1/2 & -1/2 & 0 \\
0 & -1/2 & 1/2 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},$$

in the basis $\{ |H⟩_A |H⟩_B; |H⟩_A |V⟩_B; |V⟩_A |H⟩_B; |V⟩_A |V⟩_B \}$. (see [9]) □

2. Description of QRNG

Random bits sequences for data analyse were collected from a typical quantum random number generator (QRNG). It is based on single-photon measurement. A photon is prepared in a superposition of horizontal (H) and vertical (V) polarizations, described by $|ψ⟩ = \frac{1}{\sqrt{2}} ( |H⟩ + |V⟩ )$. A polarizing beam splitter (PBS) transmits the horizontal and reflects the vertical polarization. For random bit generation, the photon is measured by two avalanche photo-diodes (APD). The path the photon takes at the output is random and there will be a detection with the same probability at each detector. We consider that a click on detector $D_0$ is recorded as a 0 bit and a detection in $D_1$ is a 1. [7]

![Quantum probabilities context](image)

3. Quantum probabilities context

We make use of the theoretical framework of universal measurements where Gleason property (see [9]) and Born rule are considered in the Hilbert space $\mathcal{H}_N$.

Gleason property precise that the transition probability depends only on the state before the measurement and the eigenstate that is actualized after the measurement.

Let’s consider an observable quantity expressed by the self-adjoint operator $A$, described by its eigenvectors $|α_i⟩$, that verify the orthogonality relation and the completeness condition

$$|α_i⟩\langle α_j| = δ_{ij}, \ i, j ∈ \{1, N\}, \ \sum_{i=1}^{N} |α_i⟩\langle α_i| = I_N$$
and the orthogonal projections and \( P_i = |\alpha_i\rangle\langle \alpha_i|, \ i \in \overline{1,N}. \) In our case \(|\alpha_i\rangle = |i\rangle, \ i \in \overline{1,N}. \) Also, for \(|\phi\rangle\) a state in \( \mathcal{H}_N \), we write \( \langle \alpha_i|\phi\rangle = \sqrt{x_i}e^{i\phi_i}, \ i \in \overline{1,N} \) in the polar form, with condition, \( \sum_{i=1}^{N} x_i = 1. \)

**Properties:** The elements of the set \( \{ P_i = |e_i\rangle\langle e_i|, i \in \overline{1,n} \} \) fulfil the conditions:

1. \( P_i^2 = P_i, \forall \ i \in \overline{1,n} \)
2. \( P_iP_j \neq 0, \forall \ i \neq j \)
3. \( \sum_{i=1}^{n} P_i = \mathbb{1} \)
4. \(|\psi\rangle - P_i|\psi\rangle\) is orthogonal to \(|e_i\rangle\)

(see for instance [13]).

The measurement of the observable expressed by \( A \) is a process in which the state \(|\phi\rangle\) pass through one of the states of the eigenvectors \(|\alpha_i\rangle\) and the probability \( P(|\phi\rangle \to |\alpha_i\rangle) \) to be one eigenvector or another is expressed by the Born rule, that is the square norm of the projection corresponding to the eigenvalue \( \alpha_i \)

\[
P(|\phi\rangle \to |\alpha_i\rangle) = \|P_i|\phi\rangle\|^2 = x_i, \ i \in \overline{1,N}.
\]

Now, if the state is degenerate, meaning that some of the \( \alpha_i \) are equal, then \(|\alpha_i\rangle, \ i \in \overline{1,m_k} \) are the eigenvectors whose index belong to the same eigenvalue \( \alpha_{i_k}; \cup_k l_{m_k} = 1_N, \sum_{k=1}^{m} m_k = N, \) then according to the Born rule, the transition probabilities are expressed by

\[
P(|\phi\rangle \to |\phi\rangle_{l_{m_k}}) = \|P_{l_{m_k}}|\phi\rangle\|^2 = \sum_{j \in l_{m_k}} x_j
\]

with

\[
|\phi\rangle_{l_{m_k}} = \sum_{i \in l_{m_k}} \sqrt{\frac{x_i}{\sum_{j \in l_{m_k}} x_j}} e^{i\phi_i}|\alpha_i\rangle
\]

**Definitions:**

1. The **probability** that a certain measurement being the result of a matrix density is defined by

\[
P[\text{outcome} = x|\text{state} = \rho] = \text{Tr}(\rho E_x)
\]

a semi-positive operator connected to \( x \) and \( E_x \) being the **projection operator**.

2. An ordered set of operators semi-positive \( E = \{E_1, E_2, \cdots E_m\} \), for which \( \sum_{x=1}^{m} E_x = \mathbb{1}_m \) express an **POVM** - Positive Operator of Measure Valuation, that could be applied to a quantic system. \( \mathcal{M} = \{E|E\} \) is **POVM**

3. Probability of error \( PE \), between two probabilities densities is defined by

\[
PE(p_0, p_1) = \frac{1}{2} \sum_{x \in X} \min(p_0(x), p_1(x)) \quad \text{or} \quad PE(p_0, p_1) = \inf_{E \in \mathcal{M}} \{p_0(E), p_1(E)\}
\]

4. The Kolmogorov distance between two matrix densities is \( K(p_0, p_1) = \frac{1}{2} \sum_{i=1}^{n} |\lambda_i| \), where \( \lambda_i \) are eigenvalues of the difference \( p_0 - p_1 \).
5. The distance between two states as a result of a measurement, or as an application of a protocol is given by the distance between two matrix densities
\[
D(\rho_0, \rho_1) = \max_{0 \leq M \leq 1} \text{Tr}[M(\rho_0 - \rho_1)] = \frac{1}{2} \text{Tr}(\sigma), \quad \sigma^2 = A^\dagger A, A = \rho_0 - \rho_1
\]
where M describes the measurement or protocol applied.

Remarks:
1. Two identical distributions have \( PE = \frac{1}{2} \). Two orthogonal distributions have \( PE = 0 \).
2. PVM-Projection Valuation Measurement is a particular case of POVM with condition
\[
E_k E_l = \delta_{kl} E_l, \quad E_x \text{ being the projection operator and } \delta(k, l) = \begin{cases} 1, & k = l \\ 0, & k \neq l \end{cases} \text{ Kronecker symbol.}
\]
3. If \( \rho_1 = \langle \psi \rangle \langle \psi \rangle \) and \( \rho_2 = \langle \varphi \rangle \langle \varphi \rangle \) are two pure states, then \( K(\rho_1, \rho_2) = \sqrt{1 - \langle \psi | \varphi \rangle^2} \).

Using the Pauli matrices, \( \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) and the base \( |e_1\rangle = \frac{1}{\sqrt{2}} \left( \begin{array}{c} 1 \\ 1 \end{array} \right), |e_2\rangle = \frac{1}{\sqrt{2}} \left( \begin{array}{c} 1 \\ -1 \end{array} \right) \), that have the eigenvalues \( \lambda_1 = 1, \lambda_2 = -1 \), one find that for all matrix densities for which \( \rho_1 - \rho_2 = \sigma_i \), the Kolmogorov distance between them is \( K(\rho_1, \rho_2) = 1 \).

4. For the ideal result, the expected one, \( \rho_0 \), and \( \rho_1 \), the obtained result obtained by applying the algorithm maximum of the probability to make the distinction between the two states is:
\[
\max \ p = \max \left( \frac{1}{2} \text{Tr}[M^{\text{ideal}}(\rho_0)] + \frac{1}{2} \text{Tr}[M^{\text{real}}(\rho_1)] \right) = \frac{1}{2} + \frac{1}{2} \max \text{Tr}[M(\rho_0 - \rho_1)].
\]

Proposition:
Let be two matrix densities \( \rho_0, \rho_1 \in \mathcal{H} \) with \( K(\rho_0, \rho_1) = \frac{1}{2} \text{Tr}|\rho_0 - \rho_1| \) then the probability of error can be computed by
\[
PE(\rho_0, \rho_1) = \frac{1}{2} - \frac{1}{4} \sum_{i=1}^{n} |\lambda_i| = \frac{1}{2} - \frac{1}{4} \text{Tr}|\rho_0 - \rho_1| = \frac{1}{2} (1 - K(\rho_0, \rho_1))
\]
with \( \lambda_i \) the eigenvalues of the difference \( \rho_0 - \rho_1 \).

4. Spectral Test for randomness

For randomness testing of binary sequences the law of large numbers will be used, if that \( (\varepsilon_n) \) is a sequence of independent random variables with the same distribution of expectation \( m \) and variance \( \sigma \), then for large values of \( n \) we have:
\[
Pr(a < \varepsilon_1 + \ldots + \varepsilon_n < b) \approx \Phi \left( \frac{b - n \cdot m + 0.5}{\sigma \sqrt{n}} \right) - \Phi \left( \frac{a - n \cdot m - 0.5}{\sigma \sqrt{n}} \right),
\]
where \( \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \) is the Laplace-Gauss function. Also, if that \( (\varepsilon_n) \) is a sequence of independent random variables with variable \( X: P(x = 1) = p, P(x = 0) = 1 - p \), then for large \( n \) one has \( \sigma = p(1 - p) \) (see [1,2])

For the Frequency (monobits) test where is investigated whether the frequency of ones in a sequence of length \( n \) is approximatively \( n/2 \), as would be expected under an assumption of randomness the probability of failing to reject the null hypothesis when it is false, \( \beta(\text{accept } H_0 | H_0 \text{ is false}) \) is expressed by (see [1,2,3]).
where $u_{1-\frac{\alpha}{2}}$ and $u_{\frac{n}{2}}$ stand for quantiles of the standard normal distribution and $q_1 = 1 - p_1$, with

$$H_0: p = p_0; H_1: p = p_1 \text{ and } p_1 \neq p_0.$$ 

For the **spectral test (DFT)**, under an assumption of randomness, the values obtained from the test should not exceed the threshold value $T = 0.95$ (see [8]). The algorithm computes the number $n_1$ of peaks in the subsequence given by the first half of the sequence, that are less than $T$:

$$\beta(\text{accept } H_0 | H_0 \text{ is false}) = \beta(n_1) = P\left(u_{\frac{n}{2}} \leq \frac{n_1 - 0.95 n p_0}{\sqrt{n p_0 q_0} 0.05} \leq u_{1-\frac{\alpha}{2}} \Big| p = p_1\right).$$

The focus of the test is the peak heights of the sequence in order to detect periodic features, whether the number of peaks exceeding the threshold is significantly different than those that does not.

For the n, the length of the bit string, $\varepsilon = \varepsilon_1, \varepsilon_2, \cdots \varepsilon_{n-1}, \varepsilon_n$, the sequence of bits being tested, produced by a Bernoulli variable $X: P(x = 1) = p, P(x = 0) = 1 - p$ and $T = 0.95$ the value $p_{\text{value}} = \text{erfc} \left(\frac{\varepsilon}{\sqrt{2}}\right)$ is computed. If the computed $p_{\text{value}}$ is less than 0.01, then is concluded that the sequence is non-random. The spectral test in both cases was described in the following table:

<table>
<thead>
<tr>
<th>Steps</th>
<th>Quantum using QFT</th>
<th>Classic using DFT</th>
</tr>
</thead>
</table>
| **Input** | - n, the length of the bit string ($n = 2^m, m \in \mathbb{N}$)  
- $\varepsilon$, the sequence of bits being tested | - n, the length of the bit string  
- $\varepsilon$, the sequence of bits being tested |
| **Test description** | 1. Apply a Quantum Fourier Transform (QFT) on $X$ to produce $S = QFT(X)$:  
2.1. Normalize the bit string.  
2.2. Compute the number of qubits used in QFT: $m = \log_2 n$.  
2.3. For each qubit (i), apply a Hadamard gate and (m-i-1) phase gates:  
- For i from 0 to m:  
- Apply H(i)  
- For j from 0 to m-i-1:  
  - Apply phase gates $\frac{\pi}{2 \sqrt{1-i+j+1}}$  
  - Apply barrier.  
- Measure the qubits: for i from 0 to m: measure (qubit[i])  
- Simulate the quantum circuit with 100 · m shots to Obtain $S = QFT(X)$ | **Input** | 1. Apply a Fast Fourier Transform (FFT) on $X$ to produce $S = FFT(X)$.  
2. Calculate $M = |S'|$, where $S'$ is the substring consisting of the first $\frac{n}{2}$ elements in $S$. |
| **Compute** | 3. Compute the 95% peak height threshold value, $T = \sqrt{\left(\log \frac{1}{0.05}\right) \cdot n}$.  
4. Compute the expected theoretical number of peaks, $n_0 = 0.95 \cdot \frac{n}{2}$  
5. Compute the actual number of peaks in $S$ that are less than $T, n_1$. | **Compute** | 4. Compute the 95% peak height threshold value, $T = \sqrt{\left(\log \frac{1}{0.05}\right) \cdot n}$.  
5. Compute the expected theoretical number of peaks, $n_0 = 0.95 \cdot \frac{n}{2}$  
6. Compute the actual number of peaks in $M$ that are less than $T, n_1$. |
7 Compute \( d = \frac{n_1 - n_0}{\sqrt{n_0} \cdot 0.95} \). 
8 Compute \( P - value = \text{erfc} \left( \frac{|d|}{\sqrt{2}} \right) \).

Output \( p\)-value \( p\)-value

<table>
<thead>
<tr>
<th>( n )</th>
<th>Classic</th>
<th>Quantum</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>passed</td>
<td>passed</td>
<td>1</td>
</tr>
<tr>
<td>128</td>
<td>1985</td>
<td>1955</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>1977</td>
<td>1975</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>1983</td>
<td>1979</td>
<td></td>
</tr>
</tbody>
</table>

Table 1.

In the quantum case the step 2 of the algorithm was explicitly presented.

5. Results and some conclusions

A comparison between the two cases for different length of the strings is made in Table 2.

Table 2.

<table>
<thead>
<tr>
<th>( n )</th>
<th>Classic</th>
<th>Quantum</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>passed</td>
<td>passed</td>
<td>1</td>
</tr>
<tr>
<td>128</td>
<td>1985</td>
<td>1955</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>1977</td>
<td>1975</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>1983</td>
<td>1979</td>
<td></td>
</tr>
</tbody>
</table>

Table 2.

Figure 3

Table 3.
Figure 3. $\beta(p_1)$ computed for 2000 strings of 256 length

$$p_0 = p_1 = \frac{1}{2}; p_1 \epsilon [0.48; 0.52]$$

$$\beta(p_1) = P \left( u \alpha \leq \frac{n_1 - 0.95 n p_0}{\sqrt{n p_0 q_0 \cdot 0.95 \cdot 0.05}} \leq u \alpha \right) \left| p = p_1 \right)$$

$$= \Phi \left( u \alpha \frac{\sqrt{p_0 q_0}}{p_1 q_1} + \frac{0.95 n (p_0 - p_1)}{\sqrt{n p_1 q_1 \cdot 0.95 \cdot 0.05}} \right) - \Phi \left( u \alpha \frac{\sqrt{p_0 q_0}}{p_1 q_1} + \frac{0.95 n (p_0 - p_1)}{\sqrt{n p_1 q_1 \cdot 0.95 \cdot 0.05}} \right)$$

We can conclude that the new technique is useful as a working tool in the validation of random generators obtained on quantum principles.

Bibliography


[8] [NIST 800-22]


