Prof. dr hab. Paweł Kurzyński
Wydział Fizyki i Astronomii UAM
Ul. Uniwersytetu Poznańskiego 2
61-614 Poznań
Email: pawel.kurzynski@amu.edu.pl

Poznań, 8 lipca 2026

Recenzja rozprawy doktorskiej mgr Tushity Prasad
„Operational approaches to quantum resources in communication and security"

Problem badawczy

Przedstawiona rozprawa doktorska Pani mgr Tushity Prasad wpisuje się w dziedzinę teorii komunikacji kwantowej, ze szczególnym uwzględnieniem roli zasobów kwantowych w zadaniach kodowania, przesyłania informacji oraz kryptografii kwantowej. Kandydatka ubiega się o nadanie stopnia doktora w dziedzinie nauk ścisłych i przyrodniczych, w dyscyplinie nauki fizyczne.

Rozprawa ma formę tak zwanej spinki i składa się z obszernego wprowadzenia oraz trzech prac naukowych. Dwie z nich zostały już opublikowane w jednym z wiodących czasopism w dziedzinie teorii informacji kwantowej, *npj Quantum Information*. Kandydatka jest pierwszą autorką jednej z prac, a jej wkład w powstanie pozostałych dwóch, potwierdzony oświadczeniami współautorów, był znaczący.

Tematyka rozprawy jest aktualna, ambitna i ważna zarówno z punktu widzenia podstaw fizyki kwantowej, jak i potencjalnych zastosowań w komunikacji kwantowej. Wszystkie trzy prace dotyczą fundamentalnego pytania: jakie zasoby kwantowe, i w jakich warunkach, pozwalają osiągnąć przewagę nad protokołami klasycznymi lub zapewnić bezpieczeństwo kryptograficzne? Pytanie to jest jednym z centralnych problemów współczesnej teorii informacji kwantowej.

Na szczególne podkreślenie zasługuje również sposób, w jaki Kandydatka motywuje badania nad zasobami kwantowymi. We wstępie stwierdza, że wartość zasobu wynika z zadań, jakie ten zasób czyni możliwymi. Bardzo dobrze oddaje to praktyczny i operacyjny charakter całej rozprawy. Osobiście podchodzę dość sceptycznie do tworzenia teorii zasobów kwantowych w oderwaniu od konkretnych zadań informacyjnych, dlatego uważam tę perspektywę za szczególnie trafną.

Rezultaty i ich ocena

Pierwsza praca dotyczy wykorzystania skończonej liczby splątanych par oraz skończonej liczby niesplątanych układów kwantowych do konstrukcji kodu pozwalającego na wierne przesłanie wiadomości. Dokładniej, autorzy rozważają sytuację, w której dostępnych jest c splątanych par oraz n−c niesplątanych układów, a celem jest przesłanie wiadomości o długości k<n. Układy kwantowe są q-wymiarowe.

Najważniejszym wynikiem tej pracy jest pokazanie, że przy wystarczającej liczbie splątanych par otrzymany kod może przekroczyć granicę Singletona, czyli klasyczne ograniczenie opisujące zależność pomiędzy długością kodu, długością wiadomości i minimalnym dystansem kodu, który opisuje jego zdolność do wykrywania i korekcji błędów. Wynik ten jest bardzo interesujący, ponieważ jednoznacznie pokazuje przewagę możliwą do osiągnięcia dzięki skończonym zasobom kwantowym.

Co więcej, rezultat nie jest trywialny. Mogłoby się wydawać, że użycie protokołu gęstego kodowania powinno prowadzić do przewagi już przy niewielkiej liczbie splątanych par. Jednak w obecności błędów sytuacja okazuje się subtelniejsza. Autorzy pokazują, że istnieje graniczna liczba splątanych par, dopiero powyżej której pojawia się przewaga nad klasyczną granicą Singletona. Uważam ten wynik za bardzo wartościowy z teoretycznego punktu widzenia, ponieważ precyzyjnie pokazuje, kiedy splątanie zaczyna pełnić rolę użytecznego zasobu w skończonym zadaniu komunikacyjnym.

Pewną wątpliwość budzi we mnie praktyczna odporność zaproponowanego protokołu na niedoskonałości rzeczywistych stanów splątanych. W szczególności chciałbym lepiej zrozumieć, jak protokół zachowuje się w sytuacji, gdy splątane pary nie są stanami czystymi, lecz stanami mieszanymi, na przykład stanami Wernera o wysokiej, lecz nieidealnej widzialności. Wracam do tej kwestii w części poświęconej uwagom.

Druga praca ma charakter teoretyczno-doświadczalny i łączy trzy ważne zagadnienia: dualizm korpuskularno-falowy, entropowe zasady nieoznaczoności oraz częściowo niezależną od urządzeń kwantową dystrybucję klucza, czyli protokoły semi-device-independent. Główna idea polega na wyrażeniu warunków bezpieczeństwa SDI, a dokładniej świadka wymiaru, za pomocą wielkości interferometrycznych, takich jak informacja o ścieżce fotonu oraz widzialność prążków interferencyjnych.

Główne wyniki tej pracy to wyrażenie świadka wymiaru jako funkcji informacji o ścieżce i widzialności interferencyjnej, znalezienie ulepszonej granicy bezpieczeństwa dla protokołów SDI oraz eksperymentalna weryfikacja typu proof of principle. Autorzy rozważają również scenariusze interferometryczne z więcej niż dwiema ścieżkami i wiążą uzyskane wyniki z entropowymi relacjami nieoznaczoności.

Uważam tę pracę za bardzo ciekawą. Ma ona znaczenie zarówno dla podstaw fizyki kwantowej, ponieważ pokazuje nowy związek pomiędzy dualizmem korpuskularno-falowym a bezpieczeństwem komunikacji kwantowej, jak i dla kwantowej teorii komunikacji. Szczególnie istotne jest wyprowadzenie ulepszonej granicy bezpieczeństwa dla protokołów SDI. Taki wynik ma potencjalne znaczenie praktyczne, ponieważ większa tolerancja na niedoskonałości eksperymentalne jest jednym z kluczowych warunków rozwoju rzeczywistych protokołów kryptograficznych.

Sam eksperyment nie wydaje mi się przełomowy, ale pełni ważną funkcję: pokazuje, że wyniki teoretyczne mają naturalną implementację optyczną i mogą zostać sprawdzone w realistycznym układzie fizycznym.

Trzecia praca dotyczy bardzo interesującego i fundamentalnego pytania o rolę splątania w praktycznych protokołach kryptografii kwantowej. Autorzy pokazują, że w obecności klasycznego wycieku informacji (side information leakage) posiadanie stanów splątanych może przestać być warunkiem wystarczającym na gwarancję bezpieczeństwa.

Autorzy rozważają dwa przypadki. W pierwszym wyciek informacji może pojawić się w dowolnej rundzie protokołu. W drugim wyciek dotyczy jedynie tych rund, które nie przyczyniają się bezpośrednio do generacji klucza. Szczególnie interesujący i nieintuicyjny jest fakt, że nawet w tym drugim przypadku samo splątanie przestaje być wystarczające do zapewnienia bezpieczeństwa.

Moim zdaniem jest to najciekawsza z trzech prac wchodzących w skład rozprawy. Wynik jest fundamentalny zarówno z punktu widzenia podstaw fizyki kwantowej, jak i teorii komunikacji kwantowej. Nie jestem specjalistą w dziedzinie kryptografii kwantowej, jednak mam wrażenie, że praca otwiera ciekawy kierunek badań i stawia ważne pytanie: jaki zasób, poza splątaniem, jest rzeczywiście odpowiedzialny za możliwość bezpiecznej generacji klucza w realistycznych warunkach? Dodatkowo, autorzy otrzymali ciekawy wynik dotyczący maksymalnej ilości niedoskonałych kwantowych powielaczy (quantum repeaters), których można użyć aby nadal móc wygenerować bezpieczny klucz kryptograficzny. Ten wynik ma praktyczne znaczenie dla sieci kwantowych, w których splątanie pomiędzy odległymi użytkownikami jest tworzone za pomocą protokołów wymiany splątania.

Podsumowując, wszystkie trzy prace stanowią oryginalne i wartościowe rozwiązania ważnych problemów badawczych. Wyniki są nietrywialne, dobrze umotywowane i opublikowane, przynajmniej częściowo, w bardzo dobrych czasopismach naukowych. Uważam, że przedstawiona rozprawa wnosi istotny wkład do teorii komunikacji kwantowej.

Wkład Kandydatki

Wszystkie trzy prace wchodzące w skład rozprawy są wieloautorskie. Kandydatka jest pierwszą autorką jednej z nich, a z oświadczeń współautorów wynika, że jej wkład w powstanie pozostałych dwóch prac był znaczący. Dwie prace zostały już opublikowane w *npj Quantum Information*, co potwierdza wysoki poziom naukowy przedstawionych wyników.

Uważam, że udokumentowany wkład Kandydatki jest wystarczający, aby przedstawione prace mogły stanowić podstawę do nadania jej stopnia doktora. Co więcej, zakres tematyczny rozprawy oraz jakość wprowadzenia pokazują, że Kandydatka bardzo dobrze orientuje się w badanej dziedzinie i posiada umiejętność samodzielnego formułowania oraz analizowania problemów naukowych.

Układ rozprawy i strona redakcyjna

Rozprawa została przygotowana bardzo starannie. Obszerne wprowadzenie napisano w sposób jasny i przystępny. Pozwala ono czytelnikowi zapoznać się z większością podstawowych pojęć z zakresu teorii komunikacji kwantowej, teorii kodowania, kwantowej dystrybucji klucza oraz z najważniejszymi wynikami stanowiącymi tło dla prac Kandydatki. Edycja tekstu jest bardzo staranna, a całość sprawia wrażenie dobrze przemyślanej i dopracowanej rozprawy doktorskiej.

Mam jedynie kilka uwag i pytań, które przedstawiam poniżej. Nie wpływają one na moją bardzo pozytywną ocenę rozprawy, lecz mogą być dobrym punktem wyjścia do dyskusji podczas obrony.

Uwagi i pytania

1. Definicje 2.6, 2.7, 2.12 i 2.13 nie są dla mnie całkowicie jasne. Wydaje mi się, że warto byłoby zdefiniować wcześniej wielkość p_{guess}, ponieważ pełni ona istotną rolę w dalszej części rozprawy. Jak rozumiem, p_{guess} nigdy nie jest mniejsze niż 1/2. Warto to podkreślić.

2. Podrozdział 2.2, dotyczący teorii kodowania, jest napisany przystępnie, ale jego ostatnia część, poświęcona kodom Reeda-Solomona, wydaje mi się zbyt powierzchowna. Ponieważ pierwsza praca w dużej mierze opiera się właśnie na tej konstrukcji, chętnie zobaczyłbym bardziej szczegółowe omówienie idei kodowania, dekodowania, wykrywania i korekcji błędów w kodach Reeda-Solomona.

3. W podrozdziale 3.2 brakuje mi nieco dokładniejszej informacji na temat wyprowadzenia ulepszonej granicy bezpieczeństwa w protokołach SDI. Ponieważ jest to jeden z najważniejszych wyników drugiej pracy, bardziej szczegółowe omówienie tej części byłoby bardzo pomocne dla czytelnika.

4. W pierwszej pracy, jak rozumiem, protokół wymaga idealnie splątanych par. Autorzy krótko omawiają niedoskonałe stany splątane, określając je jako „złe" pary, i wspominają, że protokół nadal działa, jeśli suma liczby błędów i liczby „złych" par jest mniejsza niż połowa minimalnego dystansu. Nie do końca rozumiem jednak, jak interpretować tę sytuację w realistycznych warunkach, w których każda para splątana ma niezerową domieszkę szumu. Czy wtedy każda para powinna być traktowana jako „zła"? Byłbym wdzięczny, gdyby Kandydatka mogła omówić, jak współczynnik R zależałby od widzialności v na przykład dla dwu-kubitowych stanów Wernera. Naturalnym uzupełnieniem byłaby trójwymiarowa wersja wykresu 3.2, w której dodatkowa oś opisywałaby widzialność stanu splątanego.

5. W drugiej pracy zależność S=2(D+V) jest bardzo elegancka i daje przejrzystą interpretację świadka wymiaru w języku interferometrii. Została ona jednak otrzymana przy założeniach odpowiadających równaniom (25) i (26) w pracy. Czy w sytuacji, gdy założenia te nie są dokładnie spełnione, powyższa zależność nadal pozostaje użyteczna? Innymi słowy, jak odporna jest ta relacja na realistyczne niedoskonałości eksperymentalne?

6. W trzeciej pracy kluczową rolę odgrywa klasyczny wyciek informacji. Chciałbym lepiej zrozumieć, jak taki wyciek może wyglądać w praktycznych fizycznych realizacjach protokołów EB-QKD. Czy można wskazać konkretne przykłady eksperymentalnych niedoskonałości lub procedur przetwarzania danych, które odpowiadałyby modelowi rozważanemu w pracy?

7. Również w trzeciej pracy Autorzy pytają, jaka własność, poza splątaniem, jest potrzebna do bezpiecznej kwantowej generacji klucza. Czy Kandydatka i jej współautorzy mają już potencjalnych kandydatów na taki dodatkowy zasób? Czy może chodzi raczej o pewną kombinację własności stanu, protokołu i ograniczeń na informację dostępną dla Ewy?

Podsumowanie i wniosek końcowy

Przedstawiona rozprawa doktorska jest bardzo solidnym i wartościowym opracowaniem z zakresu teorii komunikacji kwantowej. Zawiera oryginalne wyniki naukowe dotyczące kodowania z wykorzystaniem skończonych zasobów splątania, częściowo niezależnej od urządzeń kryptografii kwantowej oraz roli klasycznego wycieku informacji w protokołach opartych na splątaniu.

Wyniki przedstawione w rozprawie są nietrywialne, dobrze umotywowane i istotne dla dalszego rozwoju teorii informacji kwantowej. Na szczególne uznanie zasługuje fakt, że dwie prace zostały opublikowane w *npj Quantum Information*, a Kandydatka ma udokumentowany znaczący wkład w powstanie wszystkich trzech prac. Wprowadzenie do rozprawy zostało napisane jasno i starannie, a całość świadczy o bardzo dobrej znajomości dziedziny.

Uważam, że rozprawa spełnia wszystkie ustawowe i zwyczajowe wymagania stawiane rozprawom doktorskim w dyscyplinie nauki fizyczne. W związku z tym jednoznacznie wnioskuję o dopuszczenie Pani mgr Tushity Prasad do dalszych etapów postępowania doktorskiego. Ponadto, biorąc pod uwagę bardzo wysoką jakość naukową przedstawionych wyników, ich publikację w wiodącym czasopiśmie *npj Quantum Information*, spójność tematyczną rozprawy oraz fakt, że uzyskane rezultaty dotyczą fundamentalnych i aktualnych problemów teorii komunikacji kwantowej, wnioskuję o wyróżnienie rozprawy doktorskiej Pani mgr Tushity Prasad. W mojej ocenie rozprawa wykracza poza standardowy poziom prac doktorskich, ponieważ nie tylko rozwiązuje konkretne problemy techniczne, ale również wskazuje nowe pytania badawcze dotyczące roli zasobów kwantowych w komunikacji i kryptografii kwantowej.