mgr inż. Piotr Jóźwiak

# Zastosowanie probabilistycznych metod do oceny losowości liczb otrzymanych z kwantowych generatorów liczb losowych

## Streszczenie rozprawy doktorskiej

**Słowa kluczowe:** bezpieczeństwo systemu informatycznego, testowanie losowości, kryptografia kwantowa, algorytm probabilistyczny, generator liczb losowych.

Oczekuje się, że w niedalekiej przyszłości silnie rozwijająca się informatyka kwantowa może dostarczyć niespotykanych dotąd mocy obliczeniowych. Oprócz szeregu pozytywów dostrzega się także zwiazane z tym zagrożenia w postaci możliwej kompromitacji aktualnie stosowanych mechanizmów bezpieczeństwa systemów informatycznych. Związane jest to z szeroko wykorzystywanymi algorytmicznymi, pseudolowymi generatorami liczb losowych, które bezpośrednio wiążą się z jakością systemów kryptograficznych. Tego typu deterministyczne źródła losowości wydają się być słabym mechanizmem w sytuacji gdy komputer kwantowy będzie w stanie złamać zabezpieczenie w stosunkowo krótkim czasie. Jednym z możliwych rozwiązań problemu jest opracowanie generatorów liczb losowych nie dających się przewidzieć – niezależnie od posiadanych mocy obliczeniowych. Kwantowe źródła losowości posiadają cechę nieprzewidywalności wynikającą bezpośrednio z probabilistycznej natury mechaniki kwantowej. Wyraża się ona poprzez absolutnie nieprzewidywalny wynik kwantowego pomiaru według schematu rzutowania von Neumanna, a także w zgodzie z ogólnie przyjętą probabilistyczną interpretacją mechaniki kwantowej zwaną interpretacją kopenhaską.

Praca przedstawia problem pozyskiwania liczb losowych z wykorzystaniem kwantowych generatorów liczb losowych, a w szczególności skupia się na zagadnieniach weryfikowania i testowania generatorów. Omawia zarówno empiryczne jak i teoretyczne metody testowania. Podejście empiryczne wykorzystuje metody statystycznego testowania hipotez do weryfikacji losowości danego ciągu liczb. Nie istnieje jeden uniwersalny test statystyczny, który byłby w stanie jednoznacznie zweryfikować losowość badanego ciągu. Tym samym wybrany ciąg poddaje się badaniu zestawowi testów statystycznych zamkniętych w tak zwanych bateriach testów. Autor wykorzystał do badań najpopularniejszą baterię statystyczną opracowaną w National Institute of Standards and Technology pod nazwą Statistical Test Suite SP800-22 (NIST STS). Stanowi ona do dzisiaj światowy standard w testowaniu losowości. Badanie miało na celu określić parametry testów i ich przydatność do testowania nowej klasy kwantowych generatorów liczb losowych. Jest to szczególnie istotne zagadnie z uwagi na fakt, że analizowane narzędzie NIST STS nie zostało opracowane z myślą o testowaniu tego typu generatorów. W pracy przedstawiono szereg niedoskonałości jakie dostrzeżono w baterii NIST STS, w szczególności związanych z poszukiwaniem dalekozasięgowych korelacji oraz celowych, deterministycznych manipulacji w sekwencjach bitowych.

Przedstawia się także problem teoretycznego testowania kwantowych generatorów liczb losowych dowodząc, że tego typu podejście sprowadza się do wykazania kwantowej natury źródła losowości. W tym celu zaproponowano wykorzystanie złamania nierówności Bella-CHSH jako podstawy do oceny kwantowego generatora wykorzystującego splątanie kwantowe. Zaproponowano miarę dla niedoskonałych splątaniowych generatorów liczb losowych oraz opracowano permutacyjny test statystyczny wykorzystujący nierówność Bella-CHSH do oceny

dwóch źródeł losowości. Z uwagi na trudności w rzeczywistej realizacji generatora pozbawionego dekoherencji opracowano symulator umożliwiający otrzymanie próbek badawczych wykazujących podobieństwo względem czystego stanu splątanego. Przeprowadzono badania w kierunku wyznaczenia rozkładu prawdopodobieństwa jakim cechują się korelacje w nierówności Bella-CHSH.

Zaproponowano dalsze możliwe kierunki rozwoju kwantowych generatorów liczb prawdziwie losowych umożliwiających wykonywanie publicznej oceny jakości generatora kwantowego. Przedstawiona koncepcja kwantowego generatora liczb losowych wykorzystująca odpowiednie wieloqubitowe splątanie kwantowe jest bezpośrednią odpowiedzią na opisane problemy. Rozwiązaniem problemu ograniczonej mocy obliczeniowej jest możliwość przeniesienia testowania losowości do publicznej domeny bez narażenia sekwencji losowej. Opracowany protokół zapewnia dostarczenie wielu sprzężonych ze sobą sekwencji o tej samej statystycznej charakterystyce, tym samym umożliwiając ocenę wszystkich sekwencji na podstawie badania tylko jednej z nich. Nieujawnione sekwencje nadają się do zastosowań kryptograficznych.

W rodziałach od *pierwszego* do *czwartego* skupiono się na zagadnieniach teoretycznych losowości oraz probabilistycznych fundamentach mechaniki kwantowej w kontekście losowości.
W rozdziale *piątym* omówiono różne koncepcje kwantowych generatorów liczb losowych wykorzystanych do akwizycji materiału badawczego. Scharakteryzowano próbki badawcze, które w następnej kolejności poddano badaniom statystycznym pakietem NIST STS. Na tej podstawie dokonano krytycznej oceny pakietu NIST STS względem możliwości zastosowania jej do kwantowych źródeł losowości.
W rozdziale *szóstym* skupiono się na poszukiwaniu metod weryfikacji losowości specjalizowanych do testowania kwantowych generatorów liczb losowych. W pracy opisany został generator wykorzystujący złamanie nierówności Bella-CHSH, dla którego opracowano miarę jakości niedoskonałego generatora splątaniowego. Zbadano także rozkład prawdopodobieństwa korelacji w nierówności Bella-CHSH, aby umożliwić dalsze badania w kierunku zrozumienia statystycznej natury tego zjawiska. Opracowano symulator takiego układu oraz permutacyjny test statystyczny oceniający splątaniowy kwantowy generator liczb losowych na podstawie analizy korelacji w nierówności Bella-CHSH. Test ten umożliwia ocenę splątaniowych generatorów liczb losowych względem idealnej realizacji generatora lub względem innych tego typu generatorów.
Rozdział *siódmy* przedstawia nowy i oryginalny kierunek rozwoju kwantowych generatorów liczb prawdziwie losowych umożliwiających wykonywanie publicznej oceny jakości generatora kwantowego. Przedstawiona koncepcja kwantowego generatora liczb losowych wykorzystująca odpowiednie wieloqubitowe splątanie kwantowe jest bezpośrednią odpowiedzią na część problemów opisanych w poprzednich rozdziałach. Umożliwia generowanie w bezpieczny sposób ciągu liczb losowych, który przed wykorzystaniem w zastosowaniach kryptograficznych może być poddany publicznej weryfikacji losowości bez narażenia na jego skompromitowanie. Wykorzystuje się tu kilka ciągów losowych wzajemnie splątanych kwantowo i posiadających ten sam poziom losowości.

W zakończeniu pracy podsumowano wyniki badań uzasadniając na ich podstawie wstępnie postawione hipotezy badawcze.

Xāi 2

mgr inż. Piotr Jóźwiak

# Application of probabilistic methods to evaluate the randomness of numbers obtained from quantum random number generators

## Abstract

**Keywords:** information system security, randomness testing, quantum cryptography, probabilistic algorithm, random number generator.

It is expected that in the near future, the strongly developing quantum computing may provide unprecedented computing power. In addition to a number of positives, the associated risks in the form of the possible compromise of currently used IT security mechanisms are also recognised. This is related to the widely used algorithmic pseudo-random number generators, which are directly related to the quality of cryptographic systems. Such deterministic sources of randomness appear to be a weak mechanism when a quantum computer will be able to break security in a relatively short time. One possible solution to the problem is to develop unpredictable random number generators - regardless of the computing power available. Quantum sources of randomness have a feature of unpredictability arising directly from the probabilistic nature of quantum mechanics. It is expressed by the absolutely unpredictable outcome of quantum measurement according to the von Neumann projection scheme, and in agreement with the generally accepted probabilistic interpretation of quantum mechanics called the Copenhagen interpretation.

The paper presents the problem of obtaining random numbers using quantum random number generators, and focuses in particular on the issues of verifying and testing the generators. It discusses both empirical and theoretical testing methods. The empirical approach uses statistical hypothesis testing methods to verify the randomness of a given sequence of numbers. There is no universal statistical test that can unambiguously verify the randomness of the sequence under test. Thus, the selected sequence is subjected to a set of statistical tests encapsulated in so-called test suites. The author used the most popular statistical suite developed at the National Institute of Standards and Technology called Statistical Test Suite SP800-22 (NIST STS). It is still the global standard for randomisation testing today. The study aimed to determine test parameters and their suitability for testing a new class of quantum random number generators. This is a particularly pertinent issue given that the NIST STS tool under study was not designed to test this class of generator. The paper outlines a number of shortcomings that have been perceived in the NIST STS battery, particularly related to the search for long-range correlations and intentional, deterministic manipulations in bit sequences.

The problem of theoretical testing of quantum random number generators is also presented, proving that this type of approach amounts to demonstrating the quantum nature of the source of randomness. To this end, it is proposed to use the breaking of the Bell-CHSH inequality as a basis for evaluating a quantum generator using quantum entanglement. A measure for imperfect entanglement-based random number generators is proposed and a permutation statistical test using the Bell-CHSH inequality to evaluate two sources of randomness is developed. Due to difficulties in the real implementation of a decoherence-free generator, a simulator was developed to obtain test samples showing similarity with respect to the pure entangled state. A study was carried out to determine the probability distribution with which the correlations in the Bell-CHSH inequality are characterised.

Further possible directions for the development of quantum true random number generators enabling the performance of public quantum generator quality assessment have been proposed. The presented concept of a quantum random number generator using appropriate multi-qubit quantum entanglement is a direct answer to the described problems. The solution to the problem of limited computing power is that randomness testing can be transferred to the public domain without compromising the random sequence. The protocol developed provides multiple coupled sequences with the same statistical characteristics, thus allowing all sequences to be evaluated by testing only one of them. The unexposed sequences are suitable for cryptographic applications.

Chapters *one* to *four* focus on the theoretical issues of randomness and the probabilistic foundations of quantum mechanics in the context of randomness.

Chapter *five* discusses the various concepts of quantum random number generators used to acquire test material. The research samples were characterised, which were then statistically tested with the NIST STS package. On this basis, a critical evaluation of the NIST STS package was made with respect to its applicability to quantum random number sources.

Chapter *six* focuses on the search for randomness verification methods specialised for testing quantum random number generators. The paper describes a generator using the breaking of the Bell-CHSH inequality, for which a measure of the quality of an imperfect entanglement generator is developed. The probability distribution of correlations in the Bell-CHSH inequality was also investigated to allow further research towards understanding the statistical nature of this phenomenon. A simulator of such a system and a permutation statistical test to evaluate an entangled quantum random number generator based on correlation analysis in the Bell-CHSH inequality were developed. This test allows the evaluation of entangled random number generators against an ideal realisation of the generator or against other such generators.

Chapter *seven* presents a new and original direction in the development of quantum true random number generators enabling the performance of public quantum generator quality assessment. The presented concept of a quantum random number generator using appropriate multi-qubit quantum entanglement is a direct answer to some of the problems described in the previous chapters. It makes it possible to generate in a secure way a sequence of random numbers that can be subjected to public randomness verification before being used in cryptographic applications without being compromised. Several random sequences mutually quantum entangled and having the same level of randomness are used here.

The paper concludes by summarising the results of the research, justifying the initial research hypotheses based on them.