Kraków, 18.03.2022

Recenzja osiągnięcia naukowego oraz dorobku dr Jędrzeja Kaniewkiego w związku z postępowaniem o nadanie stopnia doktora habilitowanego

Dr Jędrzej Kaniewski uzyskał stopień nauk fizycznych w grudniu 2015 roku, na podstawie pracy doktorskiej pt. "Relativistic quantum cryptography". Stopień został przyznany przez Narodowy Uniwersytet w Singapurze. W 2011 roku, habilitant ukończył czteroletnie studia na Uniwersytecie w Cambridge.

Obecnie, od lipca 2019 roku, dr Kaniewski jest zatrudniony na stanowisku adiunkta na Wydziale Fizyki Uniwersytetu Warszawskiego. Wcześniej, przez okres roku czasu, był on zatrudniony jako adiunkt w Centrum Fizyki Teoretycznej Polskiej Akademii Nauk, w ramach programu POLONEZ z NCN. Przed przyjazdem do Polski, w okresie od stycznia 2016 do czerwca 2018, dr Kaniewski odbył staż podoktorski na Wydziale Matematyki, na Uniwersytecie w Kopenhadze.

Recenzja osiągnięcia naukowego

Tematyka osiągnięcia habilitacyjnego dotyczy wybranych teoretycznych aspektów samotestowaniem układów kwantowych. Zagadnienie to ma bezpośrednie znaczenie z punktu widzenia certyfikacji kwantowości. Certyfikacja taka jest szczególnie ważna w przypadku, kiedy nie dysponujemy pełną widzą na temat danego układu kwantowego, a chcemy potwierdzić poprawność jego działania, zgodną z zasadami mechaniki kwantowej. Przykładów takich sytuacji dostarcza kwantowa generacja losowości (Quantum Random Number Generation - QRNG), kwantowa dystrybucja klucza (Quantum Key Distribution - QKD), czy też weryfikacja poprawności działania komputerów kwantowych. W przypadku kryptografii, do której metod zaliczyć można również generowanie losowości, certyfikacja nabiera ogromnego znaczenia, rzutując na poziom bezpieczeństwa danego rozwiązania. W szczególności, samotestowanie układów kwantowych dostarcza teoretycznej metody potwierdzenia kwantowej natury generowanego, z wykorzystaniem splatania kwantowego, ciągu losowego. Jednakże, z uwagi na wyzwania eksperymentalne (w szczególności, wyeliminowanie możliwości istnienia klasycznych korelacji, wynikających z istnienia tzw. detection loophole dla fotonów) nie doczekaliśmy się, jak dotąd, praktycznych implementacji tego podejścia.

Istotną cechą metody samotestowania układów kwantowych jest abstrahowanie od szczegółów technicznych danego układu/urządzenia kwantowego. Podejście to, realizowane na zasadzie "czarnej skrzynki", nosi nazwę *niezależności od urządzenia* (Device Independence - DI). Jest to podejście szczególnie pożyteczne w przypadku, kiedy dane urządzenie kwantowe pochodzi z nieautoryzowanego źródła, a chcemy je wykorzystać w celach wymagających certyfikacji poziomu bezpieczeństwa. Warto w tym miejscu podkreślić, że jest to sytuacja która nie ma swojego odpowiednika w przypadku klasycznym i wiąże się bezpośrednio z nielokalnymi korelacjami, obserwowanymi dla stanów splątanych. Możliwość zastosowania

tego podejścia w obszarze kryptografii, poprzez ideę DIQKD, została przedstawiona przez D. Mayersa i A. Yao w 1998 roku, dając równocześnie początek kierunkowi badań nad samotestowaniem układów kwantowych.

Wyniki otrzymane przez dr Kaniewskiego stanowią wyraźny przyczynek do rozwoju tego kierunku badawczego. Warte podkreślenia jest to, że przeprowadzone rozważania teoretyczne, mogą, w przyszłości, znaleźć zastosowanie przy tworzeniu protokołów komunikacji kwantowej (np. DIQKD), generatorów losowych typu DIQRNG, czy też przy rozwoju innych technologii kwantowych. Pewne przykłady takich zastosowań można znaleźć w przedstawionym osiągnięciu naukowym.

Dla kompletności dyskusji tych wyników, należy jednak wcześniej przywołać kilka obserwacji, do których będziemy się odwoływać. Przede wszystkim, istota samotestowania wiąże się nieodzownie z korelacjami kwantowymi, występującymi dla stanów splątanych. Dla przypadku dwóch splątanych kubitów, stosowaną powszechnie miarą tych korelacji jest tzw. parametr Clausera-Hornea-Simonyego-Holta(CHSH)-Bella, który możemy zapisać jako:

$$\beta = \sum_{a,b,x,y} c_{abxy} P(a,b|x,y), \tag{1}$$

gdzie c_{abxy} są pewnymi współczynnikami, a i b są wynikami pomiarów wykonanych na pierwszym i drugim kubicie, natomiast x i y są odpowiednio parametrami określającymi ustawienia (np. baza pomiarowa) dla tych kubitów. $P(a,b|x,y)$ jest prawdopodobieństwem warunkowym. Zgodnie z istotą DI, wyrażenie na parametr β nie odwołuje się do szczegółów urządzenia eksperymentalnego, a jedynie do pewnych wielkości kontrolnych oraz do wyników pomiarów.

Dla korelacji klasycznych pomiędzy kubitami, zachodzi nierówność CHSH-Bella $\beta < 2$. Nierówność ta jest łamana, jeśli pomiędzy podukładami występuje splątanie kwantowe. Maksymalna wartość łamania jest równa $\beta = 2\sqrt{2} \approx 2.83$ (tzw. ograniczenie Tsirelsona), co jest spełnione dla stanów Bella, będących szczególnym przypadkiem stanów maksymalnie splątanych. Idea samotestowania opartego na nierówności CHSH-Bella polega na określeniu stanu kwantowego (z dokładnością do transformacji lokalnych), na podstawie wykonania pomiarów prawdopodobieństw warunkowych $P(a,b|x,y)$ i wyznaczeniu wartości parametru β. W większości przypadków jednak, samotestowanie (certyfikowanie) stanu wymaga maksymalnego łamania nierówności Bella. Jednakże, w praktyce, w wyniku obecności zarówno szumów eksperymentalnych, jak i skończonej statystyki pomiarowej, obserwowane wartości parametru β są niższe. Pytaniem jest zatem, jakie wartości parametru β, niższe od ograniczenie Tsirelsona, wciąż pozwalają na samotestowanie (certyfikowanie) nieklasyczności układu kwantowego?

Dr Kaniewski, w przedstawionym osiągnięciu naukowym, podejmuje to ważne zagadnienie, które ma zasadnicze znaczenie od strony praktycznej realizacji samotestowania. W szczególności, analizuje on przy jakim poziomie wartości parametru β, możliwe jest przeprowadzenie certyfikacji stanu kwantowego [1,4,6,8]. Dr Kaniewski rozszerza również analizę na przypadki zawierające większą ilość stopni swobody oraz wyżej-wymiarowe (niż kubit)

kwantowe stopnie swobody. Schemat samotestowania oparty na łamaniu nierówności Bella może być uogólniony przez wykorzystanie znanych wyżej-wymiarowych uogólnień nierówności Bella [7]. Jednakże, prace habilitanta pokazują, że nie jest to jedyne możliwe podejście i proponuje alternatywny schemat samotestowania, oparty o tzw. scenariusz "przygotuj-i-zmierz" [3,5]. W zależności od przeznaczenia, możliwe jest również wykorzystanie uogólnień nierówności Bella, takich jak te dla przypadku baz wzajemnie nieobciążonych (Mutually Unbiased Basses - MUB), które odgrywają szczególną rolę w kryptografii kwantowej. Habilitant, wraz ze współpracownikami, konstruuje konkretne propozycje takich uogólnień i dyskutuje je w kontekście możliwych zastosowań [7,9]. Należy również dodać, że metoda samotestowania dotyczyć może nie tylko stanów ale również operatorów rzutowych, związanych z otrzymanymi wynikami pomiarów (parametry a i b). Również ta kwestia jest eksplorowana w publikacjach dr Kaniewskiego [2,3].

W skład osiągnięcia naukowego dr Jędrzeja Kaniewskiego wchodzi 9 oryginalnych prac naukowych, opublikowanych w następujących czasopismach: Physical Review A [IF=3.989] (4 artykuły), Physical Review Letters [IF=9.161] (2 artykuły), Quantum [IF=6.777] (1 artykuł), Physical Review Research [IF - brak] (1 artykuł), Science Advances [IF=14.136] (1 artykuł).

Artykuł [1] jest publikacją jednoautorską, która ukazała się w renomowanym czasopiśmie Physical Review Letters. Na podstawie Google Scholar, artykuł był cytowany 104 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 66. Przedmiotem artykułu jest samotestowania maksymalnie splątanych stanów dwukubitowych (stany Bella) oraz stanów 3-kubitowych (stan GHZ). W tym pierwszym przypadku, testowanie opiera się na nierówności CHSH-Bella, natomiast w tym drugim, na nierówności Mermina. W przypadku, 2-kubitowym, habilitant pokazał, że istnieje niższa niż do tej pory znana wartość parametru β, zapewniająca certyfikację stanu kwantowego, równa $\beta \approx 2.11$. Publikacja jest uzupełniona materiałami, zawierającymi szczegółowe wyprowadzenie nierówności operatorowych, na których oparte są zaprezentowane wyniki. Otrzymane wyniki, dla przypadku dwu- i trzykubitowego, otwierają perspektywę uogólnienia metody do dowolnej liczby kubitów. Jest to ważna publikacja, która spotkała się z szerokim odbiorem w środowisku naukowym. Jej wyniki stanowią ważną motywację i punkt odniesienia, dla kolejnych artykułów, wchodzących w skład osiągnięcia habilitacyjnego.

Artykuł [2] jest publikacją jednoautorską, która ukazała się w czasopiśmie Physical Review A. Na podstawie Google Scholar, artykuł był cytowany 55 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 36. Publikacja ta podejmuje istotne zagadnienie samotestowania w kontekście obserwabli kwantowych. W artykule, Autor koncentruje swoją uwagę na samotestowaniu dwóch obserwabli binarnych. Wykorzystuje on znane obserwacje dotyczące relacji komutacji pomiędzy obserwablami do wyciągnięcia wniosków odnośnie niekompatybilności pomiarów. Autor konstruuje miary, pozwalające przeprowadzić certyfikację nieznanych obserwabli binarnych. Konkluzją pracy jest obserwacja dotycząca możliwości, odpornego na szum, samotestowania pary obserwabli binarnych. Rozważane podejście zostało następnie zastosowane do rodziny nierówności MABK (Mermin-Ardehali-Belinskii-Klyshko),

dla której wykazano możliwość samotestowania obserwabli.

W nowatorskiej publikacji [3] pokazano, że idea samotestowania nie koniecznie musi opierać na nierównościach Bella, czy też jej uogólnieniach. Rozpatrzono mianowicie tzw. scenariusz "przygotuj-i-zmierz" (prepare-and-measure), dla którego, przy dodatkowych warunkach, pokazano istnienie schematu samotestowania. W rozważaniach, skupiono uwagę na przypadku kwantowego kodu losowego dostępu (Quantum Random Access Code - QRAC). Publikacja ta, powstała we współpracy z czterema współautorami i została opublikowana w czasopiśmie Physical Review A. Na podstawie Google Scholar, artykuł był cytowany 75 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 51.

Artykuł [4] jest publikacją trójautorską, która ukazała się w prestiżowym czasopiśmie Physical Review Letters. Na podstawie Google Scholar, artykuł był cytowany 35 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 24. Praca dotyczy samotestowania splątania w sieciach kwantowych, opartych na splątaniu kwantowym. Jako model takiej sieci, w artykule, rozważono układ trzech urządzeń (węzłów), dla których stany splątane są generowane przez trzy niezależne źródła. Rozważając protokół tzw. entanglement swappingu (zamiany splątania), pokazano możliwość samotestowania takiego systemu, opierając się na pomiarach w bazie Bella. Zaproponowana metoda certyfikacji pozostaje skuteczna przy pewnym poziomie szumów (do ok. 5%). Jednakże, z uwagi na obecnie zbyt niskie otrzymywane eksperymentalnie poziomy ufności dla entanglement swappingu (do 84%), zaproponowana metoda nie może być jeszcze zastosowana w praktyce. Narzucającym się rozwinięciem otrzymanego kierunku, byłoby zaproponowanie metody certyfikacji, dopuszczającej nieco wyższe poziomy szumu.

Artykuł [5] rozszerza analizę z publikacji [3] (przeprowadzonej dla kubitów) do wyżejwymiarowego przypadku kwantowych kodów losowego dostępu (QRAC). Rozważania są przeprowadzone dla przypadku stanów rozpinających MUB i wykorzystują, rozwinięty w pracy [3] scenariusz "przygotuj-i-zmierz". W rozpatrywanym przypadku, dwa klasyczne dity są kodowane w jednym kudicie. Co istotne, dla przypadków $d = 3$ i $d = 4$, certyfikacja jest możliwa przy realistycznych wartościach szumu. Pozwoliło to, na eksperymentalne potwierdzenie wyników pracy, przez inny zespół badawczy. Publikacja ta, napisana została z jednym współautorem i została opublikowana w czaspiśmie Physical Review A. Na podstawie Google Scholar, artykuł był cytowany 50 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 32.

Artykuł [6] jest rozwinięciem wyniku z pracy [1] do przypadku samotestowania stanów cześciowo splątanych dwóch kubitów (w odróżnieniu do przypadku stanu maksymalnie splątanego z artykułu [1]). W tym celu, posłużono się *przechyloną* nierównością CHSH-Bella. W rozpatrywanym przypadku, wykazano, że otrzymywana metoda samotestowania jest istotnie odporna na szum. Publikacja ta, powstała z dwoma współautorami i została opublikowana w czaspiśmie Physical Review A. Na podstawie Google Scholar, artykuł był cytowany 16 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 11.

W artykule [7], dr Kaniewski, wraz z współautorami, wprowadzają nową klasę nierówności Bella, zdefiniowanych tak aby łamanie nierówności było maksymalne dla pomiarów w

bazach wzajemnie nieobciążonych (MUB). Pokazano, że dla stanów maksymalnie splątanych, pożądana własność jest spełniona dla przypadku bazy pomiarowej o wymiarze $d \in \mathbb{P} \setminus \{2\}$, gdzie $\mathbb{P}$ jest zbiorem liczb pierwszych. W oparciu o wprowadzone nierówności, pokazano możliwość samotestowania dla przypadku $d = 3$. Z uwagi na brak stosownych analitycznych ograniczeń dla przypadku $d \notin \mathbb{P} \setminus \{2\}$, możliwość certyfikacji dla tych przypadków pozostaje nieokreślona. Publikacja ta, powstała z pięcioma współautorami i została opublikowana w bardzo dobrym czasopiśmie Quantum. Na podstawie Google Scholar, artykuł był cytowany 29 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 12.

W jednoautorskim artykule [8], dr Kaniewski wykazał istnienie nowego typu słabszej postaci samotestowania, dla którego maksymalne łamanie nierówności Bella pozwala na identyfikację stanu, bez pełnego scharakteryzowania pomiarów. Wykazano, że ta słabsza forma testowania może zostać zastosowana, w szczególności, do testowania losowości kwantowej. Otrzymane konkluzje zostały potwierdzone zarówno przez rozważania analityczne, jak i numeryczne. Publikacja ta została opublikowana w czaspiśmie Physical Review Research. Na podstawie Google Scholar, artykuł był cytowany 10 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 4.

Artykuł [9] dostarcza kolejnego ciekawego uogólnienia nierówności Bella. Otrzymana nierówność jest maksymalizowana przez pewne symetryczne konstelacje pomiarów. Rozważania prowadzone są w kontekście wzajemnie nieobciążonych baz (MUB), dostarczając sposobu samotestowania nieobciążoności. W pracy, dyskutowane jest zastosowanie otrzymanej nierówności w niezależnej od urządzeń kwantowej dystrybucji klucza (DIQKD) oraz kwantowej generacji losowości typu DIQRNG. Publikacja ta, powstała z czterema współautorami i została opublikowana w znakomitym czasopiśmie Science Advances. Na podstawie Google Scholar, artykuł był cytowany 15 razy, a na podstawie bazy Web of Science, liczba cytowań wynosi: 5. Publikacja ta jednak ukazała się stosunkowo niedawno i niewątpliwie ma jeszcze dużo większy potencjał oddziaływania na środowisko naukowe.

Reasumując, przedstawione osiągnięcie naukowe, stanowi spójny ciąg badań nad konstrukcją systematycznego podejścia do samotestowania układów kwantowych. Otrzymane rezultaty stanowią widoczny wkład w rozwój badań na samotestowaniem i certyfikacją systemów kwantowych. Przeprowadzone badania dowodzą wysokich kompetencji habilitanta w zakresie matematycznych aspektów teorii informacji kwantowej. Należy jednak zaznaczyć, że przeprowadzone rozważania, od strony matematycznej, nie wychodzą znacząco poza ramy algebry liniowej. Pomimo tego, wymagają jednak dużej pomysłowości i biegłości obliczeniowej.

Motywacja do przeprowadzonych badań ma swoje źródło głównie w opracowywanych obecnie i już wdrażanych rozwiązaniach w zakresie technologii kwantowych. W szczególności, należą do nich: DIQKD, DIQRNG oraz sieci kwantowe oparte na splątaniu kwantowym. Pomimo tych silnych relacji, dyskusje przeprowadzone w ramach artykułów koncentrują się na aspektach czysto teoretycznych (lub wręcz matematycznych) a odwołania do strony eksperymentalnej mają przeważnie jedynie charakter motywacji i są śladowe. Wyjątkiem jest tu praca [9], w której znaleźć można bardziej rozbudowaną analizę zastosowań do DIQKD i

DIQRNG.

Z punktu widzenia możliwości empirycznej weryfikacji niektórych z rozważanych schematów certyfikacji w nieodległej przyszłości, można mieć nadzieję, że habilitant zbliży swoje dalsze rozważania do obszaru doświadczalnego. Szkoda również, że przeprowadzone rozważania nie doprowadzają (poza kilkoma szczególnymi przypadkami) do jawnych związków pomiędzy dolnym ograniczeniem na wierność (fidelity) testowanego stanu a wartością mierzonego parametru testującego (np. β). Taka zależność pozwoliłaby lepiej zrozumieć to, jak różnice w wyznaczeniu parametru β tłumaczą się na poziom samotestowania stanów.

Od strony związku teorii z doświadczeniem, należałoby również przeprowadzone badania rozszerzyć o analizę statystyczną, związaną z estymacją parametrów w skończonej próbie. Ponadto, przeprowadzone rozważania ograniczają się do stanów czystych, pomijając kwestię niezerowego splątania układu kwantowego ze środowiskiem. Uwzględnienie w rozważaniach mieszania, wynikającego z oddziaływania ze środowiskiem, jest niewątpliwie wyzwaniem. Jego podjecie wydaje się jednak konieczne z punktu widzenia możliwych praktycznych zastosowań rozwijanej metody.

Z perspektywy fizyki teoretycznej, nie zaś matematycznym aspektów informacji kwantowej, warto również zapytać o to, jakie nowe zrozumienie własności świata kwantowego wynika z przeprowadzonych badań. W szczególności, czy metoda samotestowania układów kwantowych ma znaczenie w oderwaniu od motywacji praktycznej, związanej z technicznym wykorzystaniem splątania kwantowego? Czy samotestowanie rzuca jakieś nowe światło na zagadnienie kwantowej nielokalności, korelacji kwantowych, problem pomiaru czy też kwantowej losowości? W moim odczuciu, dyskusje przeprowadzone w publikacjach koncentrują się na aspektach czysto technicznych (na opracowaniu metody), pomijając szerszą dyskusję fizycznych implikacji otrzymanych wyników. Nie umniejsza to wysokiemu poziomowi naukowemu samych wyników. Pozostaje jednak pewien niedosyt z punktu widzenia warstwy czysto poznawczej. Można mieć jednak nadzieję, że habilitant rozwinie te kwestie w ramach swojej dalszej pracy naukowej.

Inne osiągnięcia naukowe i organizacyjne

Poza wchodzącym w skład osiągnięcia habilitacyjnego cyklem dziewięciu publikacji, dr Kaniewski jest autorem i współautorem czternastu publikacji, dotyczących zagadnień w obszarze informacji kwantowej oraz kryptografii kwantowej. Analizując aktywność naukową dr Kaniewskiego, w bazie Google Scholar, można znaleźć 34 publikacje i preprinty, cytowane łącznie 1213 razy. Indeks Hirsha habilitanta, na podstawie Google Scholar, wynosi 17. Publikacje wchodzące w skład osiągnięcia habilitacyjnego były cytowane: 389 razy, według bazy Google Scholar i 241 razy, według bazy Web of Science. Są to wyniki bardzo dobre, w odniesieniu do reprezentowanej dyscypliny, etapu kariery naukowej, oraz czasu jaki upłynął od publikacji artykułów.

Na podstawie dostępnych danych, stwierdzić można, że habilitant kontynuuje swoją aktywność badawczą, regularnie publikując i prowadząc projekty naukowe. Z przedstawionych

dokumentów wynika, że habilitant był kierownikiem grantu POLONEZ z NCN, oraz HOMING z FNP. Aktualnie, jest kierownikiem grantu SONATA z NCN.

Habilitant prezentował wyniki swoich badań na międzynarodowych konferencjach, Na uwagę zasługuję wysoka internacjonalizacja działalności naukowej habilitanta. Uczestniczy on regularnie w miedzynarodowych konferencjach, również w ramach wykładów zaproszonych.

Habilitant angażuje się również w rozwój młodej kadry naukowej. Z załączonej dokumentacji wynika, że był on łącznie promotorem czterech prac licencjackich, trzech prac magisterskich oraz promotorem pomocniczym dwóch prac doktorskich.

Doświadczenie dydaktyczne habilitanta obejmuje prowadzenie ćwiczeń do kursu obliczeń kwantowych i kwantowej komunikacji, oraz dwa wykłady dotyczące kwantowej informacji.

Dr Kaniewski wykazać się może również sporym zaangażowaniem na rzecz środowiska naukowego, poprzez regularne zaangażowanie w recenzowanie publikacji.

Z powyższych informacji, wyłania się obraz aktywnego i wykwalifikowanego badacza, znakomicie odnajdującego się w realiach pracy naukowej.

Za słabszą stronę dorobku habilitanta można uznać obszar pracy organizacyjnej i popularyzacyjnej. W szczególności, w przedłożonej dokumentacji, nie wykazano ani jednej pracy popularnej habilitanta. W mojej opinii, o tak ciekawych badaniach, mogących znaleźć zastosowanie praktyczne, warto próbować komunikować również poza ramami środowiska naukowego.

Podsumowanie

Podsumowując, przedstawione osiągnięcie naukowe dr Kaniewskiego prezentuje bardzo wysoki poziom naukowy. Znaczący wkład dr Kaniewskiego w przedstawione osiągnięcie naukowe, w tym trzy prace jednoautorskie, nie pozostawiają wątpliwości co do naukowej samodzielności habilitanta. Nie bez znaczenia jest to, że habilitant z powodzeniem pozyskuje środki na prowadzone przez niego badania, stwarzając również warunki do naukowego rozwoju studentów. Działalność naukowa dr Kaniewskiego jest silnie osadzona w środowisku międzynarodowym. Odbył on zagraniczne staże naukowe, jak również ukończył zagraniczne studia magisterskie i doktoranckie.

W mojej ocenie, doktor Jędrzej Kaniewski spełnia ustawowe i zwyczajowe warunki stawiane kandydatom do stopnia doktora habilitowanego w dziedzinie nauk fizycznych. Wnoszę o przejście do dalszych etapów postępowania habilitacyjnego.

Z poważaniem,

Jakub Mielczarek

dr hab. Jakub Mielczarek
Instytut Fizyki Teoretycznej
Uniwersytet Jagielloński