

dr hab. inż. Marek Sawerwain, prof. UZ
Instytut Sterowania i Systemów Informatycznych
Wydział Informatyki, Elektrotechniki i Automatyki
Uniwersytet Zielonogórski
ul. Licealna 9
65-417 Zielona Góra
tel.: 68 328 2321
e-mail: M.Sawerwain@issi.uz.zgora.pl

Zielona Góra, 13.08.2026r.



Recenzja rozprawy doktorskiej Pana mgra Roberta Okuły

Szacowanie informacji kwantowej: relacje pomiędzy miarami w kryptografii kwantowej

(in english: *Quantifying Quantum Information: Relationships between
measures in Quantum Cryptography*)

Przedmiotem recenzji jest rozprawa doktorska pt. „Szacowanie informacji kwantowej: relacje pomiędzy miarami w kryptografii kwantowej” przygotowana przez Pana mgra Roberta Okułę pod kierunkiem dr hab. inż. Piotra Mironowicza.

1 Ogólna charakterystyka pracy i jej tematyka

Informatyka kwantowa to obecnie dynamicznie rozwijająca się dziedzina nauki obejmująca zarówno zagadnienia sprzętowe dotyczące fizycznej realizacji modelu obliczeń kwantowych, a także zagadnienia aplikacyjne tj. m.in. rozwój algorytmów kwantowych oraz zadania teoretyczne dotyczące fundamentalnych pytań dotyczących modelu obliczeniowego, granic obliczalności oraz istoty pojęcia informacji kwantowej.

W obszarze informatyki kwantowej niezwykle ważną rolę odgrywają zagadnienia bezpieczeństwa tj. kryptografia kwantowa. Dostarcza ona nowych rozwiązań w zakresie nowoczesnych metod kryptograficznych, co naturalnie staje się istotnym zagadnieniem ważnym dla obecnie stosowanych rozwiązań w szeroko rozumianym zakresie bezpieczeństwa. Recenzowana praca odnosi się do zagadnień kryptografii kwantowej, a dokładniej do badania zależności między różnymi miarami informacji kwantowej. Jak podaje jej Autor, ma ona na celu wzmocnienie teoretycznych podstaw kryptografii kwantowej. Autor pracy analizuje protokoły, opisuje i rozszerza metody certyfikacji odnoszące się do bezpieczeństwa oraz jakości generowanych danych np. kluczy. W swojej pracy wykorzystał techniki programowania nieliniowego oraz pół-określonego, a także przedstawił analityczne rozważania na temat podejmowanych w swojej rozprawie zagadnień.

Po analizie wstępu pracy, niestety w pracy brakuje typowego sformułowania tezy głównej, Autor określił następujące zagadnienia jako główne tezy swojej pracy:

- (T1) analiza zagadnienia bezpieczeństwa kwantowej dystrybucji w kontekście kwantowego determinizmu,
- (T2) certyfikacji kwantowego źródła losowości opartego o splątanie z wykorzystaniem entropii Shannona,
- (T3) certyfikację nierówności Bella w kontekście generowania losowości,
- (T4) poszukiwanie optymalnych protokołów certyfikacji do zadań przedstawionych w (T2) i (T3),
- (T5) analiza związku między nie-lokalnością Bella, a kwantowym dyskordem (Autor analizował numerycznie korelację dla jakiej wartości następuje łamanie nierówności Bella a dyskordem).

Przedstawione tezy odnoszą się zatem bezpośrednio do tematu pracy tj. badania relacji pomiędzy miarami kwantowych korelacji w obszarze kwantowej kryptografii a w szczególności bezpieczeństwa dystrybucji klucza kwantowego i jakości danych losowych. Tak sformułowany temat oraz tezy rozprawy odnoszą się naturalnie bezpośrednio do prac w dziedzinie informatyki kwantowej oraz do obszaru dyscypliny informatyki technicznej i telekomunikacja.

W rozprawie pokazano rolę otoczenia nie tylko jako źródła dekoherencji ale Autor wskazuje iż otoczenie może przyczyniać się do wycieku informacji właśnie do otoczenia co może wzmacniać podatność kanału kwantowego na ataki typu ang. side-channel. Taka analiza naturalnie stanowi duży walor rozprawy i pokazuje istotną rolę otoczenia w konstrukcji protokołów kryptografii kwantowej.

W przedstawionych tez, można wskazać też na drugi obszar wyników przedstawionych w rozprawie dotyczący certyfikacji źródeł losowości leżących w nierównościach Bella. Autor pokazuje także trzeci obszar rezultatów tj. teza (T5) wskazująca między nie-lokalnością Bella a kwantową korelacją typu dyskord, która to, co jest bardzo ważne, wskazuje na najsłabsze kwantowe korelacje nawet przy braku obecności kwantowego splątania.

Praca zatem oprócz rozważań teoretycznych wskazuje również na znacznie praktyczne otrzymanych rezultatów, a także przeprowadza eksperymenty które w sposób praktyczny pokazują znaczenie dyskutowanych rozwiązań oraz wnosi też kilka istotnych rezultatów analitycznych w obszarze dystrybucji klucza, certyfikacji i nierówności Bella, co świadczy o jakości osiągniętych przez Autora rozprawy wyników.

2 Zawartość rozprawy

Całość rozprawy to 149 stron, gdzie pierwsze 15 stron to strona tytułowa, spis treści, spis publikacji, streszczenie, rozdział wprowadzający. Następnie, rozprawa przedstawia trzy rozdziały wstępne a pozostałe rozdziały oraz Dodatek A stanowią główny trzon rozprawy.

W początkowych rozdziałach Autor przedstawia informacje wstępne stanowiące podstawę dla dalszych rozważań podejmowanych w rozprawie. Rozdział pierwszy przedstawia wybrane istotne informacje w kontekście tematy dotyczące modelu obliczeń kwantowych. Rozdział drugi przedstawia na podobnej zasadzie informacje dotyczące obszaru kryptografii kwantowej. A rozdział trzeci

nakreśla teorię kwantowego Darwinizmu, która to jest podstawą rezultatów omawianych w dalszej części rozprawy.

Rozdziały czwarty, piąty oraz szósty przedstawiają oryginalne rezultaty odnoszące się do tez postawionych we wstępnym rozdziale rozprawy. Rozdział czwarty przedstawia zagadnienie dekoherencji oraz kwantowej dystrybucji klucza, jednakże otoczenie tu nie jest traktowane jako źródło losowości ale jako świadek, do którego przekazywana jest część informacji podczas pomiaru, co potencjalnie oznacza możliwość ataku i ten aspekt jest analizowany przez Autora.

W rozdziale piątym analizowano zagrożenia certyfikacji źródeł losowych, a rozdział szósty dyskutuje związek między relacją dyskoru kwantowego, a nierównością Bella. Wyniki z pracy uzupełnia także Dodatek A, gdzie podano techniczne rezultaty dotyczące rozkładu QR oraz wprowadzenie drugiej pochodnej entropii Shannona. Pracę podsumowują naturalnie uwagi końcowe, lista ilustracji i tabel, indeks oraz obszerna, bo licząca 210 pozycji bibliografia.

Ogólnie, przyjęty podział na wstęp, rozdziały wprowadzające, rozdziały właściwe tematyce rozprawy i dodatki uzupełniające pozwolił Autorowi na pełną prezentację osiągniętych wyników i struktura pracy jest prawidłowa i można ją ocenić jako bardzo dobrą.

3 Najważniejsze osiągnięcia zaprezentowane w rozprawie

Główne rezultaty osiągnięte przez Autora rozprawy przedstawiono w rozdziałach od trzeciego do szóstego. Odnoszą się one kolejno do tez (T1)-(T5) przedstawionych na początku rozprawy.

3.1 Dekoncentracja oraz dystrybucja klucza kwantowego

Teza (T1) jest dyskutowana w rozdziale czwartym. Autor wykazuje iż pomiar w kontekście kwantowego darwinizmu, może doprowadzić do ujawnienia danych klucza, co pokazano na przykładzie protokołu BB84. Należy też podkreślić iż rozdział ten powstał na podstawie wyników zaprezentowanych w pracy (P1). W rozdziale przeanalizowano jak atakujący może odzyskać dane wykorzystując poziomy otoczenia. Wartości tego prawdopodobieństwa ogólnie dla wielu warstw podano w Tezie 1, na stronie 66 pracy. Przy czym wcześniejsze rezultaty 4.11, 4.12 dotyczą pojedynczego poziomu i podwójnego poziomu.

Autor także przedstawia eksperymenty numeryczne pokazujące rozróżnialność stanów otoczenia, i wprost pokazuje na przykładzie Tabeli 4.1 ile bitów klucza kwantowego atakujący może odgadnąć kontrolując otoczenie.

W tej części Autorowi udało się pokazać interesujący i niedyskutowany wcześniej schemat pomiaru który pozwala na analityczną i także eksperymentalną analizę bezpieczeństwa protokołu BB84. I wskazuje jednoznacznie na sposób konstrukcji rejestru kwantowego tak aby możliwe było ograniczenie możliwości ataku na proces generowania klucza kwantowego. Autor podkreśla także znaczenie jakości przeprowadzania pomiaru jako operacji która może w sposób istotny przyczynić się do stopnia bezpieczeństwa generowanego klucza kwantowego.

3.2 Certyfikacja losowości

Tezy (T2) oraz (T3) są przedmiotem rozdziału piątego. Autor prezentuje procedurę certyfikacyjną strona 79 rozprawy, a następnie w dalszej części rozdziału omawiane są wartości entropii Shannona dla różnych wariantów nierówności Bella. Wyniki zostały opublikowane w pracy (P2) oraz preprintcie (P3). Różne warianty certyfikacji dla wybranych typów nierówności zostały zaprezentowane w rozdziale 5.2. W ten sposób Autor pokazał iż możliwe jest testowanie jakości uzyskanych w ten sposób losowych wartości w kontekście entropii Shannona oraz zmieniającej się wartości szumu. Oprócz numerycznych wyników dla konkretnych przypadków nierówności w rozdziale 5.2.6 pokazano dolne ograniczenia na entropię. Istotnym wynikiem jest tu też rozdział 5.3 (związany z tezą T(4)), gdzie zaprezentowana dyskusja jak poszukiwać lepszych protokołów certyfikacji na przykładzie kilku różnych schematów pomiaru, co ma duże znaczenie dla praktycznego zastosowania źródeł kwantowej losowości, aby maksymalizować wartość entropii na wybranych wartości szumu.

3.3 Nie-lokalność Bella oraz kwantowy dyskord

Nierówności Bella, to uznane narzędzie do analizy splątania, losowości w obszarze zastosowań metod kwantowych. Jednakże, jak celnie zauważa Autor nie jest jedyny i takim jest pojęcie kwantowego dyskordu. Autor w omawiając zagadnienia dot. tezy T(5) pokazuje jak powiązać nie-lokalność Bella wraz pojęciem dyskordu. Rezultaty zaprezentowane w rozdziale mają charakter numeryczny, to w interesujący sposób łączą te dwa pojęcia i jak się wydaje jest to bardzo interesujące połączenie tych dwóch pojęć. Autor pokazuje też jak różne typy nierówności Bella i dyskord są zależne od wartości szumu kwantowego w badanym układzie w kontekście utraty kwantowych korelacji obecnych w systemie.

3.4 Uwagi krytyczne oraz pytania

Praca, co naturalnie, obszernie przedstawia uzasadnienie przyjętych tez, jednakże można nakreślić kilka pytań i dodatkowych problemów do Autora pracy, a przedstawiałyby się one następująco:

- (PY1) na stronie 66 pracy, podano ogólniejsze relacje dla prawdopodobieństwa zgadnięcia oraz szybkości generacji klucza, jednak sposób wyprowadzenia tego wzoru został podany w ograniczony sposób, toteż należałoby się zapytać o nieco szerszy opis wyprowadzenia tych relacji,
- (PY2) w analizie certyfikacji nierówności Bella, w wielu przypadkach jednoznacznie widać spadek wartości entropii, jak wygląda szybkość tego spadku, i jak bardzo jest ten spadek jest wrażliwy na poziom szumu?,
- (PY3) analogicznie dla wartości dyskordu, który rośnie wraz ze wzrostem wartości szumu, również można się zapytać o szybkość tego wzrostu?,
- (PY4) w pracy przeprowadzono szereg eksperymentów numerycznych, jednakże brakuje technicznych informacji, na jakim sprzęcie, ile trwały, jakie wymagania pamięciowe należało spełnić, czy też jaki typ oprogramowania został wykorzystany do realizacji konkretnego eksperymentu, dlatego wydaje się zasadne aby w ramach odpowiedzi Autor rozprawy doprecyzował te aspekty.

3.5 Pytania ankietowe bezpośrednie do rozprawy

W tej części recenzji znajdują się odpowiedzi na ankietowe pytania krótko charakteryzujące całość recenzowanej rozprawy.

(PA1) Jaki jest problem naukowy (teza) rozprawy i czy został on trafnie i jasno sformułowany?

ODP.

Głównym tematem jest badanie jakości bezpieczeństwa dystrybucji klucza kwantowego oraz certyfikacji źródeł losowości kwantowych, oba te zagadnienia poprzez tezy formułowane przez Autora zostały zdefiniowane w sposób niebudzący wątpliwości.

(PA2) Czy Autor rozwiązał postawiony problem i czy użył do tego właściwych metod dowodząc, że posiadał umiejętności związane z metodyką i metodologią prowadzenia badań naukowych?

ODP.

Postawione tezy oraz ich przedstawienie nie budzi żadnych wątpliwości co do jakości osiągniętych rezultatów, a sposób prezentacji mimo braku wyższego rygoru matematycznego, w postaci lematów, stwierdzeń dowodów, jednoznacznie pokazuje umiejętności w posługiwaniu się omawianymi pojęciami, oraz przeprowadzeniem analizy teoretycznej

(PA3) Czy tematyka rozprawy jest aktualna lub dostatecznie ważna?

ODP.

Tak, informatyka kwantowa to nowoczesny dział informatyki którego dynamiczny rozwój można obserwować w ciągu ostatnich dwudziestu, trzydziestu lat. A rozwój metod kryptografii kwantowej, to niewątpliwie jeden z jej ważniejszych obszarów. Praca w podejmowanym obszarze zagadnień dostarcza nietrywialnych narzędzi do oceny jakości dystrybucji klucza o certyfikacji źródeł losowości.

(PA4) Na czym polega oryginalny dorobek Autora i jakie jest jego znaczenie poznawcze lub przydatność praktyczna dla nauki lub techniki?

ODP.

Zaproponowany mechanizm certyfikacji losowości, oraz szukanie relacji pomiędzy wartościami dyskordu oraz nierównościami Bella, to bardzo interesujące zagadnienia omawiane w pracy. Jednakże, w szczególności pokazanie roli otoczenia jako świadka w procesie generacji klucza, pokazuje iż bezpieczeństwo oferowane przez metody kwantowe nadal wymaga dalszych badań i pozwala na wskazywanie nowych obszarów, które pozwalają na dalsze jego zwiększanie oraz pokazywanie potencjalnych luk do ataku. Świadomość tych ograniczeń naturalnie poszerza naszą wiedzę o bezpieczeństwie oferowaną przez kwantową kryptografię.

(PA5) Czy rozprawa świadczy o dostatecznej wiedzy Autora, wiedzy na zaawansowanym poziomie, o charakterze podstawowym dla dziedziny nauk technicznych oraz o charakterze szczegółowym, odpowiadającej obszarowi prowadzonymi badan naukowych?

ODP.

Tak, w pracy znalazły się zarówno wyniki o charakterze analitycznym np. dolne ograniczenie wartość entropii Shannona, a także rezultaty eksperymentów numerycznych. A biegłość w posługiwaniu się pojęciami z obszary informatyki kwantowej, kryptografii oraz teorii informacji jest w pracy pokazana na wysokim poziomie.

(PA6) Czy rozprawa obejmuje najnowsze osiągnięcia nauki i świadczy o znajomości współczesnej literatury z dyscypliny naukowej, której dotyczy?

ODP.

Tak, o czym wspomniano już w odp. do (PA3), dodatkowo Autor pracy opracował szeroką bibliografię co świadczy o bardzo obszernej wiedzy dotyczącej diskutowanych zagadnień.

(PA7) Jakie są wady i słabe strony rozprawy?

ODP.

W ogólności praca została napisana staranie, jednakże Autor nie dostarczył np. w postaci dodatku aspektów numerycznych przeprowadzonych eksperymentów, brakuje także aspektów technicznych które mogłyby być wartościowe dla osoby, która chciałaby samodzielnie przeprowadzić podobne obliczenia. Praca choć niewątpliwie posiada także charakter teoretyczny jednakże nie oferuje bardzo rygorystycznego stylu prezentacji pojęć matematycznych, brakuje bardziej formalnego podziału na lematy, stwierdzenia i dowody. Jednakowoż, mimo tego braku lektura pracy jednoznacznie pokazuje i uzasadnia prawdziwość analizy i poprawności eksperymentów przeprowadzonych przez Autora.

(PA8) Do której z następujących kategorii Recenzent zalicza rozprawę:

- a/ nie spełnia wymagań,
- b/ wymagająca wprowadzenie poprawek i ponownego recenzowania,
- c/ zadowalająco spełniająca wymagania,
- d/ wyraźnie wykraczająca poza poziom przeciętny (spełniająca wymagania z nadmiarem),
- e/ wybitna.

ODP.

Odpowiedzi na wcześniejsze pytania pozwalają na wskazanie, iż praca ta spełnia wymagania z nadmiarem (d/), choć nie jest wolna o braku pewnych szczegółów w obszarze przeprowadzonych eksperymentów numerycznych oraz większego rygoru matematycznego prezentacji otrzymanych rezultatów analitycznych.

4 Podsumowanie oraz konkluzja końcowa

Dorobek publikacyjny Autora bezpośrednio odnoszące się do tematyki podejmowanej w rozprawie wprost podane przez Autora dysertacji na stronie piętnastej to:

- (P1) Robert Okuła, Piotr Mironowicz, How decoherence affects the security of BB84 quantum key distribution protocol. Quantum Information Processing, 24(2). February 2025. DOI: 10.1007/s11128-025-04650-8
- (P2) Robert Okuła, Piotr Mironowicz, Device-independent Shannon entropy certification. New Journal of Physics, 27(11):114519, November 2025, DOI: 10.1088/1367-2630/ae20b2
- (P3) Robert Okuła, Piotr Mironowicz, Extensive search of Shannon entropy-based randomness certification protocols, 2025, arXiv: 2511.22771, preprint.

W mojej ocenie wyniki przedstawione w rozprawie pozwalają utworzyć system oceny jakości i bezpieczeństwa dystrybucji klucza kwantowego, a zaproponowane rozwiązanie certyfikacji, czy też analizy dyskoru oraz nierówności Bella, to bardzo nowatorskie i interesujące narzędzia do badania wybranych aspektów w obszarze informatyki kwantowej i kryptografii, i są one istotnym oraz znaczącym wkładem w rozwój dyscypliny naukowej Informatyka Techniczna i Telekomunikacja.

4.1 Konkluzja końcowa

W konkluzji końcowej, na podstawie przedstawionych wcześniej uwag i komentarzy, należy jednoznacznie stwierdzić iż rozprawa doktorska Pana mgra Roberta Okuły pt. „Szacowanie informacji kwantowej: relacje pomiędzy miarami w kryptografii kwantowej” (ang. Quantifying Quantum Information: Relationships between measures in Quantum Cryptography) spełnia wymagania ustawy właściwej dla dziedziny nauk inżyneryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja, zatem wnoszę o jej przyjęcie oraz dopuszczenie do publicznej obrony.

13.08.2026 Marek Szczerbowicz
.....
(data oraz podpis)