Prof. dr hab. Paweł Horodecki
Wydział Fizyki Technicznej i Matematyki Stosowanej
Politechnika Gdańska

Gdańsk, 15.11.2017

Recenzja rozprawy doktorskiej mgr. Ryszarda Savitara Veynara pt.
„Fizyczne ograniczenia na przetwarzanie informacji kwantowej"

Rozprawa doktorska pana Ryszarda Veynara dotyczy - jak pisze we wstępie sam doktorant - wybranych zagadnień z dziedziny przetwarzania informacji kwantowej z perspektywy fizycznych ograniczeń. Rozprawa liczy sobie 102 strony i jest zasadniczo oparta na trzech artykułach opublikowanych przez doktoranta wraz z promotorem profesorem Wiesławem Laskowskim oraz promotorem pomocniczym doktorem Marcinem Pawłowskim i współpracownikami w pismach Physical Review A, Journal of Physics A oraz International Journal of Quantum Information, a także jednym manuskrypcie nieopublikowanym, napisanym wspólnie z promotorem pomocniczym i współpracownikami. Trzy spośród tych prac mają czterech autorów, a jedna - trzech. Rozprawa zawiera też analizy wcześniej nie publikowane. Struktura pracy odpowiada czterem różnym tematom związanym z czterema powyższymi artykułami i wpisuje się w tendencję ostatnich kilku lat, aby po rozstrzygnięciu wielu zagadnień kwantowej teorii informacji na poziomie zasadniczym poszukiwać rozwiązań praktycznych z punktu widzenia realizacji eksperymentalnych, a nawet komercyjnych.

Praca rozpoczyna wstęp zawierający krótki rys historyczny, po którym następuje rozdział drugi, gdzie autor przybliża te elementy klasycznej teorii informacji oraz podstawowe pojęcia kwantowego formalizmu, które są istotne z punktu widzenia teorii informacji kwantowej. Kolejny rozdział poświęcony jest praktycznym aspektom bezpieczeństwa komunikacyjnego. Punktem wyjścia jest tu tzw. kod losowego dostępu, który docelowo ma służyć generacji klucza kryptograficznego. Po opisie działania tego protokołu w wariancie z dwoma bitami wejściowymi następuje szczegółowa analiza ataków kryptograficznych w wariancie typu *semi-device independent* (SDI) tzn. gdy niektóre parametry urządzeń (w szczególności wymiar przestrzeni Hilberta układu przygotowanego w urządzeniu nadawcy), w przeciwieństwie do innych, są poza zasięgiem adwersarza. Pozostałe założenia dotyczą (i) kontroli urządzeń przez adwersarza, których działanie może zależeć od kontrolowanej przez niego ukrytej zmiennej (ii) typowego założenia ataków indywidualnych (iii) reprezentacji najlepszej wiedzy o bicie za pomocą ściśle określonego pojedynczego bitu (iv) niezależności efektywności detekcji u odbiorcy od przeprowadzonego pomiaru. Pewną motywację stanowi tu ważny atak kryptograficzny bazujący na oślepieniu detektorów, który pochodzi od Vadima Makarowa.

Prezentowane są analizy dla ataków typu „przechwyć/prześlij" w trzech wariantach. Dwa pierwsze z możliwością wpływu na stany nadawane oraz jej brakiem, ostatni z wpływem zarówno na stany nadawane jaki i na pomiary w laboratorium odbiorcy. Kombinowana probabilistyczno-numeryczna analiza prowadzi do wniosku, że dwa pierwsze przypadki są równoważne i znacznie kryptograficzne korzystniejsze od trzeciego. Kolejny etap badawczy dotyczy interesującej sytuacji, gdy adwersarz ma do dyspozycji kubit pamięci i dokonuje jego pomiaru po zakończeniu protokołu przez strony zainteresowane. Co interesujące - przypadek ten okazuje się równoważny wersji, gdy adwersarz kontroluje jedynie urządzenie odbiorcy. Wyniki zilustrowano odpowiednimi wykresami.

Rozdział trzeci poświęcono zagadnieniu kwantowej teleportacji w sytuacji ograniczonej pojemności kanału kwantowego przy idealnym zasobie kwantowym tj. splątaniu maksymalnym. Znaleziono formułę wierności transmisji, która jest analogiczna do obowiązującej w sytuacji idealnego kanału klasycznego i zaszumionego zasobu kwantowego. Zasadniczym wynikiem tego rozdziału jest wyliczenie minimalnej pojemności kanału klasycznego C, powyżej której mamy do czynienia z teleportacją kwantową - wartość ta jest najbardziej niekorzystna (najwyższa) dla wymiaru d = 4. Zbadano także i zilustrowano przy pomocy wykresu przypadek, gdy mamy do czynienia z kanałem idealnym, ale o niższej wymiarowości, który - jak pokazano, może sprawować się lepiej jako narzędzie dla pewnego zakresu parametrów C oraz d.

Rozdział piąty poświęcono optymalnej mocy pompowania w kwantowo-optycznej realizacji protokołu Bennetta, Brassarda i Mermina z roku 1992. Celem było odtworzenie sytuacji, gdy analizatory splątania wielofotonowego zachowują się tak, jakbyśmy mieli do czynienia z pojedynczymi fotonami (modulo ewentualna niemożność rozróżniania przez detektor liczby fotonów, o ile ta jest niezerowa). W rozdziale przedstawiono optymalizację prawdopodobieństwa takiego zachowania, które jest podstawą odpowiedniej preselekcji, ze względu na kąty analizatorów oraz jego zależność od parametru charakteryzującego amplitudę lasera pompującego. Niestety czytelnik nie dowie się dlaczego protokół ten spełnia warunek braku korelacji z układem adwersarza, tj. czy i - ewentualnie - dlaczego jego statystyki *po postselekcji* byłyby równoważne statystykom na stanie czystym (dodajmy zresztą, że z punktu widzenia teorii tzw. stanów prywatnych taka czystość nie byłaby w ogólności potrzebna). Przypomnijmy - protokół BBM92 działa dlatego, że stuprocentowe korelacje stanów między polaryzacjami dwóch pojedynczych fotonów w dwóch różnych płaszczyznach gwarantują czystość i maksymalne splątanie stanu, podczas, gdy w bieżącym protokole dopuszczamy absorpcję stanów wielofotonowych. Dodatkowo, dla dobra czytelnika warto było zaznaczyć, że stosowana tu postselekcja jest dozwolona dlatego, że nie jest to przypadek tzw. *device-independent*, a zatem użytkownicy protokołu mają pewność, że mierzą ten, a nie inny stopień swobody. Zasadniczo omawiana tu część rozprawy jest napisana zbyt skrótowo.

Rozdział szósty poświęcono problemowi detekcji splątania w sytuacji, gdy mamy ograniczenie, jakim jest koszt przeprowadzenia pomiaru każdej obserwabli. Zasadnicza koncepcja polega tu na wyprowadzeniu na bazie wcześniejszego bardzo ogólnego testu splątania zaproponowanego w pracy [P. Badziąg, C. Brukner, W. Laskowski, T. Paterek, M. Żukowski, Phys. Rev. Lett. 100, 140403 (2008)] interesującego kryterium splątania, które autor nazywa liniowym. Kryterium to jest sformułowane za pomocą wzoru (6.12). Faktycznie mamy tu, tak jak w przypadku oryginalnym, do czynienia z kryterium nieliniowym, o czym zaświadcza prawa strona nierówności, ale rezultat trudniejszych obliczeń spoczywa w nim po lewej, liniowej stronie, co do pewnego stopnia uzasadnia przyjętą nomenklaturę. Metoda sprawdza się w przypadku stanów o dodatkowej symetrii, jako że wymaga dodatkowo znajomości najbliższego stanu separowalnego ρ_0 (lub PPT - jeżeli mamy do czynienia z detekcją splątania typu NPT). Znajomość taka pozwala na sukcesywne zwiększanie liczby pomiarów identyfikujących elementy odpowiedniego tensora, jedynie do momentu gdy warunek (6.12) zostanie spełniony, co może nastąpić na długo przed wyczerpaniem ustawień tomograficznych. Wynik jest bardzo wartościowy, ale wydaje się, że jego ograniczeniem jest, iż odwołuje się do wiedzy *a priori* - wysokiej symetrii stanu, na podstawie której można wyznaczyć ρ_0. W tym sensie metoda wydaje się nadawać do zastosowań jako szybki i wydajny laboratoryjny test wstępny, ale nie - ostateczny. Nawiasem mówiąc, warto było zaznaczyć

explicite już przy wzorze (6.12), że wystarczy znaleźć odpowiednio ciasne ograniczenie górne lewej strony zamiast jej maksimum. W rozdziale przytoczono kilka przykładów zastosowania, w tym jeden dotyczący detekcji splątania związanego przy pomocy opracowanej metody.

Zanim przejdę do oceny ogólnej, sformułuję jeszcze kilka uwag. Praca jest napisana jakby z nierównym zaangażowaniem. W rozdziale drugim po interesującym wstępie dotyczącym kodów ze swobodnym dostępem następuje część badawcza, która w sporej części jest powieleniem treści odnośnego artykułu. O ile autor w obu częściach, jak i tekście w całej pracy, wykazuje się przystępnym, trafiającym w sedno stylem, jeżeli idzie o sam opis zjawisk - co, podkreślmy, jest dużą wartością niniejszej rozprawy jako całości i nie może być pomijane - o tyle formuły matematyczne pojawiają się nierzadko bez dostatecznego uzasadnienia (choćby (3.15), którą można łatwo objaśnić jako sumę członów bayesowskich). W wielu ważnych miejscach brakuje w pracy jakości dodanej, która powinna charakteryzować każdą dobrze napisaną pracę doktorską - wywód formalny powinien być dopracowany i uzupełniony o te szczegóły, na które nie ma miejsca w artykułach naukowych. Przykładem jest tu wspomniany już rozdział 5, z punktu widzenia formalizmu matematycznego - powtórzmy - kompletnie oderwany od protokołu BBM92 jeżeli idzie o jego istotę tj. brak korelacji z potencjalnym adwersarzem gwarantowany przez strukturę stanu, jaką odczytujemy z wyników pomiarów. Kontrastuje z nim rozdział o detekcji splątania.

Z uwag szczegółowych - w rozdziale drugim zabrakło podkreślenia, że założenie o wolnej woli dotyczy też Alicji w tym sensie, że jej bity są wybrane losowo. Ponadto w opisie schematu ataku przez oślepienie pod rysunkiem 3.2 nie ma uwagi o jakich stanach kwantowych jest tu mowa (przypadki stanów jednofotonowego i koherentnego zasadniczo się różnią). Zupełnie brakuje odniesienia do literatury w podrozdziale 4.2. Rysunki 4.1 oraz 4.2 pojawiły się w rozdziale czwartym zupełnie przez pomyłkę jako kopie tychże z rozdziału piątego. Czytelnik musi skorzystać z oryginalnego artykułu, aby uzupełnić ten brak podczas lektury. Rozprawa zawiera też pewną liczbę usterek typograficznych oraz gramatycznych, które tu pominiemy.

Niezależnie od powyższych uwag krytycznych rozprawę pana Ryszarda Veynara uważam za wartościową badawczo. Podjęto w niej szereg problemów praktycznych i zaproponowano rozwiązania, które nawet jeżeli nie są ostateczne, to mają element pomysłowości i nowości. Dość zaskakująca wydaje się wykazana w pracy słabość ataku kryptograficznego z opóźnionym pomiarem. Koncepcja, by zbadać teleportację kwantową tak, jak to zrobiono w rozprawie, dowodzi między innymi, że paradygmat LOCC, w którym komunikacja klasyczna nic nie kosztuje, przyjmowano w przypadku teleportacji do tej pory w literaturze zbyt dosłownie. Badania nad znaczeniem mocy lasera dla kryptografii mają oczywiste znaczenie praktyczne, podobnie jak nowy test splątania, który może przyspieszyć wstępne fazy eksperymentów kwantowo-optycznych. Interesującym pytaniem badawczym na przyszłość może być kwestia, czy istnieje szansa na wariant adaptacyjny tego protokołu, który choć w części usunąłby jego aprioryczny charakter oraz uwzględniał skończoną wielkość błędu doświadczalnego. Na koniec warto zaznaczyć, że choć pewnym mankamentem może być wieloautorski charakter prac stanowiących zasadniczą podstawę niniejszej rozprawy, to w znacznym stopniu aspekt ten jest równoważony przez wszechstronny charakter zaprezentowanych badań: od rozwiązań użytecznych pod kontem przyszłych zastosowań komercyjnych (protokoły SDI, problem pompowania laserowego), poprzez zagadnienie komunikacyjne z elementem Shannonowskim (kanał teleportacyjny), aż po zagadnienie fundamentalne, choć nacechowane dbałością o minimalizację praktycznych zasobów (test splątania).

W podsumowaniu pragnę stwierdzić, że w mojej opinii praca magistra Ryszarda Veynara w dostatecznym stopniu spełnia wszystkie ustawowe oraz zwyczajowe wymogi stawiane dysertacjom w procedurze ubiegania się o stopień naukowy doktora i tym samym wnoszę o dopuszczenie jej autora do dalszych etapów przewodu doktorskiego.