Uniwersytet Gdański

International Centre for Theory of Quantum Technologies

Gdańsk, 26.06.2025

Recenzja rozprawy doktorskiej

Rozprawa mgr Adama Widomskiego pt. „High-dimensional quantum key distribution with time-phase encoding" jest w istocie rozbudowaną dokumentacją eksperymentalnej dystrybucji klucza kwantowego (QKD) przeprowadzonej w Warszawie w 2024 roku przez mgr Widomskiego wraz ze współpracownikami. Układ rozprawy jest bardzo dobrze przemyślany i zaplanowany.

W pierwszych dwóch rozdziałach autor zamieścił wstęp oraz ogólny opis dziedziny, w której praca się porusza. W rozdziale 3 opisane są podstawowe zjawiska i metody eksperymentalne wykorzystywane w dalszej części. W tym miejscu szczególnie podoba mi się zachowanie dobrego balansu pomiędzy zawarciem wszystkich istotnych informacji, a wchodzeniem w zbędne szczegóły. Kolejne rozdziały dokumentują proces przygotowania i przeprowadzenia eksperymentu. W rozdziale 4 opisany jest nadajnik zdolny do przygotowywania wysokowymiarowych stanów kwantowych w dwóch komplementarnych bazach. Rozdział ten zawiera nie tylko opis samego urządzenia, ale także proces jego charakteryzacji. Rozdział 5 dotyczy odbiornika. Jest to najbardziej kreatywna część pracy gdzie zastosowano czasowy efekt Talbota do pomiaru stanów kwantowych zakodowanych w jednej z baz. Pozwala to na uproszczenie odbiornika i umożliwia łatwiejsze skalowanie układu do pracy ze stanami kwantowymi w wyższych wymiarach. Szósty rozdział łączy urządzenia opisane w dwóch poprzednich i przedstawia eksperymentalną realizację protokołu QKD opartego o czterowymiarową generalizację protokołu BB84, szczególną uwagę poświęcając procesowi kalibracji urządzeń. Ostatni rozdział stanowi krótkie podsumowanie wyników opisanych w poprzednich.

Rozprawa napisana jest w języku angielskim i nie zawiera istotnych błędów ortograficznych ani gramatycznych. Większość tekstu jest klarowna i dość łatwa do zrozumienia, choć pojawiają się w nim fragmenty z dużą ilością technicznego żargonu. Zdarzają się także akapity, których konstrukcja jest dość toporna, lecz nie wpływa to na możliwość prześledzenia zawartego w nich rozumowania. Rozprawa opatrzona jest bibliografią, która w większości jest bardzo dobrze dobrana choć zdarzają się wyjątki, które opiszę poniżej.

Merytoryczną wartość pracy oceniam bardzo wysoko. Eksperyment opisany w rozdziale 6 łączy w sobie kilka nowatorskich rozwiązań, takich jak zastosowanie czasowego efektu Talbota, kodowania informacji w wysokowymiarowych stanach kwantowych oraz układów PIC. Dzięki temu przyczynia się do znaczącego postępu w dziedzinie kwantowej dystrybucji klucza kryptograficznego. Z zawartych we wstępach rozdziałów informacji o wkładzie autora wynika także, że jego udział był kluczowy dla całości projektu.

International Centre for Theory of Quantum Technologies (ICTQT)
University of Gdańsk
tel. +48 58 523 51 80
e-mail: marcin.pawlowski@ug.edu.pl
ul. Jana Bażyńskiego 1A
80-309 Gdańsk, Poland
www.ug.edu.pl
www.ictqt.ug.edu.pl

Moje uwagi krytyczne skupiają się na prezentacji wyników, która nie jest najlepsza, zwłaszcza w początkowych rozdziałach. Odnoszę wrażenie, że autor skupił się na przedstawieniu własnej pracy w laboratorium (co jest częściowo zrozumiałe, biorąc pod uwagę etos pracy naukowca) lecz nie poświęcił wystarczającej uwagi reszcie rozprawy. Moje szczegółowe uwagi są następujące:

- W rozdziale 1 wspomniane jest wykorzystanie szyfru Vernama w QKD. Choć można wykazać, że w przypadku idealnej implementacji kryptosystemu jest on odporny na każdy rodzaj ataku, to ma on wystarczająco dużo wad (np. długość klucza czy szyfrowanie pojedynczych bitów), że nie jest rozważany jako opcja od zastosowanie w praktycznej dystrybucji klucza.
- W punkcie 2.1.5 gdzie wymienione są zalety układów PIC należałoby dodać stabilność zawartych w nich interferometrów zwłaszcza, że układy wykorzystywane w dalszych rozdziałach je posaidają.
- Moje największe zastrzeżenia budzi punkt 2.2.1, a zwłaszcza fragment o założeniach w realistycznych protokołach QKD. Zbudowanie zestawu spójnych założeń jest w takim przypadku dość trudnym zadaniem głównie przez to, że trudno jest precyzyjnie zdefiniować przymiotnik „realistyczny" w tym kontekście. Pomimo tego, lista założeń ułożona przez autora jest zdecydowanie nienajlepsza. Po pierwsze brakuje w niej założenia dotyczącego losowości wyboru stanów kwantowych przez nadajnik oraz baz pomiarowych przez odbiornik. Po drugie, stwierdzenie „quantum and classical devices are assumed secure" jest wysoce nieprecyzyjne. Zakładam, że autorowi chodzi tutaj o brak wycieku informacji z tych urządzeń, ale w realistycznej kryptografii takie założenie trudno przyjąć bez dodatkowych zabezpieczeń w protokole i jego implementacji. Po trzecie, założenie, że stany przygotowywane przez nadajnik są idealne nie jest ani realistyczne ani potrzebne. Nieduże odchylenia nie stanowią problemu.
- Także w punkcie 2.2.1 autor pisze „Device-dependent security proofs assume a prepare-and-measure protocol". Nie jest to prawdą. O ile w kryptografii niezależnej od urządzeń protokoły prepare-and-measure są niemożliwe, nie oznacza to, że w standardowej są jedyną opcją. Przykładem jest protokół BBM92.
- W punkcie 2.2.3, opisując protokół E91, autor pisze: „Alice and Bob perform Bell state measurements". Przez "Bell state measurements" rozumiemy zwykle pomiary rozróżniające 4 maksymalnie splątane stany 2 kubitów. E91 nie wykorzystuje takich pomiarów. Autor mógł mieć na myśli to, że w tym protokole wykorzystywane są te same pomiary co w nierówności Bell-CHSH, ale nie uwzględnia to dodatkowej, trzeciej bazy pomiarowej wykorzystywanej przez jedną ze stron.
- Tłumacząc równanie (2.7) autor odnosi się do pracy [91]. Nie jest to ani praca gdzie te równanie zostało wyprowadzone, ani praca przeglądowa tłumacząca jego znaczenie, lecz jedna z tysięcy, która je wykorzystuje. Podobna sytuacja pojawia się w rozprawie kilkakrotnie.
- W punkcie 2.2.4 autor pisze „Mutual information between Alice and Bob is proportional to the bit value and error they make in communication". Po pierwsze nie jest jasne czym jest "bit value" w tym kontekście. Po drugie informacja wzajemna może być monotoniczną funkcją tych wartości, ale na pewno nie jest do nich proporcjonalna.

International Centre for Theory of Quantum Technologies (ICTQT)
University of Gdańsk
tel. +48 58 523 51 80
e-mail: marcin.pawlowski@ug.edu.pl
ul. Jana Bażyńskiego 1A
80-309 Gdańsk, Poland
www.ug.edu.pl
www.ictqt.ug.edu.pl

- Symbol „μ”, który jest w tekście po (2.8) nie pojawia się w tym równaniu.
- W punkcie 2.2.4 przy opisie metod użytych do mitygacji ataku PNS należałoby opisać atak, któremu zapobiegają. Metody typu „decoy-state” nie maja zastosowania przy atkach wykorzystujących jedynie pasywny odbiór części sygnału, który jest nieodróżnialny od strat w światłowodzie.
- Opis wzoru (2.13) zawiera symbole i oraz Y_1, które nie pojawiają się we wzorze.
- W punkcie 5.2.2 autor pisze: „The following mathematical interlude serves as a
- demonstration showing that the optimal approach is to simply select the most probable symbol for a given detection time” jednak żaden matematyczny przerywnik nie pojawia się po tym zdaniu.
- W punkcie 5.3 autor pisze: “The results indicate that the optimal strategy is always to select the most probable symbol at a given detection time.” Nie został przedstawiony dowód, że jest to prawda. W dodatku taki rodzaj przetwarzania informacji zmniejsza informację wzajemną pomiędzy nadawcą i odbiorcą i redukuje prędkość generacji klucza.
- Punkt 6.1.2 nie jest opisany w jasny sposób. Nie wynika z niego jak TBS prowadzi do zrównania efektywności detekcji w obu bazach.

Oprócz powyższych mam też 2 ogólne uwagi:

- Punkt 2.2 jest dość dokładnym opisem protokołów dystrybucji klucza jednak ograniczonym wyłącznie do kubitów. Takie ograniczenie nie jest zbyt sensowne w rozprawie, która w samym tytule ma wysokowymiarową QKD.
- Zastanawia mnie czy zamiast dodawać do implementacji dodatkowy element – TBS, nie proście byłoby uwzględnić różną efektywność detektorów na poziomie teorii. Taka uwaga jest na tyle oczywista, że może przyjść na myśl większości czytających dlatego dobrze byłoby w rozprawie zawrzeć na nią odpowiedź.

Powyższe uwagi, choć liczne, nie wpływają na moją bardzo pozytywną ocenę merytorycznych wyników zawartych w rozprawie.

Podsumowując: Praca mgr Adama Widomskiego jest dojrzałym, nowatorskim i wartościowym dziełem naukowym. Spełnia wszystkie wymagania stawiane rozprawom doktorskim w dziedzinie fizyki i stanowi istotny wkład w rozwój technologii dystrybucji klucza kwantowego. Z pełnym przekonaniem wnioskuję o dopuszczenie rozprawy do publicznej obrony oraz przyznanie autorowi stopnia naukowego doktora nauk fizycznych.

Z poważaniem,

Marcin Pawłowski

Elektronicznie podpisany przez Marcin Pawłowski
Data: 2025.07.08 11:25:34 +02'00'

Marcin Pawłowski.

International Centre for Theory of Quantum Technologies (ICTQT)
University of Gdańsk

tel. +48 58 523 51 80
e-mail: marcin.pawlowski@ug.edu.pl

ul. Jana Bażyńskiego 1A
80-309 Gdańsk, Poland

www.ug.edu.pl
www.ictqt.ug.edu.pl