Fundusze Europejskie Inteligentny Rozwój

Projekt realizowany w ramach Programu Operacyjnego Inteligentny Rozwój, poddziałanie 1.1.1 'Badania przemysłowe i prace rozwojowe realizowane przez przedsiębiorstwa', współfinansowany ze środków Budżetu Państwa oraz Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

SZCZEGÓŁOWY OPIS ZREALIZOWANYCH PRAC ORAZ UZYSKANYCH WYNIKÓW W RAMACH ETAPU 1 PROJEKTU PT. "JURAND - NARODOWY KWANTOWY GENERATOR LICZB LOSOWYCH"

I. Podsumowanie wyników badań w ramach etapu 1 projektu

Przedmiotem realizacji etapu 1 projektu "JURAND - Narodowy Kwantowy Generator Liczb Losowych" były badania przemysłowe w zakresie modelu weryfikacji losowości ciągów losowych generowanych w procesach kwantowych. Głównym rezultatem przedmiotowych badań było wynalezienie nowej koncepcji kwantowego generatora liczb losowych z własnością publicznej weryfikacji losowości kwantowo generowanego ciągu bez ujawnienia jego poufnej postaci, co stanowi zasadniczy i nowatorski jakościowo wynik teoretyczny odnośnie planowanego w etapie 1 projektu zdefiniowania modelu weryfikacji kwantowej losowości. Jest to bardzo istotny wkład na poziomie koncepcyjnym w zakres dotychczasowych rezultatów nad inżynierią generacji losowości w skali międzynarodowej. Koncepcja ta została opisana w formie publikacji naukowej (P-1) i przesłana do międzynarodowego dziedzinowego periodyku naukowego "Entropy" w dniu 1 listopada 2017 r., a także zgłoszona do ochrony patentowej w ramach procedury krajowej w Urzędzie Patentowym Rzeczypospolitej Polskiej UPRP oraz procedury międzynarodowej w ramach układu Patent Cooperation Treaty (PCT) do Światowej Organizacji Własności Intelektualnej (World Intellectual Property Organization, WIPO) w Genewie (zgłoszenia patentowe odpowiednio ZP-1 oraz ZP-2).

W raporcie (R-1) zawarto szczegółowe sprawozdanie merytoryczne z wyników prac badawczych z realizacji etapu 1 projektu "JURAND - Narodowy Kwantowy Generator Liczb Losowych". W ramach wyników zrealizowanych prac badawczych realizator wytworzył następujące dokumenty formalne:

1. R-1: Raport z realizacji badań przemysłowych w ramach etapu 1 projektu, pt. "JURAND - Narodowy Kwantowy Generator Liczb Losowych" (kamień milowy z realizacji etapu 1 projektu) [autorzy: Witold A. Jacak, Janusz E. Jacak, Wojciech A. Donderowicz, Lucjan Jacak]
2. P-1: Publikacja w języku angielskim w międzynarodowym naukowym czasopiśmie dziedzinowym "Entropy", pt. "Quantum random number generator protocols based on topologically inequivalent entanglements of quantum states" ([01.11.2017]; [Witold A. Jacak, Janusz E. Jacak, Wojciech A. Donderowicz, Lucjan Jacak]; [Entropy - Open Access Journal, ISSN 1099-4300; CODEN: ENTRFG, MDPI])
3. P-2: publikacja w języku angielskim na międzynarodowej platformie internetowej kwantowego bezpieczeństwa "seQre.net", pt. "Randomness" ([31.12.2017]; [Witold A. Jacak, Janusz E. Jacak, Wojciech A. Donderowicz, Lucjan Jacak]; [seQre.net])
4. P-3: publikacja w języku angielskim na międzynarodowej platformie internetowej kwantowego bezpieczeństwa "seQre.net", pt. "Random numbers generator statistical tests" ([31.12.2017]; [Witold A. Jacak, Janusz E. Jacak, Wojciech A. Donderowicz, Lucjan Jacak]; [seQre.net])
5. ZP-1: Zgłoszenie patentowe w języku polskim (procedura krajowa URPP), pt. "Splątaniowy Kwantowy Generator Liczb Losowych z publiczną certyfikacją losowości" (numer zgłoszenia: P.424140 z dnia 30.12.2017)
6. ZP-2: Zgłoszenie patentowe w języku angielskim (procedura międzynarodowa PCT), pt. "Entanglement Quantum Random Number Generator with public randomness certification" (numer zgłoszenia: WIPO ST 10/C PL424140 z dnia 31.12.2017)
7. W-1: Dane źródłowe i statystyczne w zakresie prowadzonych analiz losowości generowanych laboratoryjnie ciągów

W ramach badań przemysłowych objętych etapem 1 zrealizowano wstępne opracowanie koncepcyjne nowych i oryginalnych kwantowych protokołów generowania liczb losowych QRNG opartych na splątaniu wieloqubitowym. Wykazano również teoretycznie (ww. publikacja w zgłoszeniu do specjalistycznego wydawnictwa naukowego) całkiem nowe właściwości odkrytych splątaniowych protokołów QRNG, pozwalające realizować publiczną weryfikację losowości generowanych ciągów bez ich ujawniania, co wprowadza nową jakość w zakresie możliwości zastosowań kryptograficznych. Prace te stanowią istotny rezultat ostatniej fazy etapu 1 projektu (tj. zadania 3. dotyczącego badań nad modelowym odwzorowaniem fizycznej struktury zjawiska odpowiadającego za losową generację wartości bitu w końcowym ciągu losowym). Modelowanie to przyjęło za podstawę nowo odkrytych protokołów QRNG całkowicie nieklasyczne (niemające klasycznego odpowiednika i naruszające uwarunkowania lokalności klasycznych teorii fizycznych) zjawisko splątania kwantowego (powstające w wielu znanych procesach fizycznych, zwłaszcza w optyce kwantowej), w którym nielokalne korelacje pomiarowe łamią klasyczne ograniczenia statystyczne (złamanie nierówności Bella i CHSH, tzw. paradoks EPR i tw. Bella), a jednocześnie przy odpowiedniej konfiguracji modelowej protokołu QRNG pozwalają wprowadzić powiązane informacyjnie (tj. skorelowane w wartościach bitowych) losowe ciągi bitowe, z których ujawnienie jednego nie ujawnia zawartości informacyjnej (bitów) drugiego, a jednocześnie umożliwia bezwarunkową publiczną weryfikację entropii statystycznej losowości (tj. weryfikację, że generowany ciąg losowy rzeczywiście jest prawdziwie losowy spełniając właściwe miary, czyli jest generowany w wyniku fundamentalnie niedeterministycznego

procesu kwantowego).

Ponadto zgodnie z planem badawczym etapu 1 projektu zrealizowano badania w zakresie modelowania prawdziwej losowości w tym miar statystycznych i modeli stochastycznych dla charakteryzacji parametrycznej jakości i efektywności procesów generowania liczb losowych opartych na zjawiskach kwantowych w celu określenia w etapie 2. optymalnej technologii dla opracowania zakładanego w projekcie kwantowego generatora losowości QRNG. W szczególności w etapie 1 projektu zrealizowano badania teoretyczne w zakresie weryfikacji stacjonarności i ergodyczności procesu stochastycznego modelowych bitowych ciągów losowych oraz parametryzacji ich właściwości statystycznych w tym wartości średnich, wariancji, funkcji korelacyjnych (dotyczy to zarówno badanych modelowych procesów kwantowej losowości jak i procesów pseudolosowych, uzyskiwanych w ramach dostępnej aparatury laboratoryjnej). Zrealizowany zakres badawczy stanowił obszar zadania 1. wchodzącego w skład 3 zadaniowej struktury merytorycznej badań w ramach etapu 1. Przeprowadzono także badania analityczno-teoretyczne w zakresie poszukiwania powtarzających się podciągów, ew. stanowiących rozpoznawalne wzorce w ciągach losowych generowanych na dostępnych platformach laboratoryjnych źródeł kwantowych i klasycznych, a także badania w zakresie optymalnych testów statystycznych pozwalających najwłaściwiej mierzyć poziom losowości zwłaszcza kwantowo generowanych ciągów bitowych (klasyczne generatory losowości, oparte o deterministyczne procesy fizyczne wprowadzają do ciągów losowych przewidywalne wzorce, obniżając wartości parametrów statystycznych np. złożoność Kolmogorova - odwrotnie proporcjonalną do potencjału kompresyjnego, jak również entropię Shannona) - ten zakres badawczy stanowił obszar zadania 2 etapu 1. Badania statystyczne losowości generowanych laboratoryjnie ciągów losowych w procesach kwantowych oraz klasycznych mają udokumentowaną formę elektroniczną i ze względu na ograniczenia rozmiarowe danych pomiarowych przechowywane są w pamięciach masowych klastra obliczeniowego, na którym prowadzono złożone obliczeniowo analizy (tj. badania analityczno-teoretyczne w zakresie miar statystycznych i poszukiwania powtarzających się podciągów bitowych pod kątem weryfikacji występowania wzorców w ciągach losowych generowanych na dostępnych platformach laboratoryjnych źródeł kwantowych i klasycznych, a także badania w zakresie optymalnych testów statystycznych pozwalających najwłaściwiej mierzyć poziom losowości zwłaszcza kwantowo generowanych ciągów bitowych - klasyczne generatory losowości, oparte o deterministyczne procesy fizyczne wprowadzają do ciągów losowych przewidywalne wzorce, obniżając wartości parametrów statystycznych np. złożoność Kolmogorova - odwrotnie proporcjonalną do potencjału kompresyjnego, jak również entropię Shannona).

W toku realizacji etapu 1 projektu przeprowadzono również zakup koniecznej do realizacji badań aparatury badawczej, w tym w zakresie klastra obliczeniowego wysokiej wydajności wykorzystanego w celach numerycznej weryfikacji statystycznych charakterystyk ciągów losowych generowanych kwantowo i klasycznie w realizowanych w etapie 1 badaniach nad oceną losowości i jej parametryzacji statystycznej (co dotyczy wykazania przewag ciągów fundamentalnie niedeterministycznych, generowanych kwantowo, które jak zostało dowiedzione w wyniku ww. opisanych nowych uzyskanych rezultatów badawczych w toku etapu 1 projektu, posiadają nie tylko przewagi ilościowe w zakresie statystycznym losowości, ale również jakościowe, oparte na nielokalnym zjawisku splątania kwantowego i umożliwiające publiczną weryfikację losowości bez ujawniania faktycznej zawartości ciągu losowego, co ma istotne i przełomowe zastosowania kryptograficzne).

II. Wyniki badań w zakresie teorii i modelowania losowości

Definicja generowania prawdziwej losowości charakteryzuje się dużą problematyką koncepcyjną w ujęciu teorii probabilistycznych i statystycznych. Definicja ta próbuje formalnie opisać koncepcję, w odniesieniu co do której nie wiadomo nawet czy ma charakter matematyczny. Koncepcja ta w kategoriach fundamentalnych prowadzi do problemów filozoficzno-epistemologicznych, które poważnie warunkują również interpretację i niepełne obecnie rozumienie samego pojęcia prawdopodobieństwa. Dodać można, że jakkolwiek w zakresie historii badań prawdopodobieństwa i losowości sformułowane zostały ogólne, wysoce sformalizowane definicje losowości oparte na każdorozowo rozwijanym aparatem matematycznym, to jednak sformułowania te nie są w stanie uchwycić kompletnego opisania na fundamentalnym poziomie idei, która stoi za całkowicie niedeterministyczną, tj. prawdziwą losowością. W sytuacji najprostszego logicznie systemu klasycznego, tj. dwuwymiarowego (binarnego) logicznego systemu klasycznego, którego reprezentacja formalna jest zbiorem dwuelementowym, np. $\{0, 1\}$ w kodowaniu binarnym, dowolny ciąg utworzony w ramach elementów takiego zbioru można definiować jako liczba rzeczywista np. należąca do zbioru $[0, 1]$. Z tym właśnie wiąże się bardzo fundamentalny problem z defincją losowości. Problem ten związany jest dokładniej z faktem, że skoro długość dowolnego losowego ciągu binarnego jest teoretycznie nieskończona (jeśli długość ciągu przyjąć jako n, to jest to co najwyżej przeliczalna liczba nieskończona, aleph-zero, tj. liczba kardynalna np. zbioru liczb naturalnych), to zbiór wszystkich takich możliwych losowych ciągów, zdefiniowane jako kombinacje binarne dwuelementowego zbioru $\{0, 1\}$ na n pozycjach ciągu ma 2^n elementów (tyle jest kombinacji zer i jedynek na n pozycjach bitowych). Jednak, jak wykazał Cantor w swoich słynnych twierdzeniach dotyczących nieskończoności, liczba 2^n, gdzie n jest policzalnie nieskończone - jest równe kontinuum (tj. liczbie kardynalnej c, charakteryzującej nieprzeliczalną nieskończoność, np. mnogość zbioru liczb rzeczywistych, ale również wszelkich pozbiorów tych liczb, w tym m.in. także i podzbioru $[0, 1]$.

To wykazuje, że fundamentalny problem dotyczący losowości kwantowej wiąże się z fundamentalnymi problemami dotyczącymi nieskończoności i nieskończonych zbiorów nieprzeliczalnych.

Szczegółowe wyniki badań zreferowane w raporcie (R-1) z realizacji etapu 1 projektu. Z wniosków badawczych wynika, że w ramach odniesienia klasycznego kwestia prawdziwej losowości wymyka się ścisłym ujęciom matematycznym (zarówno w zakresie ewoluujących testów statystycznych jak i ujęcia opartego na teorii złożoności obliczeniowej). Sytuacja ta wynika z fundamentalnych problemów definicyjnych związanych z nieskończonościami, przeliczalnością i nieprzeliczanością w matematyce, jednak ma również istotny charakter interpretacji losowości jako kwestii semantyki językowej. Wobec omówionych fundamentalnych problemów interpretacyjnych oraz konstrukcji teoretycznych, można wskazać podsumowująco, że oba podejścia klasycznej definicji losowości (oparte na testach statyscznych oraz złożoności obliczeniowej) nie mogą stanowić pełnego kryterium nieuchwytnej losowości. Wydaje się w kontekście powyższej dyskusji, że istota prawdziwej losowości jest związana z fundamentalnym niedeterminizmem, istniejącym w reżimie kwantowym i abstrahującym od niedoskonałości klasycznych formalnych usiłowań ścisłego uchwycenia losowości. Przykładowo zgodnie z argumentacją Khrennikowa i Zeilingera [1], możliwa jest sytuacja, w której czysto matematyczne ujęcie koncepcji losowości i formalizacji jej definicji jest niemożliwe, ponieważ ramy matematyczne mogą być niewystarczające do teoretycznego sformułowania problematyki niedeterminizmu. Wiele wskazuje na to, że to raczej fizyczne zjawiska są dziedziną, w której ktwi natura prawdziwej i niedeterministycznej losowości. Dotyczy to procesów fizyki kwantowej, która w ujęciu pomiaru kwantowego, tj. przekrycia z klasyczną rzeczywistością jest fundamentalnie niedeterministyczna. W mechanice kwantowej funkcjonują równolegle nieweryfikowalne fizycznie intepretacje. Jedną z głównych interepretacji jest tzw. interpretacja kopenhaska mechaniki kwantowej, którą sformułował N. Bohr i W. Heisenberg w 1927 w Kopenhadze, w powiązaniu z koncepcjami M. Borna, tj. interpretowaniem funkcji falowej w kategoriach probabilistycznej. Przykładowo dla funkcji falowej w mechanice kwantowej w ramach tzw. reprezentacji położeniowej, kwadrat modułu funkcji falowej (należącej do przestrzeni Hilberta definiowanej nad ciałem liczb zespolonych) określa gęstość prawdopodobieństwa znalezienia tej cząstki w danym punkcie przestrzeni lub też w obszarze przestrzeni [2]). W obecnym ujęciu mechaniki kwantowej przedmiotowa interpretacja nosi miano standardowej i najbardziej upowszechnionej. Niezależnie rozwijają się inne konkurencyjne interpretacje mechaniki kwantowej, z których w przedmiotowym kontekście najistotniejsze są te, które charakteryzują się odmiennym rozumiem prawdopodobieństwa. Do takich interpretacji należy coraz powszechniej akceptowana interpretacja nazywana Kwantowym Bayesianismem, która zaproponowana została Fuchsa [3], w dość istotnym zaprzeczeniu podstawowym założeniom interpretacji kopenhaskiej, zwłaszcza w zakresie właśnie interpretacji problematycznej do uchwycenia natury prawdopodobieństw. W ramach standardowej reprezentacji kopenhaskiej rola prawdopodobieństwa wyraża się poprzez pomiar układu kwantowego, który w ujęciu von Neumanna w sposób losowy (probabilistyczny) doprowadza do rzutowania stanów kwantowych będących superpozycjami stanów klasycznych na konkretne stany klasyczne (jest to tzw. kolaps funkcji falowej, który ma charakter niedeterministycznie losowy). Rzutowanie realizujące ww. kolaps funkcji falowej zachodzi w wyniku oddziaływania zewnętrznego obserwatora, czyli w ogólności zewnętrznego i makroskopowego (co stanowi właśnie podstawe kryterium definicji pomiaru) układu mierzącego, który scharakteryzowany jest przez ogromną liczbę stopni swobody rzędu liczby Avogadro, tj. 10^23 – z podlegającym pomiarowi układem kwantowym. Taki schemat pomiaru kwantowego był przedmiotem badań teoretycznych von Neumanna [4], w toku których von Neumannn wysunął tzw. "ansatz pomiaru", jako aksjomat stwierdzający, że wobec wykonywanego pomiaru funkcja falowa kwantowego układu ulega kolapsowi co odbywa się w całkowicie niedeterministyczny, a zatem w prawdziwie losowy sposób, będąc rzutowaną do jednego z możliwych stanów klasycznych (tzw. stanów własnych obserwabli lub tożsamo odpowiadającej tej obserwabli bazy pomiarowej, tworzonej ze stanów własnych tej obserwabli) z konkretnym, niezerowym prawdopodobieństwem, stanowiącym z warunku unormowania kwadrat modułu współczynnika superpozycji kwantowej (kombinacji liniowej w rozwinięciu funkcji falowej właśnie w stanach własnych danej obserwabli i odpowiadającej jej bazy). W ujęciu teoretycznym definicja losowości w kontekście sformułowania teorii mechaniki kwantowej oraz powiązanej z nią silnie teorii informacji kwantowej odpowiada pojęciu nieznanego stanu kwantowego (co może być identyfikowane z pojęciem nieznanej informacji kwantowej). Jako zasadnicze aspekty takiego sformułowania występują pojęcia niedeterminizmu oraz superdeterminizmu, a także problematyka filozoficzno-epistemologiczna dotycząca założenia realizmu w mechanice kwantowej. Aby udzielić odpowiedzi na przykład nad pytanie czy dana liczba (np. reprezentujący ją ciąg binarny stanowiący inaczej serię pomiarów kwantowych qubitów w bazie obliczeniowej) jest losowa czy też nie, trzeba udzielić wcześniej odpowiedzi na pytanie czy informacja kwantowa podlegająca pomiarowi jest reczywiście obiektywnie nieznana. Pytanie to sprowadza się do problemu czy istnieje gdzieś nośnik wiedzy dotyczącej tej właśnie konkretnej liniowej kombinacji stanu kwantowego ciągu qubitów, definiujących informację kwantową. Nie jest tu istotne, czy np. konkretne qubity są w stanach kombinacji liniowych znajdujących się bardzo bliskio stanów bazy (co alternatywnie oznacza, że prawdopodobieństwa wystąpienia 0 lub 1 w pomiarze są bliskie wartości 1) lub nawet, że faktycznie znajdują się dokładnie w stanach bazowy (wówczas prawdopodobieństwa zmierzenia 0 lub 1 w ciągu bitów reprezentującym rejestr qubitów są równe 1). Istotny jest natomiast fakt, czy konfiguracje tych stanów kwantowych są znane czy nie. Ten warunek w ogólności odpowiada znacznie szerszej kwestii definicji istnienia nieznanej informacji kwantowej (co to znaczy, że nieznana informacja kwantowa istnieje),

czy nawet istnienia informacji kwantowej w ogóle (tj. czym w istocie informacja kwantowa jest).

W zakresie praw mechaniki kwantowej, przyczyną losowości jest rzutowanie von Neumanna oraz nieznana konfiguracja stanu kwantowego (tj. nieznana koherentna, inaczej znormalizowana, kombinacja liniowa, inaczej superpozycja, stanów znanych, reprezentujących klasyczną informację). Pomiar kwantowy wiąże się jednak z losowo przebiegającym procesem dekoherencji (w którym losowość wynika z niewspółmierności liczby stopni swobody układu pomiarowego i procesu zupełnego defazowania układu mierzonego, będącego w nieznanym stanie kwantowym, np. nieznanego qubitu w toku wspólnej ewolucji z makroskopowym układem pomiarowym). W tym sensie przebieg dekorenencji kwantowej jest (w sformułowaniu superwyboru Żurka) podstawą definicji niedeterministycznej zmiennej losowoej. Pozostaje pytanie o przygotowanie lub dostępność w rzeczywistości prawdziwie nieznanego stanu kwantowego i wątpliwości czy nie jest on może jednak znany dla zewnętrznego, innego obserwatora. Wówczas obserwator ten mógłby potencjalnie skomunikować się z obserwatorem lokalnym, który wykonuje pomiar na (w jego przekonaniu) nieznanym stanie kwantowym, przekazując mu informację klasyczną o konfiguracji bazy pomiarowej, natychmiast redukującą kwantowość stanu mierzonego przez lokalnego obserwatora do informacji klasycznej. W związku z tym definicja prawdziwej losowości, może być oparta na pomiarze kwantowym jedynie prawdziwej informacji kwantowej, zatem fundamentalnie nieokreślonej – tj. nieznanej dla żadnego klasycznego obserwatora. Jak wspomniano powyżej, czy taka informacja istnieje jest obecnie kwestią nierozstrzygniętą i powiązaną z problematyką filozoficznej epistemologii.

Należy jednak wskazać pewne interesujące własności odnoszące się do losowości takiej informacji, gdyby rzeczywiście istniała. Okazuje się, że w takiej sytuacji losowość zawarta już w jednym tylko qubicie takiej właśnie nieznanej informacji – może być równoważna losowości zawartej w n qubitach i wiąże się z pojęciem kwantowego splątania.

Jest to bardzo fundamentalny wynik badawczy również o nowatorskim charakterze realizacji przedmiotowego projektu w zakresie koncepcji randomizacji ciągu n qubitowego tylko pojedynczym qubitem znajdującym się w stanie nieznanej informacji kwantowej poprzez wieloqubitowe splątanie. Ilustruje to procedura OQP, One-Qubit Pad, która została opracowana jako istotny nowy protokół kryptografii kwantowej również przez autorów projektu w toku niezależnych badań.

Realizowana w protokole OQP randomizacja n qubitów w określonych stanach kwantowych pojedynczym tylko qubitem w nieokreślonym / nieznanym stanie kwantowym stanowi poważny rezultat formalnego wykazaniem, że losowość pojedynczego prawdziwie nieznanego qubitu jest równoważna losowości n qubitów, co wiąże się z własnościami zbiorów gęstych (tj. nieprzeliczalnych konfiguracji superpozycji pojedynczego qubitu). Efekt polega na zadaniu poprzez wielokrotne splątanie kwantowe (iteracyjne wykonanie kwantowej operacji unitarnej kontrolowanej negacji CNOT, zawsze z tym właśnie pojedynczym i randomizującym qubitem kontrolnym znajdującym się w nieznanym stanie kwantowym oraz kolejnymi qubitami rejestru jako qubitami celowymi CNOT) propagacji losowości (w toku wieloqubitowego splątania) z pojedynczego qubitu randomizującego na n qubitów w stanach predefiniowanych (nawet klasycznych). Działania OQP nie tylko randmizuje stan rejestru qubitów, ale także umożliwia odwrócenie tej randomizacji, co stanowi odkrycie podstawowego kwantowego szyfru uogólniającego klasyczny szyfr One-Time Pad (w pzypadku kwantowym z kluczem o długości zaledwie 1 qubitu – można tu dodać, że na podobnej zasadzie w analogii klasycznej, procedura szyfru One-Time Pad OTP to także randomizacja randomizacja wcześniej predefiniowanego konkretnego binarnego ciagu klasycznego, ale wymaga w sytuacji klasycznej n bitów randomizujących). W przypadku kwantowym ze względu na nieprzeliczalną mnogość zbioru stanów pojedynczego qubitu jego pojemność losowa (zawarta w fundamentalnie nieznanym stanie) pozwala zrandomizować stany n (nawet nieskończonej ale przeliczalnej liczby) qubitów, stanem tylko pojedynczego qubitu (odpowiada to wynikom Cantora w zakresie teorii nieskończoności, według której dowolnie mały podzbiór zbioru nieskończonego nieprzeliczalnego o liczbie kardynalnej kontinuum c, sam również ma taką liczbę kardynalną, tj. kontinuum c – ale także bardzo istotnej roli splątania kwantowego, całkowicie nieklasycznego zasobu informacji kwantowej).

Należy wreszcie dodać, że splątanie kwantowe stanowiące bardziej obiektywny zasób kwantowy od nieznanego stanu kwantowego, jest również istotnym elementem definicji prawdziwej losowości kwantości (wskazuje na to jego fundamentalna rola w randomizacji n qubitów pojedynczym nieznanym stanem jednego qubitu). Samo splątanie kwantowe jest ponadto kluczowym elementem wprowadzenia całkowicie jakościowo nowej klasy kwantowej generacji liczb losowych, tj. koncepcji splątaniowego kwantowego generatora liczb losowych (EQRNG) z publicznym poświadczeniem losowości generowanego ciągu bitowego przy zachowaniu jego tajności. Jest to również nowatorski i istotny w zastosowaniach kryptograficznych rezultat koncepcyjny 1 etapu realizacji projektu.

Szczegółowe wyniki badań w tym zakresie przedstawiono w raporcie (R-1) jak również w publikacji technicznej (P-2).

III. Splątaniowy Kwantowy Generator Liczb Losowych z publiczną certyfikacją losowości

Najistniejszym wymiarem zrealizowanych prac badawczych i ich wyników jest nowatorska koncepcja generatora EQRNG z publicznym poświadczeniem losowości.

Ponieważ kwantowe generatory liczb losowych zyskują na popularności, zwłaszcza w odniesieniu do możliwości budowy skalowalnego komputera kwantowego, proponuje się nowy wynalazek w tym obszarze w oparciu o topologiczne właściwości splątania kwantowego. Proponowany Splątaniowy Kwantowy Generator Liczb Losowych (Entanglement QRNG) wykorzystuje pewną konfigurację wieloqubitowego splątania stanów kwantowych w celu uzyskania losowości z publiczną certyfikacją. Wynalazek opisuje zarówno protokół, jak i implementujące go wzorcowe urządzenie, obejmujące specyficzne 3-qubitowe splątanie kwantowe typu uogólnionego stanu Bella (topologicznie nieekwiwalentne względem innych możliwych typów konfiguracyjnych 3-qubitowego splątania i łatwo uogólnialne na wielostronnie splątane qubity, jak przedstawiono w opisie wynalazku), charakteryzowane również w kategoriach topologicznych, które umożliwia generowanie tajnych ciągów prawdziwie losowych z publicznie dostępnym dowodem ich losowości, umożliwiając w ten sposób podmiotowi zewnętrznemu swobodne i publiczne zweryfikowanie losowości wygenerowanej sekwencji bez ujawniania tej stronie jej tajności lub zniekształcania jej w jakikolwiek sposób (ta właściwość kwantowego generatora losowości QRNG jest proponowana po raz pierwszy i ma ważną rolę dla zastosowań zarówno w kryptografii kwantowej, jak i w kryptografii klasycznej).

Szczegółowy opis wynalazku w tym zakresie przedstawiono w raporcie (R-1) jak również publikacji technicznej (P-1) oraz zgłoszeniach patentowych (ZP-1 i ZP-2).

Generator Liczb Losowych (Random Number Generator, RNG) to urządzenie, które produkuje liczby losowe, zwykle kodowane jako sekwencje bitów 0 i 1 tworzących ramy logiczne komputerowych i komunikacyjnych architektur.

Generatory liczb losowych zwykle dzielone są na dwie klasy: generatory pseudolosowe (Pseudo RNG, PRNG) i generatory prawdziwie losowe (True RNG, TRNG) w oparciu o procesy fizyczne stanowiące podstawę generacji losowości. Większosc obecnie używanych generatorów liczb losowych to urządzenia oparta na procesach deterministycznych i klasycznym (również deterministycznym) chaosie - stanowi to oparcie generacji losowości na klasycznych prawach fizyki. W przypadku pseudolosowych generatorów (PRNG), uzyskiwana losowość nie jest prawdziwa będąc w pełni zależną od złożoności układu w ramach którego odbywa się fizyczny proces generowania losowości, która w takiej sytuacji może być przewidziana przy założeniu posiadania wystarczającej wiedzy nt. warunków początkowych układu fizycznego a także mocy obliczeniowej do symulowania jego zachowania. Jako że układy makroskopowe stanowiące tego typu pseudolosowe generatory PRNG podlegają prawom fizyki klasycznej, które są w pełni deterministyczne, nawet jeśli bardzo złożone i pozornie nieprzewidywalne, to jednak wystarczająco zaawansowana technologia może w zasadzie odtworzyć fizyczną ewolucję takiego generatora RNG oraz jego oddziaływanie z otoczeniem i w ten sposób przewidzień generowany ciąg losowy. Przykładem tego typu pseudolosowych generatorów są procesory komputerów klasycznych, które mogą generować pseudolosowe ciągi w relacji do ich determnistycznego reżimu działania przy użyciu złożonych algroytmów (algorytm parametryzuje się tzw. liczbą inicjującą, która jest przekształcana w skomplikowany sposób do nowej pseudolosowej liczby).

Inna klasa generatorów liczb losowych to generatory prawdziwie losowe (True RNG, TRNG), w których losowość jest absolutna. Pojęcie absolutnej lub całkowitej losowości jest ściśle ekwiwalentne z cechą całkowicie niedeterministycznej ewolucji układów fizycznych, które tworzą prawdziwie losowy generator. Jednakże prawdziwie niedeterministyczna ewolucja charakteryzuje tylko układy kwantowo-mechaniczne i w bardziej precyzyjnym sformułowaniu obecna jest tylko i wyłącznie w pomiarze kwantowym stanów tych układów. Dlatego prawdziwie losowe generatory TRNG są w istocie równoważne generatorem kwantowym (Quantum RNG, QRNG), które odnoszą się do klasy generatorów losowości, w których absolutna, tj. zrównoważona i nieprzewidywalna losowość jest oparta na fundamentalnych prawach mechaniki kwantowej, a nie prawach fizyki klasycznej.

Istotnym jest również nadmienić, że czasem używany jest inny podział klasyfikujący generatory losowości RNG: różnicując programowe (Software RNG, SRNG) wobec sprzętowych generatorów (Hardware RNG, HRNG). Klasycznie rozumiane programowe generatory (SRNG) oparte są na urządzeniach deterministycznie przetwarzających informację (np. na klasycznych komputerach lub innych klasycznych układach elektronicznych) i w związku z tym są zawsze generatorami pseudolosowymi (PRNG). Jednakże można również rozważać programowe generatory SRNG oparte na algorytmach komputerów kwantowych, i jako takie SRNG będą mogły dostarczyć prawdziwej losowości stając się generatorami TRNG (a w istocie generatorami QRNG). Z drugiej strony generatory sprzętowe (HRNG) dzielone mogą być jedynie w odniesieniu do fizycznych (a nie algorytmicznych) implementacji procesów stanowiących źródło losowości, w związku z czym mogą również pseudolosowymi generatorami PRNG (jeśli opierają się na deterministycznych klasycznych układach) lub prawdziwymi generatorami losowości TRNG/QRNG (jeśli oparte są na niedeterministycznych, prawdziwie losowych procesach, tj. procesach kwantowych). Dlatego poprawnym i racjonalnym podziałem generatorów losowości RNG jest odniesienie do ich klasyczności (pseudolosowe generatory PRNG) lub kwantowości (prawdziwie losowe generatory TRNG/QRNG).

Dlatego rozważanie splątania kwantowego jako fundamentalnego układu prawdziwie niedeterministycznych kwantowych generatorów losowości QRNG ma istotne znaczenie dla autorów koncepcji i w tym kontekście uzasadnionym jest zaproponowany nowy protokół QRNG oparty skorelowanych i antykorbowalnych stanach Bella, ponieważ samo splątanie kwantowe wydaje się być podstawą prawidłowego określenia informacji kwantowej, która w tym ujęciu składa się raczej z nieklasycznych, nielokalnych korelacji (naruszających klasyczne nierówności Bella w statystykach, a

także posiadających ujemną warunkową entropię [5], alternatywnie formułowaną jako pojęcie informacji częściowej [6] obecne tylko dla informacji kwantowej, mierzącej ilość klasycznyej informacji, która może być nadmiarowo przekazywana w supergęstym protokole kodowania [7], z maksymalnym limitem dla splątanych stanów Bella równym jednemu dodatkowemu bitowi informacji o stopniu na każdym 1 bit kodowany na przekazywanym 1 qubicie (kodowanie 2 bitów na 1 qubicie za pomocą lokalnych na nim operacji przy założeniu, że jest on maksymalnie splątany w stanie Bella z innym później mierzonym qubitem).

Główną cechą splątania jest jego zasadniczo nielokalny charakter jako zjawiska fizycznego. Dlatego też jest to jakościowo inny zasób w kontekście problemu dekoherencji kwantowej niż lokalny czysty stan np. pojedynczego qubitu, ponieważ dekoherencja z powodu lokalnego uwarunkowania oddziaływania fizycznego ma zasadniczo lokalny charakter [8, 9]. W ramach problematyki przeciwdziałania dekoherencji, poza standardowymi metodami kwantowej korekcji błędów według koncepcji Shora [10], zaawansowane wielocząstkowe stany splątane są jedną z możliwych opcji [11] dla zapewnienia odporności na dekoherencję co jest oczywiste, jeśli rozważyć np. uogólnienie 3-qubitów stanów splątanych W: $\frac{1}{\sqrt{n}}\left(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle\right)$ (tylko jeden stan $|1\rangle$ w nieseparowalnym tensorowym iloczynie n-qubitów). W takim przypadku lokalna dekoherencja jednego z splątanych n qubitów nie spowoduje żadnego znaczącego odchylenia dla stanu całego układu, a w szczególności nie zmieni stopnia zmieszania jakiegokolwiek innego qubitu indywidualnego (dekoherujący qubit w najgorszym przypadku całkowitej dekoherencji po prostu oddzieli się od całego splątanego stanu W, pozostawiając go w stanie qubitów n-1 niewiele odbiegającym od pierwotnej konfiguracji, szczególnie gdy n jest duże: $\frac{1}{\sqrt{n-1}}\left(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle\right)$ (ponownie symetryczna konfiguracja tylko jednego stanu $|1\rangle$ w nieseparowalnym względem iloczynu tensorowego stanie n-1 qubitów). W związku z ogólną koncepcją nielokalności vs. lokalnek dekoherencji [12], ostatnio dostrzegalne jest duże zainteresowanie rozważaniem informacji kwantowej opartej na topologicznych stopniach swobody [13–15], co naturalnie dotyczy uwzględnienie topologicznego charakteru splątania kwantowego, a tym samym podkreśla rolę prezentowanego wynalazku.

Można rozważyć następującą formalizację protokołu, który nazwiemy splątaniowych kwantowym generatorem losowości z publicznym dowodem losowości::

1. Załóżmy, że Alicja posiada generator opisany powyżej.
2. Alicja w sposób ciągle powtarzany inicjuje układ kwantowy przedstawiony na Fig. 3 stanem wejściowym $|000\rangle_{ABC}$.
3. Po każdej inicjalizacji Alicja przeprowadza pomiar kwantowy na qubicie A i zachowuje dla siebie w tajemnicy wynik pomiaru (sekwencję uzyskanych tajnych wyników ww. pomiaru nazwiemy A_i). Tylko Alicja ma wiedzę na temat konfiguracji splątania, która została losowo wybrana dla każdej generowanej pary.
4. W rezultacie zostaje wygenerowany ciąg splątanych par qubitów B i C, ze splątaniem definiowanym przez elementy ciągu A_i (cf. Fig. 5), w następujący sposób:
   - $0 \rightarrow \frac{|00\rangle_{BC}+|11\rangle_{BC}}{\sqrt{2}}$ – stan skorelowany,
   - $1 \rightarrow \frac{|01\rangle_{BC}+|10\rangle_{BC}}{\sqrt{2}}$ – stan antyskorelowany.
5. Następnie Alicja wykonuje pomiar na qubitach w każdej parze, czego wynikiem są dwa ciągi bitowe:
   - B_i – ciąg losowych bitów wynikający z pomiaru qubitu B dla każdej pary,
   - C_i – ciąg losowych bitów wynikający z pomiaru qubitu C dla każdej pary (w istocie nie jest koniecznym dokonywanie pomiaru qubitu C, jako że ciąg B_i i A_i definiują ciąg C_i w sposób jednoznaczny).
6. Alicja kończy protokół z trzema równej długości ciągami bitowymi:
   - A_i – ciągiem określającym losowo typy splątania wybranej dla każdej pary
   - B_i i C_i – wzajemnie skorelowane, wartościami ciągu A_i, losowe ciągi.

Dla kogoś kto nie posiada wiedzy o konfiguracjach splątania wybranych dla każdej pary, ciągi B_i i C_i są całkowicie losowe i przewidzenie bitów jednego z nich na podstawie drugiego jest niemożliwe w takiej sytuacji. Z drugiej strony, dla Alicji, z tych trzech ciągów (B_i, C_i oraz ciągu konfiguracji splątaniowych A_i) tylko dwa (i dowolne dwa) przedstawiają losową informację.

Jednak najważniejszą kwestią jest że dowolne dwa ciągi, np. B_i i C_i muszą posiadać identyczne właściwości statystyczne (z powodu splątaniowych korelacji lub antykorelacji), i ta cecha jest kluczowa w proponowanym wynalazku umożliwiając Alicji zastosowanie publicznej weryfikacji losowości.

Ponieważ zawsze istnieje wątpliwość, czy wygenerowana sekwencja jest prawdziwie losowa, czy nie, zarówno w przypadku klasycznym, jak i kwantowym (w klasycznym przypadku wątpliwość ta może być adresowana do problemu definicji samej losowości, a w przypadku kwantowym odpowiada różnicom interpretacyjnym mechaniki kwantowej pomiędzy koncepcją pomiaru von Neumanna opartą na obiektywnym prawdopodobieństwie częstotliwościowym a teorią Kwantowego Bayesjanizmu Fuchsa, tzw. QBismem, opartą na raczej subiektywnym prawdopodobieństwie warunkowym [16, 17], np. omówionym w Ref. 1)—statystyczne testowanie losowości oferuje pewną weryfikację. Ale z testowaniem losowości wiąże się podstawowy problem - brak uniwersalnej definicji losowości i jej charakterystyk, a w związku z tym zestawu testów. W rzeczywistości istnieje nieskończona liczba różnych testów dopasowania wzorca, ponieważ istnieje nieskończona liczba wzorów.

Dlatego kompleksowe testowanie może być bardzo zasobochłonne, a na ogół niedostępne do wdrożenia w zminiaturyzowanych rozwiązaniach generatorów liczb losowych. Z drugiej strony wysoce pożądana jest losowość wysokiej jakości do aplikacji kryptograficznych (sekrety początkowe, wektory inicjujące, kryptograficzne noncje tj. wyrażenia okazjonalne, itd.). Proponowany protokół może być użyty do przeniesienia ciężaru testów losowości z urządzenia generującego lub użytkownika na pewną zewnętrzną stronę publiczną (która może mieć nieograniczone zasoby obliczeniowe w porównaniu do pojedynczego użytkownika / generatora).
W związku z powyższymi uwagami dalsze etapy proponowanego protokołu można przedstawić w następującym scenariusz użycia:

7. Alicja wątpiąca w losowość ciągu B_i publicznie wysyła ciąg C_i do centrum weryfikacji (VC).
8. VC publicznie wykonuje serię zasobo-chłonnych prób losowości, decydując, czy sekwencję C_i można uznać za prawdziwie losową czy nie.
9. VC publicznie informuje Alicję o swojej decyzji.
10. W przypadku pozytywnej decyzji Alicja zyskuje pewność, że sekwencja B_i pozostająca w utajnieniu jest również prawdziwie losowa.

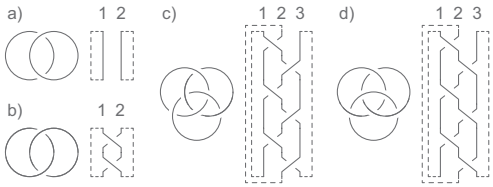
W tym protokole Alicja może przeprowadzić własne testowanie początkowej losowości i użyć VC do usprawnienia procedury testowania. Ze względu na specyficzny sposób generowania ciągów B_i i C_i, publiczne ogłoszenie jednego z nich nie wpływa na tajność drugiego. Publiczny charakter procedury badania losowości VC służy jako gwarancja przeciwko oszustwom - decyzja VC może być zweryfikowana przez dowolną inną stronę publiczną (ogólnie Alicja może jednocześnie używać wielu VC w celu zwiększenia precyzji przekazanej jej decyzji).
Warto wspomnieć, że VC może być ewentualnie wyposażony w komputer kwantowy, który może być użyty do sprawdzenia, czy proces generowania jest rzeczywiście losowy lub stronniczy (na przykład przez obecność klasycznego, a tym samym deterministycznego wpływu na proces generowania).
Proponowany protokół oferuje losowość potwierdzoną przez klasyczne testy statystyczne przeprowadzone publicznie. Tutaj losowość kwantowa ma podwójny charakter – wynika z pomiaru kwantowego, który wybiera skorelowany lub antyskorelowany stan splątania pary qubitów oraz pomiaru odplątującego w ramach tej pary. Alicja, losowo wykonująca weryfikację istnienia splątania, próbuje sprawdzić, czy kwantowe źródło entropii jest dobrej jakości, czy też nie. W tym kontekście protokół można uznać za członka szerokiej klasy tzw. Device Independent RNG [18, 19], które są również weryfikowane statystycznie, ponieważ proces ich generowania można uznać za stronniczy. W proponowanym przypadku rozważana losowość kwantowa jest oparta na kwantowym pomiarze, ale odchylenie może odpowiadać tutaj nie tylko niedoskonałościom implementacji, jak rozważono dla niezależnej od urządzenia koncepcji RNG [18, 19], ale także nietrywialnemu problemowi wprowadzenia subiektywizmu do pomiaru kwantowego z powodu zakwestionowania poprawności wykorzystania częstościowego prawdopodobieństwa w koncepcji pomiaru von Neumanna zamiast warunkowego prawdopodobieństwa opisanego w teorii Kwantowego Bayesjanizmu [16, 17]. Ponieważ pomiar kwantowy w jego fundamentach jest niepowtarzalny i niszczycielski, a zostosowanie ma twierdzenie o zakazie klonowania informacji kwantowej [20], koncepcja opisania pomiaru z prawdopodobieństwem częstościowym jest istotnie problematyczna. Niezależnie jednak od charakteru błędu (podstawowego lub implementacyjnego) proponowany protokół pozwala na wykonywanie niedostępnych w standardowym przypadku, w wyniku nieefektywności obliczeniowej, jednoczesnych (przy użyciu wielu wirtualnych centrów weryfikacji VC) testów losowości na dużych blokach danych (zamiast raczej krótkich bloków w standardowych testach, na przykład w pakiecie testów NIST [21]).
Problem analizy entropii źródła losowości jest z pewnością kluczowy dla niedoskonałych fizycznych implementacji kwantowych generatorów losowych (np. [19, 22]). Niektóre podejścia są ograniczone do określonych technik generowania i konfiguracji [19, 23, 24]. Bardziej uniwersalnymi podejściami są koncepcje niezależnego urządzenia RNG [18, 25], w którym niektóre protokoły wyodrębniają kwantową losowość i odrzucają deterministyczne zachowanie [26, 27] ze względu na niedociągnięcia w implementacji procesów kwantowych. Samo-testujące protokoły QRNG są również uważane za część podejścia niezależnego od urządzenia, na przykład w Ref. 28, gdzie testowanie wymiarów niescharakteryzowanych systemów klasycznych i kwantowych umożliwia obserwatorowi oddzielenie części kwantowej losowości od deterministycznej części klasycznej, co skutkuje bardzo wysokim poziomem ufności 99% wygenerowanych bitów [28]. Jednak podstawowa kwestia typu prawdopodobieństwa w ramach schematu pomiarowego von Neumanna wciąż może być tu kwestionowana. Mając to na uwadze, koncepcja nieograniczonego przez zasoby testowania klasycznych korelacji wydaje się być interesującym krokiem ku prawdziwej lub "bezwarunkowej" losowości w rzeczywistym układzie, który może zostać podniesiony do dowolnego pożądanego poziomu (podobnie jak teoretyczne bezwarunkowe bezpieczeństwo kwantowej dystrybucji klucza w fizycznym wdrożeniu może zostać zwiększone do dowolnego referencyjnego poziomu).

Opis rysunków technicznych

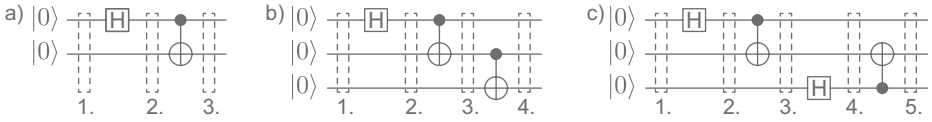
[Rys. 1] Prosty model topologiczny odpowiadający nieekwiwalentności topologicznej podstawowych typów konfiguracyjnych splątania dwuwymiarowych układów kwantowych (qubitów). Jako że elementy grup warkoczowych są w istocie zamkniętymi pętlami, linie przerywane zostały dodane dla jasności.

[Rys. 2] Przykładowe podstawowe obwody kwantowe przedstawiające schematy generacji topologicznie nieekwiwalentnych typów konfiguracyjnych splątania. Oddzielone obszary przedstawiają kolejne kroki ewolucji kwantowego obwodu.
[Rys. 3] Schemat bramek kwantowych generatora losowych korelacji splątaniowych z 2-qubitowym stanem splątanym i pojedynczym dodatkowym qubitem X. Bez (a) lub z (b,c) losowym wyborem typu 2-qubitowego stanu splątaniowego. Podwójna linia reprezentuje informację klasyczną związaną z wynikiem pomiaru kwantowego.
[Rys. 4] Schematyczne elementy protokołu splątaniowego kwantowego generatora liczb losowych z publicznym dowodem losowości: a) generacja losowych korelacji; b) typy korelacji; c) możliwe wyniki pomiarowe.
[Rys. 5] Obwód kwantowy z bramkami generatora losowych korelacji splątaniowych z 3-qubitowym stanem splątanym i dwoma dodatkowymi qubitami X i Y. Rozszerzenie protokołu (zwiększone bezpieczeństwo wielokrotnej zgody) jest uzyskiwane poprzez losowy wybów typu 3-qubitowego stanu splątanego, co jest pominięte w przypadku (a) i uwzględnione w przypadkach (b,c). Podwójna linia reprezentuje klasyczną informację dotyczącą wyników pomiarów.
[Rys. 6] Schemat bramek kwantowych dla generatora losowych korelacji splątaniowych z 4-qubitowym splątaniem i trzema dodatkowymi qubitami X, Y i Z. Bez (a) i z (b,c) losowym wyborem typu 4-qubitowego stanu splątanego. Podwójna linia reprezentuje klasyczną informację dotyczącą wyników pomiarów.

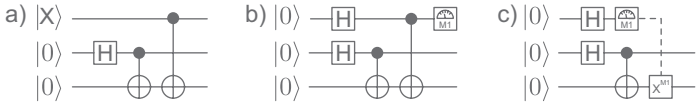
Rysunki techniczne



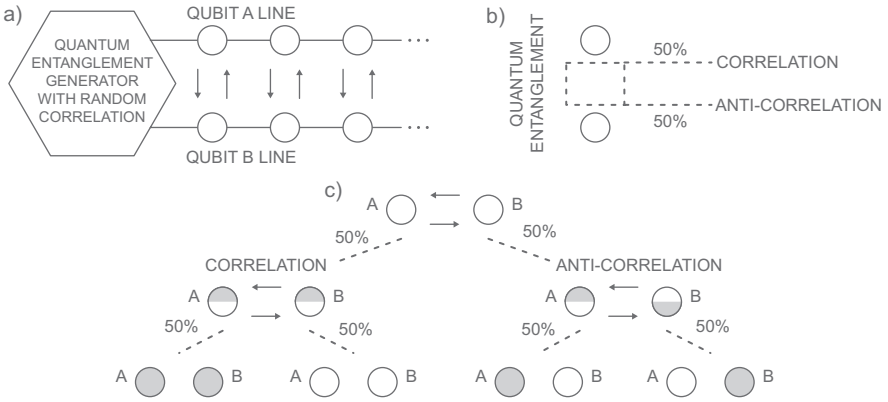
Rysunek 1.



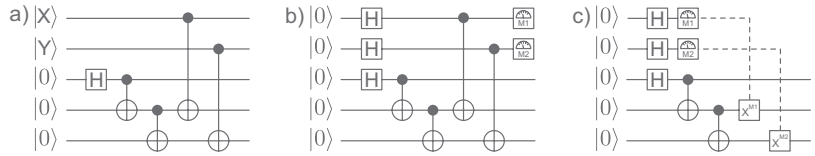
Rysunek 2.



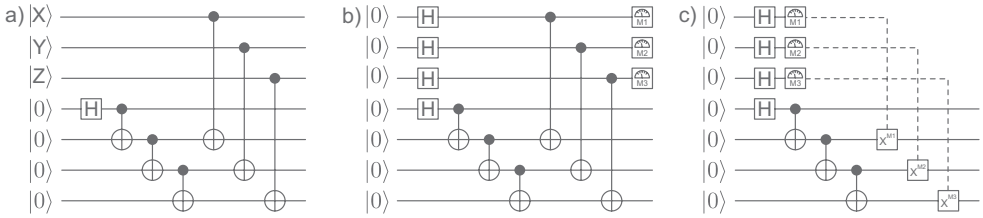
Rysunek 3.



Rysunek 4.



Rysunek 5.



Rysunek 6.

IV. Modele testowania i parametryzowania statystycznego losowości

Ostatnim obszarem wyników badawczych była dziedzina testowania empirycznego losowości ciągów bitowych. W tym obszarze przeprowadzono badania teoretyczno-analityczne oraz wstępne badania empiryczne, których kontynuację przewidziano w etapie 2 projektu w zakresie charakteryzowania poszczególnych źródeł kwantowej losowości. Wyniki badań w tym obszarze przedstawiono w raporcie (R-1) oraz publikacji technicznej (P-3) (dane źródłowe i analityczne testowania losowości generowanych laboratoryjnie ciągów udokumentowano w zasobach elektronicznych W-1). Podsumowując, w ramach metodologii testowania losowości ciągów generowanych kwantowo i klasycznie za podstawę modelu przyjęto zgodnie z założeniami projektowymi metody testowania hipotez, jak również teorię losowości opartą na kompressji i złożoności obliczeniowej Kołmogorowa (1965) jak również w oparciu transformację Hadamarda-Walsha (Kak, 1971 i Philips, 1972) dla szybkiej analizy w obrazie transformaty Fouriera rozkładów spektralnych ciągów losowych. W ramach modelu testowania statysznego generacji losowości wykorzystano również późniejsze osiągnięcia w dziedzinie badań podstawowych nad problematyką definicji losowości i jej weryfikacji (tj. zwłaszcza rezultaty badań Chaitina, Bennetta, Yuena, Hopkinsa, Marsaglii, Zamana publikowane w latach 1975-1995), w tym zawarte w otwartych bibliotekach programistycznych (Diehard - Marsaglia 1995, Dieharder - Brown 2004, TestU01 - Lecuyer 2007, jak również NIST 2010). W tym miejscu należy również przypomnieć, że analiza i weryfikacja prawdziwej losowości generowanych jako losowe ciągów bitowych jest procesem o bardzo dużej złożoności obliczeniowej (jeśli ciągi nie zawierają jakiś elementarnych odchyleń od losowości, co oczywiście nie ma miejscu w przypadku generatorów liczb losowych, nawet klasycznych) – w ramach badań zatem wykorzystywano zaawansowane koncepcje testów w zakresie algorytmiki konsumujące ogromne zasoby obliczeniowe. Prowadzenie wstępnych badań w tym zakresie (planowanych do rozszerzenia w kierunku faktycznej parametryzacji różnych źródeł kwantowych) wymaga dużych mocy obliczeniowych, które w projekcie umożliwione były zakupem aparatury zaawansowanego klastra obliczeniowego. Ponownie dodać można jednak, że wobec istotnego rezultatu koncepcyjnego etapu 1 projektu w postaci protokołu EQRNG z publicznym poświadczeniem losowości, optymalność testowania poziomu losowości ciągów bitowych generowanych splątaniowo według tego protokołu przy ujawnieniu jednego z nich (i pozostawieniu drugiego tajnym) nie jest kwestią zasadniczej wagi. Podlegające poniżej przedstawionym analizom metody realizacji testów losowości będą wykorzystane do faktycznych badań losowych ciągów generowanych w różnych procesach kwantowych zgodnie z założeniami projektu w etapie 2.

Efektem końcowym realizacij etapu 1 jest przede wszystkim opracowana w toku realizacji projektu nowatorska koncepcja modelu publicznego poświadczania losowości ciągów bitowych generowanych w procesach kwantowych opartych na splątaniu wieloqubitowym, przy wykorzystaniu najważniejszych opisanych poniżej metod testowania losowości, w tym obarczonych dużą konsumpcją zasobów obliczeniowych. Generowane w procesach kwantowych ciągi losowe powinny charakteryzować się esktramalnie niskimi odchylenia entropii od wartości maksymalnych na poszczególnych pozycjach bitowych – odchylenia te mogą być rzędu nawet 2^{-64} tj. rzędu 10^{-20} (wykrycie tak niewielkich odchyleń statystcznych w entropii wymaga ogromnej zasobochłonności analiz statycznych). W toku poniżej zreferowanych badań przemysłowych w zakresie metod testowania losowości zidentyfikowano i scharakteryzowane najważniejsze z tzw. baterii testów losowości, stanowiących szeroko przyjęty i upowszechniony w specjalistycznych zastosowań (zwłaszcza kryptograficzny) matematyczny standard referencyjny dla weryfikacji poziomu losowości.

Literatura

[1] Andrei Khrennikov. Randomness: quantum versus classical. *Int. J. Quantum Inform.*, 14:1640009, 2016.
[2] L. Landau and L. Lifschitz. *Machanika kwantowa, teoria nierelatywistyczna.* PWN, 2012.
[3] N. David Mermin. Physics: QBism puts the scientist back into science. *Nature*, 507:421–423, 2014.
[4] J. von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton Univ. Press, Princeton, 1955.
[5] N. J. Cerf and C. Adami. Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, 79:5194–5197, 1997.
[6] Michal Horodecki, Jonathan Oppenheim, and Andreas Winter. Partial quantum information. *Nature*, 436:673, 2005.
[7] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.
[8] Wojciech Hubert Zurek. Decoherence, einselection, and the quantum origins of the classical. *Rev. Mod. Phys.*, 75:715–775, 2003.
[9] L. Jacak, J. Krasnyj, W. Jacak, R. Gonczarek, and P. Machnikowski. Unavoidable decoherence in semiconductor quantum dots. *Phys. Rev. B*, 72:245309, 2005.
[10] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, 1995.
[11] A. Borras, A. P. Majtey, A. R. Plastino, M. Casas, and A. Plastino. Robustness of highly entangled multiqubit states under decoherence. *Phys. Rev. A*, 79:022108, 2009.
[12] Paolo Zanardi and Seth Lloyd. Topological protection and quantum noiseless subsystems. *Phys. Rev. Lett.*, 90:067902, 2003.
[13] Sankar Das Sarma, Michael Freedman, and Chetan Nayak. Topologically protected qubits from a possible non-abelian fractional quantum hall state. *Phys. Rev. Lett.*, 94:166802, 2005.
[14] Chetan Nayak, Steven H. Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80:1083–1159, 2008.
[15] A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303:2–30, 2003.
[16] N. David Mermin. Physics: QBism puts the scientist back into science. *Nature*, 507:421—423, 2014.
[17] Christopher A. Fuchs and R´udiger Schack. Quantum-Bayesian coherence. *Rev. Mod. Phys.*, 85:1693–1715, 2013.
[18] Matej Pivoluska and Martin Plesch. Device independent random number generation. *Acta Phys. Slovaca.*, 64:600–663, 2014.
[19] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *Quantum Inf.*, 2:16021, 2016.
[20] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.
[21] 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. *Natl. Inst. Stand. Technol. Spec. Publ.*, 2010. 800-22rev1a http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.
[22] N. Nisan and A. Ta-Shma. Extracting randomness: a survey and new constructions. *J. Comp. Sys. Sci.*, 58:148–173, 1999.
[23] D. Frauchiger, R. Renner, and M. Troyer. True randomness from realistic quantum devices. *ArXiv e-prints*, 2013. arXiv:quant-ph/1311.4547.
[24] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A*, 87:062327, 2013.
[25] Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna. Quantum cryptography: Key distribution and beyond. *Quanta*, 6:1—-47, 2017.
[26] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021—-1024, 2010.
[27] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, , and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406, 2013.
[28] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, , and Nicolas Brunner. Self-testing quantum random number generator. *Phys. Rev. Lett.*, 114:150501, 2015.