Kraków, 31.12.2025

Recenzja rozprawy doktorskiej mgr Chithry Raj pt. "Information Processing Tasks as a Toolbox for Quantum Information"

Praca doktorska Pani mgr Chithry Raj pt. "Information Processing Tasks as a Toolbox for Quantum Information" została przygotowana na Wydziale Matematyki, Fizyki i Informatyki Uniwersytetu Gdańskiego. Promotorem pracy był dr hab. Marcin Pawłowski, prof. UG, a promotorem pomocniczym dr Pedro Ruas Dieguez.

Tematyka rozprawy doktorskiej koncentruje się na wybranych teoretycznych aspektach teorii informacji kwantowej, w szczególności w kontekście certyfikowania kwantowości układów fizycznych. Certyfikacja nabiera szczególnego znaczenia w sytuacjach, w których nie posiadamy pełnej wiedzy o badanym układzie kwantowym, a mimo to dążymy do potwierdzenia poprawności jego działania w zgodzie z zasadami mechaniki kwantowej. W obszarze kryptografii, certyfikacja odgrywa kluczową rolę, bezpośrednio wiążąc się z poziomem bezpieczeństwa danego rozwiązania.

Szczególnie interesujący podejściem do certyfikacji układów kwantowych jest abstrahowanie od technicznych szczegółów działania danego urządzenia kwantowego. Podejście to, oparte na traktowaniu systemu jako "czarnej skrzynki", określane jest mianem *niezależności od urządzenia* (Device-Independence – DI). Ma ono szczególne znaczenie w sytuacjach, gdy wykorzystywane urządzenie kwantowe pochodzi z nieautoryzowanego lub niezweryfikowanego źródła, a jego zastosowanie wymaga wiarygodnej certyfikacji poziomu bezpieczeństwa. Warto przy tym podkreślić, że jest to sytuacja niemająca bezpośredniego odpowiednika w fizyce klasycznej.

Zastosowanie idei niezależności od urządzeń w kryptografii kwantowej, w szczególności w ramach koncepcji DIQKD, zostało po raz pierwszy wskazane przez D. Mayersa i A. Yao w 1998 roku.

Dla przypadku dwóch splątanych kubitów, stosowaną powszechnie miarą tych korelacji jest tzw. parametr Clausera-Hornea-Simonyego-Holta(CHSH)-Bella - S. Zgodnie z istotą DI, wyrażenie na parametr S nie odwołuje się do szczegółów urządzenia eksperymentalnego, a jedynie do pewnych wielkości kontrolnych oraz do wyników pomiarów. Dla korelacji klasycznych pomiędzy bitami, zachodzi nierówność CHSH-Bella $S < 2$. Nierówność ta jest łamana, jeśli pomiędzy podukładami występuje splątanie kwantowe. Maksymalna wartość łamania jest równa $S = 2\sqrt{2} \approx 2.83$ (tzw. ograniczenie Tsirelsona), co jest spełnione dla stanów Bella, będących szczególnym przypadkiem stanów maksymalnie splątanych.

Niestety, praktyczna realizacji idei DI jest wciąż dużym wyzwaniem eksperymentalnym. Stąd, zrodziła się koncepcja jej słabszej wersji, określanej jako Semi-Device-Independence (SDI). W podejściu tym, dokonywane są pewne założenia co do natury testowanego układu fizycznego, takie jak ustalenie wymiaru przestrzeni Hilberta dla wykorzystanego kanału kwan-

towego. Jednymi z najprostszych i najpopularniejszych protokołów SDI są tzw. Quantum Random Access Codes (QRAC). Co ważne, QRAC działa na zasadzie Prepare and Measure (PM) i nie wymaga wykorzystania splątania kwantowego. W podejściu tym, wprowadzany jest tzw. *świadek wymiaru* S, o własnościach analogicznych do parametru CHSH. Spełnienie warunku $S > 2$ pozwala na certyfikację kwantowości protokołu. Analiza parametru S nie jest jednak jedyną drogą do certyfikacji, co stanowi istotną część analizy przedstawionej w dysertacji.

W szczególności, pojęcia znane z dyskusji podstaw mechanik kwantowej, takie jak *dualizm korpuskularno-falowy* czy też *realizm* nabrały w ostatnich dekadach operacyjnego charakteru, dostarczając nowych narzędzi do analizy układów kwantowych. Przywołane tu wielkości, jak również *entropowa relacja nieoznaczoności*, są przedmiotem dyskusji mgr Raj, dostarczając nowych i oryginalnych sposobów certyfikowania kwantowej natury układów fizycznych. Do grona tego należy również zaliczyć własności korelacji kwantowych ograniczone przez, tak zwaną, własność *monogamii* oraz *przyczynowość informacyjna* (ang. Information Causality - $\mathcal{IC}$).

Wyniki przedstawione w dysertacji eksplorują te możliwości, dostarczając nowego i cennego wglądu zarówno w podstawowe własności świata kwantowego jak i w praktyczną stronę urzeczywistnienia koncepcji SDI.

Zaprezentowane wyniki stanowią wkład do dwóch publikacji:

> [1] L. Pollyceno, A. Chaturvedi, C. Raj, P. R. Dieguez and M. Pawłowski, "Security of device-independent quantum key distribution via monogamy relations from multipartite information causality," Phys. Rev. A **112** (2025) no.4, 042201
>
> [2] C. Raj and P. R. Dieguez, "Wave-Particle Realism in Quantum-Controlled Interferometers Assisted by Entanglement," Open Syst. Info. Dyn. **32** (2025) no.02, 2550009

oraz jednego preprintu:

> [3] C. Raj, T. Prasad, A. Chaturvedi, L. Pollyceno, D. Spegel-Lexne, S. Gómez, J. Argillander, A. Alarcón, G. B. Xavier and M. Pawłowski, *et al.* "Certifying semi-device-independent security via wave-particle duality experiments," [arXiv:2507.00679 [quant-ph]].

Praca liczy 114 stron, wliczając stronę tytułową i została napisana w języku angielskim. Dysertacja została podzielona na sześć rozdziałów (zawierających podrozdziały) oraz bibliografię, zawierającą 135 pozycji literaturowych.

Rozdział 1 dysertacji stanowi wprowadzenie do tematyki rozprawy, zarysowujący proces badawczy prowadzący do dyskusji będącej przedmiotem dysertacji. W szczególności, przedstawiono motywację stojącą za wprowadzeniem tzw. podejścia Semi-Device-Independent

(SDI), zasady przyczynowości informacyjnej ($\mathcal{IC}$) oraz entropowej relacji nieoznaczoności (EUR). Koncepcje te odgrywają zasadniczą rolę w przedstawionych wynikach.

Pewien niedosyt budzi jednak brak nakreślenia szerszej perspektywy omawianej problematyki. Autorka ogranicza się bowiem do pojęć i modeli bezpośrednio związanych z tematyką dysertacji, co może prowadzić czytelnika do mylnego wrażenia co do rzeczywistego zakresu i bogactwa dyskutowanego obszaru badawczego. W szczególności, w kontekście podejścia SDI, zasadne byłoby omówienie różnych schematów SDI analizowanych w literaturze oraz uzasadnienie, dlaczego zasadniczy nacisk w pracy położony został na protokoły typu QRAC.

Warto byłoby również odwołać się do istniejących wyników doświadczalnych związanych z implementacją protokołów SDI, w szczególności realizacji QRAC w zastosowaniach do kwantowej dystrybucji klucza, co pozwoliłoby lepiej osadzić rozważania teoretyczne w kontekście eksperymentalnym.

W Rozdziale 2 wprowadzono podstawy fizyczne niezbędne do zrozumienia dalszej części pracy. Obejmują one elementarne zagadnienia mechaniki kwantowej oraz wybrane własności układów kwantowych, istotne z punktu widzenia prowadzonych rozważań. Do omawianych pojęć należą m.in. splątanie kwantowe, nielokalność kwantowa, monogamia splątania, realizm kwantowy oraz dualizm korpuskularno-falowy. Na szczególną uwagę zasługuje fakt, że dualizm korpuskularno-falowy został wprowadzony w swojej współczesnej, ścisłej postaci, co ma istotne znaczenie dla dalszych analiz.

W kontekście prowadzonej dyskusji istotną rolę odgrywają również takie koncepcje jak zasada *no-signaling* oraz przyczynowość informacyjna. Ponadto, w rozdziale tym sformalizowano pojęcia *device-independence* (DI) oraz *semi-device-independence* (SDI), które stanowią ramy pojęciowe dla dalszych rozważań i w obrębie których analizowane będą wcześniej wprowadzone zagadnienia.

Rozdział 3, przywołuje wyniki artykułu [1]. Centralnym wynikiem zaprezentowanym w tym rozdziale jest uogólnienie zasady Information Causality do przypadku układu wielu stron, połączonych zaszumionymi kanałami kwantowymi. W oryginalnym sformułowaniu, $\mathcal{IC}$ dotyczyło dwóch stron, natomiast w ostatnich latach uogólnioną tę zasadę do przypadku zaszumionego kanału dla dwóch stron oraz do przypadku wielu stron połączonych idealnym kanałem komunikacji. Skonstruowane uogólnienie może być podstawą do skonstruowania realistycznych protokołów DIQKD.

W kontekście otrzymanego uogólnienia, otrzymano ciekawy wynik łączący wielostronowe-$\mathcal{IC}$ z własnością monogamii. Otrzymane wyniki, wspierają wcześnie znane argumenty, iż $\mathcal{IC}$ może stanowić zasadę, którą możemy posiłkować się przy certyfikacji kwantowych własności układów. Przykładem jest tu realizacja DIQKD.

W moje ocenie, rozdział ten mogłaby wzmocnić dodatkowa dyskusja dostarczającą zrozumienia fizycznego otrzymanych wyników, wychodząca poza bardzo formalną analizę. W

szczególności, dotyczy to obecności monogamii w $\mathcal{IC}$, wychodząc poza układy dwuczęściowe. Jak intuicyjnie wytłumaczyć wynikanie monogamii z kauzalności informacji?

Rozdział 4, przywołuje wyniki przedstawione w preprincie [3]. Dotyczą one możliwości certyfikowania podejścia SDI za pomocą analizy dualizmu korpuskularno-falowego. Konkretnie, analizowany jest przypadek QRAC typu (4,2,2), który jest jednym z najpopularniejszych scenariuszy SDI, dla którego przyjmowane jest założenie co do wymiaru przestrzeni Hilberta dla kanału kwantowego. Przypadek ten był wcześniej analizowany z wykorzystaniem tzw. *świadka wymiaru* (ang. dimension witness), skonstruowanego w oparciu o obserwowane korelacji pomiędzy wartościami zmiennych binarnych (trzech kontrolnych i jednej wyjściowej). Wyniki przedstawione w dysertacji przedstawiają nową konstrukcję teoretyczną, wykorzystującą wariant interferometru Macha-Zehndera do realizacji protokołu QRAC. Co więcej, zaproponowane zostało wprowadzenie alternatywnego świadka wymiaru, zbudowanego w oparciu o wielkości interferometryczne, kwantyfikujące korpuskularną (rozróżnialność dróg $\mathcal{D}$) oraz falową (widzialność $\mathcal{V}$) naturę eksperymentu, co jest bardzo ciekawym pomysłem. Ponadto, jak udowodniono, podejście takie pozwala na nieznaczne zwiększenie zakresu parametrów dla których możliwa jest certyfikacja kwantowości protokołu. Dodatkowy wgląd teoretyczny dostarcza przeprowadzona analiza entropowej relacji nieoznaczoności, skonstruowanej w oparciu o wartości parametrów $\mathcal{D}$ i $\mathcal{V}$. Analiza ta jest przydatna, w szczególności, z punktu widzenia ilościowej oceny bezpieczeństwa protokołu, kwantyfikując liczbę bezpiecznie wymienianych bitów informacji. Co niezwykle ważne, omówiony schemat został przetestowany w warunkach doświadczalnych. Opis realizacji doświadczalnej, zrealizowanej przez zaprzyjaźnioną grupę eksperymentalną, jest jednak niestety bardzo skąpy. Nie przywołane zostały informacje które pozwoliłyby ocenić na ile spełnione zostały założenia teoretyczne. W szczególności, układ opiera się na tłumionej wiązce koherentnej, która generuje nie pojedyncze fotony a impulsy z liczbą fotonów danych przez rozkład Poissona. Podanie wartość parametru μ (średniej ilości fotonów) dla rozważanego eksperymentu, pozwoliłoby na wstępną ocenę tego na ile założenie impulsów 1-fotonowych jest spełnione. Warto byłoby również uogólnić przeprowadzone rozważania teoretyczne dla przypadku w którym na jeden z portów wejściowych pierwszego dzielnika wiązki podawany jest impuls koherentny, parametryzowany przez μ. Ciekawe byłoby odpowiedzenie na pytanie dla jakiego zakresu wartości parametru μ, proponowany schemat dopuszcza możliwość certyfikacji kwantowości. Warto również zwrócić uwagę na fakt, że dyskutowana certyfikacja dotyczy jedynie istnienia dodatniej szybkości wymiany sekretnego klucza. Nie jest to zaś pełny dowód bezpieczeństwa protokołu kwantowego, co wymaga dalszej, bardziej szczegółowej analizy. Finalnie, warto podkreślić, że pomimo tego, że przywołane wyniki nie zostały jeszcze opublikowane (stanowią wkład do preprintu), w mojej ocenie, z uwagi na ich nowatorskość oraz potwierdzenie doświadczalne, prognozują możliwość opublikowania w czasopiśmie z najwyższą punktacją MEiN.

Rozdział 5 przedstawia wyniki zaprezentowane w artykule [2], dotyczące uogólnienia znanego eksperymentu Wheelera z opóźnionym wyborem. W rozważanym uogólnieniu część interferometru podlega kontroli kwantowej. Przeanalizowano kilka scenariuszy realizacji takiego eksperymentu. W tym kontekście omówiono również, stosunkowo niedawno wprowadzoną, wielkość służącą do kwantyfikacji realizmu. Zaproponowany model stanowi interesujące pole doświadczalne do badania koncepcyjnych aspektów mechaniki kwantowej. Jednakże, w mojej ocenie, jego znaczenie jako przyczynka do rozprawy jest relatywnie mniejsze. Także, związek z główną narracją rozprawy jest tu wyraźnie słabszy. Stąd, w moje ocenie, warto byłoby silniej podkreślić, w jaki sposób analiza realizmu wpisuje się w ogólną ideę certyfikacji oraz SDI.

Rozprawę zamyka Rozdział 6, zawierający podsumowanie uzyskanych wyników oraz ogólne wnioski. Rozdział ten obejmuje również uwagi dotyczące możliwych kierunków dalszych badań. W mojej ocenie, przedstawiona dyskusja ma jednak charakter zbyt ogólny i wymaga zarówno doprecyzowania, jak i istotnego rozszerzenia. Szczególnie interesujące wydaje się przeanalizowanie zachowania omawianych scenariuszy w kontekście ich fizycznych realizacji, które wymagają m.in. uwzględnienia stanów mieszanych oraz realistycznych źródeł światła (opisywanych rozkładem Poissona).

Reasumując, rozprawa stanowi spójny i logiczny ciąg rozumowania, w pełni zgodny z metodologią pracy naukowej. Przeprowadzona analiza świadczy o solidnym warsztacie pojęciowym oraz matematycznym autora. Choć zastosowane obliczenia nie wykraczają istotnie poza zakres algebry liniowej i teorii prawdopodobieństwa, ich poprawne i twórcze przeprowadzenie wymagało znacznej biegłości oraz pomysłowości. Wyprowadzenia są staranne, a argumentacja klarowna i konsekwentna. Na podstawie treści rozprawy i publikacji należy także uznać, że doktorantka odegrała znaczącą rolę w uzyskaniu zaprezentowanych wyników.

Publikacje stanowiące wkład do niniejszej dysertacji zostały opublikowane w uznanym czasopiśmie fizycznym Physical Review A (IF = 2.9, 100 pkt MEiN) oraz w czasopiśmie Open Systems & Information Dynamics (IF = 1.6, 70 pkt MEiN), o niższej pozycji rankingowej. Choć są to periodyki rozpoznawalne i istotne dla omawianej tematyki, warto zauważyć, że żadna z prac nie ukazała się w czasopiśmie o wyższej kategorii punktowej (140 lub 200 pkt), co mogłoby dodatkowo wzmocnić ocenę bibliometryczną dorobku.

Jak wskazano wcześniej, w mojej ocenie wyniki stanowiące podstawę przygotowanego preprintu rokują możliwość publikacji w czasopiśmie o najwyższej punktacji MEiN (200 pkt).

Dotychczas uzyskane rezultaty nie spotkały się jeszcze z szerokim zainteresowaniem środowiska naukowego, co znajduje odzwierciedlenie w niewielkiej liczbie cytowań, ograniczają-

cej się do pojedynczego odwołania do wymienionych prac. Należy jednak podkreślić, że ograniczona rozpoznawalność tych wyników wynika najprawdopodobniej z relatywnie niedawnego terminu ich publikacji, a tym samym z naturalnego opóźnienia w procesie ich recepcji przez środowisko naukowe.

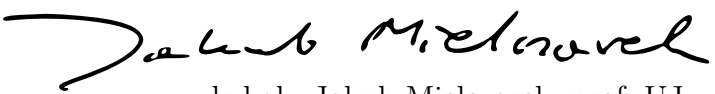
Część z moich uwag do pracy zawarłem w powyższej dyskusji. Do dalszych komentarzy, jakie nasuwają się po zapoznaniu z treścią pracy, można zaliczyć:

- Brak definicji *tangle* τ, użytego we wzorze (2.16).
- Wydaje się, że na stronie 26 powinno być $P_B = 0.75$, nie zaś $P_B \approx 0.75$.
- Referencje [86] i [105] to ta sama publikacja.
- Brak analizy przypadku realistycznych źródeł światła, dla przypadku tłumionych impulsów koherentnych.
- Warto byłoby porównać protokoły SDI, takie jak QRAC, do standardowych protokołów QKD. W szczególności, jakich temp wymiany sekretnego klucza (SKR) możemy się spodziewać w tym pierwszym przypadku i jak to się ma do standardowych protokołów QKD typu PM.
- Jak wykorzystanie pamięci kwantowej przez adwersarza wpływa na bezpieczeństwo dyskutowanego protokołu QRAC?
- Co możemy powiedzieć o różnicy w możliwym do osiągnięcia SKR dla SDI opartego na splątaniu oraz bez splątania, jak w przypadku QRAC?

Powyższe uwagi nie stanowią krytycznych zastrzeżeń wobec treści dysertacji, lecz należy je traktować jako konstruktywną zachętę do dalszej, pogłębionej eksploracji poruszanych w niej zagadnień. Nie wpływają one na ogólnie pozytywną ocenę pracy, zarówno pod względem koncepcyjnym, jak i rzetelności oraz dojrzałości przeprowadzonej analizy, a także trafności i zasadności zastosowanych i rozwiniętych metod badawczych.

Podsumowując, stwierdzam, że praca Pani mgr Chithry Raj pt. "Information Processing Tasks as a Toolbox for Quantum Information" spełnia warunki określone w Art. 186 ustawy z dnia 20 lipca 2018 roku - Prawo o szkolnictwie wyższym i nauce i wnioskuję o przejście do kolejnego etapu procedury związanej z przyznaniem Pani mgr Chithrze Raj stopnia doktora w dziedzinie nauk ścisłych i przyrodniczych w dyscyplinie nauki fizyczne.

Z poważaniem,



dr hab. Jakub Mielczarek, prof. UJ
Instytut Fizyki Teoretycznej, Uniwersytet Jagielloński