

dr hab. inż. Łukasz Paweła
Instytut Informatyki
Teoretycznej i Stosowanej
Polskiej Akademii Nauk
ul. Bałtycka 5, 44-100 Gliwice

Gliwice, 24 lipca 2026 r.

Recenzja rozprawy doktorskiej mgr inż. Robert Okuły „Quantifying Quantum Information: Relationships between measures in Quantum Cryptography”

Uwagi wstępne

Forma drukowana recenzowanej rozprawy obejmuje 149 stron. Praca ma charakter klasycznej monografii, jest napisana w języku angielskim i zawiera:

- streszczenia w językach polskim i angielskim;
- wykaz notacji oraz wykaz akronimów;
- przedmowę zawierającą wykaz artykułów naukowych, których wyniki weszły w skład rozprawy;
- sześć rozdziałów, z których trzy pierwsze stanowią wprowadzenie teoretyczne, a trzy kolejne prezentują wyniki własne Doktoranta;
- podsumowanie;
- wykaz literatury liczący 210 pozycji;
- spisy rysunków i tabel oraz indeks rzeczowy;
- dwa dodatki: **A**, dotyczący rozkładu QR (na czynnik ortogonalny lub unitarny Q oraz czynnik górnotrójkątny R), oraz **B**, zawierający wprowadzenie drugiej pochodnej entropii Shannona.

Tytuł pracy oddaje jej zawartość, a przyjęty układ pracy jest właściwy. Rozprawa dotyczy zależności między różnymi miarami informacji kwantowej w kontekście kryptografii kwantowej, ze szczególnym uwzględnieniem certyfikacji losowości niezależnej od urządzeń (ang. *device-independent*, DI) oraz wpływu dekoherencji na bezpieczeństwo kwantowej dystrybucji klucza (ang. *quantum key distribution*, QKD), w szczególności protokołu Bennetta i Brassarda z 1984 r. (BB84).

Praca zawiera wyniki opublikowane wcześniej przez Autora we współautorstwie z promotorem:

- [1] R. Okuła, P. Mironowicz, *How decoherence affects the security of BB84 quantum key distribution protocol*, Quantum Information Processing 24(2), 2025.
- [2] R. Okuła, P. Mironowicz, *Device-independent Shannon entropy certification*, New Journal of Physics 27(11):114519, 2025.
- [3] R. Okuła, P. Mironowicz, *Extensive search of Shannon entropy-based randomness certification protocols*, arXiv:2511.22771.

Trzecia z wymienionych prac pozostaje, według strony arXiv sprawdzonej 20 lipca 2026 r., preprintem w wersji v1, bez danych publikacji czasopismowej. Nie wpływa to na formalną ocenę rozprawy mającej postać monografii, jednak odnotowuję ten fakt dla porządku. Rozdział 6 zawiera ponadto wyniki wcześniej niepublikowane.

Przedmiot rozprawy

Rozdziały 1–3 stanowią wprowadzenie do formalizmu teorii informacji kwantowej: przestrzeni Hilberta, pomiarów, operatorów Bella, miar entropowych, dyskoru kwantowego, metod numerycznych z hierarchią Navascuésa–Pironio–Acína (NPA) na czele, kryptografii kwantowej oraz kwantowego darwinizmu. Materiał ten jest dobrany trafnie i w znacznej części jest wykorzystywany w rozdziałach wynikowych.

Rozdział 4 analizuje oryginalne i interesujące pytanie badawcze: czy proces dekoherencji, który zgodnie z teorią kwantowego darwinizmu wymaga propagacji informacji do środowiska, może otworzyć kanał boczny, analogiczny do klasycznych ataków van Ecka, w protokole BB84. Autor proponuje model środowiska warstwowego, wyprowadza wyrażenia na prawdopodobieństwo odgadnięcia bitu klucza i generowania klucza oraz prowadzi niezależną analizę numeryczną rozróżnialności stanów środowiska na podstawie pomiaru Helstro-

ma. Koncepcja jest ciekawa, choć przejście od średniego prawdopodobieństwa odgadnięcia do informacji wzajemnej i ilości klucza wymaga ponownej analizy, o czym piszę niżej.

Rozdział 5, najobszerniejszy i moim zdaniem najwartościowszy, proponuje metodę szacowania losowości z użyciem entropii Shannona. Ograniczenia na prawdopodobieństwa wyników uzyskiwane są na poziomie Q_2 hierarchii NPA za pomocą programowania półokreślonego (ang. *semidefinite programming*, SDP) i programu MOSEK, a następnie używane jako więzy niewypukłej optymalizacji entropii. Autor stosuje algorytm *Constrained Optimization BY Quadratic Approximations* (COBYQA) wraz z heurystyką *basin-hopping*. Motywacją wyboru entropii Shannona zamiast standardowej min-entropii jest asymptotyczna własność ekwipartycji (ang. *asymptotic equipartition property*, AEP) oraz znane oszacowania dla ciągów niezależnych próbek.

Metoda zostaje zastosowana do czterech rodzin nierówności Bella: nierówności Clausera–Horne’a–Shimony’ego–Holta (CHSH) i jej wersji zmodyfikowanej (ModCHSH), nierówności Braunsteina–Cavesa, rodzin I_1/I_2 oraz nierówności Woollortona–Browna–Colbecka. Rozdział obejmuje również analityczną dolną granicę entropii, scenariusz trzywynikowy oraz przegląd ponad pół miliona wyrażeń Bella wraz z analizą samotestowania (ang. *self-testing*) wybranych kandydatów. Zakres obliczeń świadczy o bardzo dobrym opanowaniu programowania półokreślonego, relaksacji NPA i heurystycznego przeszukiwania przestrzeni rozwiązań. Jednocześnie certyfikowany status części wartości otrzymanych przez niewypukłą optymalizację powinien zostać doprecyzowany.

Rozdział 6 bada numerycznie zależność między dyskordem kwantowym a łamaniem sześciu nierówności Bella. Autor wykorzystuje piętnastoparametrowy opis mieszanych stanów dwukubitowych, związany z parametryzacją specjalnej grupy unitarnej stopnia czwartego $SU(4)$, oraz optymalizuje dyskord przy zadanej wartości wyrażenia Bella. Zaobserwowane rodziny wyników lokalnej optymalizacji stanowią interesujący punkt wyjścia do dalszych badań, nie należy ich jednak utożsamiać z udowodnionymi gałęziami minimów globalnych.

Całość pokazuje, że Doktorant potrafi sformułować problem badawczy, dobrać narzędzia analityczne i numeryczne oraz osadzić wyniki w literaturze przedmiotu. Na uznanie zasługują szeroki zakres tematyczny, indeks rzeczowy oraz przedstawienie części ograniczeń zastosowanych metod. W kilku miejscach zakres gwarancji formułowanych na podstawie obliczeń numerycznych jest jednak szerszy, niż uzasadnia to przedstawiona procedura.

Uwagi krytyczne, dyskusyjne i redakcyjne

1. Na s. 11–12 w wykazie akronimów wyraz „distrbution” występuje trzykrotnie zamiast „distribution”, w rozwinięciach skrótów QKD, BB84 i E91 (protokół Ekerta z 1991 r.).
2. Na s. 17 zapisano $\langle \phi | \psi \rangle = \langle \phi | \psi \rangle^*$, co oznaczałoby, że iloczyn jest zawsze rzeczywisty. Poprawnie $\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^*$.
3. Na s. 19 dla bazy obliczeniowej indeksowanej od zera wektor $|i\rangle$ ma i zer przed jedyneką oraz $d - i - 1$ zer po niej, a nie $i - 1$ zer po obu stronach. W akapicie o pomiarze opisywanym miarą operatorową o wartościach dodatnich (ang. *positive operator-valued measure*, POVM) brakuje stanu w zdaniu poprzedzającym regułę Borna. Najogólniejsza poprawna postać to $p(m) = \text{Tr}(\rho E_m)$, natomiast $p(m) = \langle \psi | E_m | \psi \rangle$ jest przypadkiem stanu czystego. Wektory bazy obliczeniowej i Hadamarda nie są ponumerowane. Sam brak numeru nie jest błędem, lecz wzory centralne albo przywoływane dalej powinny być numerowane konsekwentnie.
4. Na s. 28 definicja odległości całkowitego wahania pozostaje bez numeru, mimo że jest niezbędna do numerowanej definicji wygładzonej min-entropii (1.18). Jest to kolejny przykład niespójnej, a nie po prostu oszczędnej, numeracji wzorów.
5. Na s. 36 omówienie sprowadzenia pomiarów POVM do pomiarów projekcyjnych przez dylatację Naimarka występuje dwukrotnie niemal w tej samej postaci.
6. Na s. 39–42 blisko trzy strony poświęcono szyfrom biblijnym, skytale, Enigmie, algorytmowi Rivesta–Shamira–Adlemana (RSA), kryptografii krzywych eliptycznych (ang. *elliptic-curve cryptography*, ECC) i schematowi ElGamala są, w mojej ocenie, nieproporcjonalnie obszerne względem celu rozprawy. Ważniejszy jest błąd pojęciowy na s. 41. Termin *perfect forward secrecy* (PFS) nie oznacza gwarancji, że problem matematyczny stanowiący podstawę kryptosystemu nigdy nie zostanie rozwiązany. PFS jest własnością protokołu ustanawiania klucza: późniejsze ujawnienie długoterminowego materiału kluczowego nie powinno pozwolić na odtworzenie kluczy zakończonych sesji, o ile efemeryczne sekrety sesyjne zostały usunięte. *Harvest now, decrypt later* (HNDL, „przechwyć teraz, odszyfruj później”) jest strategią przeciwnika, który zapisuje dziś szyfrogram i publiczny transkrypt, aby odszyfrować je później po uzyskaniu nowego

algorytmu lub większej mocy obliczeniowej, bez konieczności późniejszego przejścia klucza długoterminowego. Są to własności logicznie odrębne. Uwierzytelniona efemeryczna wymiana Diffiego–Hellmana może zapewniać PFS wobec późniejszej kradzieży klucza uwierzytelniającego, a jednocześnie być podatna na HNDL, jeśli przyszły komputer kwantowy pozwoli rozwiązać problem zapisany w publicznym transkrypcie. Kryptografia postkwantowa (ang. *post-quantum cryptography*, PQC) ma przeciwdziałać znanym atakom kwantowym, lecz nadal opiera się na założeniach obliczeniowych. Może być stosowana w protokole z PFS albo bez tej własności, sama nie zapewnia bezpieczeństwa informacyjno-teoretycznego ani wieczystej poufności. Jeżeli zamiarem Autora było przeciwstawienie QKD kryptografii postkwantowej, właściwym rozróżnieniem jest zatem bezpieczeństwo informacyjno-teoretyczne wobec bezpieczeństwa opartego na założeniach obliczeniowych, a opisywanym zagrożeniem jest HNDL, nie brak PFS.

7. Na s. 49 zapowiedziano gwarancję „genuine, private randomness” nawet dla urządzeń przygotowanych przez przeciwnika. W rozdziale 5 minimalizowana jest jednak entropia rozkładu wyników $H(AB|XY)$, bez jawnego systemu informacji ubocznej przeciwnika E i bez przejścia do $H(AB|XYE)$. Wysoka entropia rozkładu mieszanego nie gwarantuje sama przez się prywatności wobec podmiotu znającego składnik mieszaniny. Proszę o wyjaśnienie, czy proponowany certyfikat dotyczy entropii wyjściowego zachowania przy przyjętym założeniu prób niezależnych o jednakowym rozkładzie (ang. *independent and identically distributed*, i.i.d.) i izolacji urządzeń, czy również prywatnej losowości względem klasycznej lub kwantowej informacji ubocznej. W tym drugim przypadku w rozprawie brakuje odpowiedniego kroku dowodowego. Uwaga o mieszaniu strategii na s. 92–93 nie zastępuje jawnego modelu systemu E .
8. Na s. 54–58 opis sita przewidywalności mówi o maksymalizacji funkcjonału, którym ma być entropia von Neumanna lub czystość. Kryteria te mają przeciwne kierunki: stany wskaźnikowe minimalizują produkcję entropii, czyli zachowują możliwie dużą czystość i przewidywalność. Ponadto w równaniu (3.1) iloczyn powinien przebiegać po nieobserwowanym fragmencie $\bar{F}$, po którym wykonuje się ślad częściowy:

$$\Gamma_F(t) = \sum_{i \neq j} |\sigma_{ij}| \prod_{k \in \bar{F}} |\gamma_{ij}^{(k)}(t)|, \quad |\bar{F}| = (1 - f)M,$$

a nie po obserwowanej frakcji o liczności fM . W tym samym fragmencie liczba podukładów środowiska jest oznaczana wymiennie przez N i M , zaś ρ_0 oznacza zarówno stan układu, jak i stan podukładu środowiska.

Wreszcie Γ nie jest znormalizowana: gdy wszystkie $|\gamma_{ij}^{(k)}| = 1$, otrzymuje się $\Gamma = \sum_{i \neq j} |\sigma_{ij}|$, niekoniecznie 1. Zdanie, że $\Gamma = 1$ zawsze oznacza brak dekoherencji, nie jest więc ogólnie prawdziwe. Należy też odróżnić wpływ liczby obserwowanych podukładów na ten współczynnik od dostępności redundantnej informacji w środowisku.

9. Na s. 60 zapis „computationalor” powinien brzmieć „computational or”.
10. Na s. 65–66 w centralnych wzorach rozdziału 4 występuje kumulacja błędów algebraicznych:

- zgodna z (4.16) postać (4.12) dla dwóch warstw to

$$P_{\text{guess}}^{N_i=2} = \frac{1}{2} + \frac{1}{2} \frac{q^3}{(p^2 + q^2)^{3/2}};$$

wersja wydrukowana może dawać wartość większą od jedności, na przykład $\epsilon = 0, 2$, $\alpha = 0$.

- w (4.14) oba składniki powinny mieć znak minus,

$$r = -(1 - P_{\text{guess}}) \log_2(1 - P_{\text{guess}}) - P_{\text{guess}} \log_2 P_{\text{guess}};$$

- w (4.15) argument pierwszego logarytmu powinien wynosić $p^2/(p^2 + q^2)$, nie $q^2/(p^2 + q^2)$.

Problem nie ogranicza się jednak do usterek drukarskich. Twierdzenie Holevo–Helstroma daje średnie prawdopodobieństwo poprawnej decyzji, lecz nie implikuje założonego w rozprawie symetrycznego kanału klasycznego. Dla $\eta = q/\sqrt{p^2 + q^2}$ otrzymuje się

$$P(e = 0|a = 0) = \frac{1 + \eta}{2}, \quad P(e = 1|a = 1) = \frac{1 - \eta + 2\eta^{2n-1}}{2}.$$

Wielkości te są równe tylko dla $n = 1$. Dla $n > 1$ entropia warunkowa $H(A|E)$ nie jest zatem wyznaczona przez samo średnie P_{guess} , toteż nawet po poprawieniu znaków wzór (4.17) nie daje ogólnie dokładnego oszacowania klucza. Przykładowo dla $\epsilon = 0,2$, $\alpha = 0$ i $n = 2$ entropia binarna $h_2(P_{\text{guess}})$ wynosi około 0,25795, podczas gdy bezpośrednio obliczone $H(A|E)$ wynosi około 0,24498. Co gorsza, w podanym przykładzie daje wartość większą od rzeczywistej, a więc przeszacowuje ilość bezpiecznego klucza. Nie może być bez dalszego dowodu traktowany jako bezpieczna dolna granica.

W tym samym fragmencie warstwa dostępna przeciwnikowi jest oznaczana przez $\mathcal{E}_{N_l}$, a następnie przez $\mathcal{E}_{N_l-1}$. Wzór na P_{guess} z Hipotezy 1 można ponadto wykazać krótką indukcją: różnica stanów zredukowanych ostatniej warstwy ma wartości własne $\pm|\eta|^{2n-1}$, skąd

$$P_{\text{guess}}^{(n)} = \frac{1}{2} + \frac{1}{2}|\eta|^{2n-1}.$$

Proszę Doktoranta o przedstawienie dowodu i o ponowne wyprowadzenie informacji wzajemnej oraz ilości klucza bez założenia symetrii kanału.

11. Na s. 68 Autor stwierdza, że dla zaakceptowanych bitów $\Gamma = 0$, ponieważ stan jest od początku stanem wskaźnikowym i „does not undergo decoherence”. Nie pasuje to do interpretacji ze s. 58, gdzie $\Gamma = 0$ oznacza pełną dekoherencję.
12. Na s. 72 i 75 występują odpowiednio „viewed as as” oraz „is given by $|B|_p$ is given by”.
13. Na s. 77–79 funkcja celu problemu optymalizacyjnego (5.13) ma postać, w której indeks sumowania nie występuje w składniku, a dodatkowy znak minus odwracałby kierunek optymalizacji, jeżeli $H(P)$ oznacza entropię. Czy zapis powinien brzmieć

$$\min_{P \in C} H(P) = \min_{P \in C} \left[- \sum_i P_i \log_2 P_i \right], \quad C = \left\{ P : l_i \leq P_i \leq u_i, \sum_i P_i = 1 \right\},$$

zgodnie z opisem na rysunku 5.1? Należy również podać, jaka funkcja została faktycznie zaimplementowana.

14. Na s. 80 warstwa graficzna wykresów, w szczególności rysunku 5.2, nie jest w pełni spójna z typografią rozprawy. Na rysunku 5.2 opisy osi, podziałki i legenda używają kroju bezszeryfowego wyraźnie odmiennego od szeryfowego kroju tekstu głównego. Różne są także stopnie pisma i sposób składu symboli matematycznych. Na rysunku 5.2 legenda zajmuje dużą część pola danych, podziałki osi odciętych są stłoczone, oznaczenia „(a)–(c)” nie podają bezpośrednio wartości ε , a ogólny opis osi rzędnych „Entropy” nie informuje, że przedstawiono liczbę bitów na zdarzenie. Zapis $k \approx 30k$ jest ponadto dwuznaczny, ponieważ k oznacza zarazem liczbę zdarzeń i skrót „tysiąc”. Zalecam użycie jednego kroju zgodnego z tekstem rozprawy, spójnych rozmiarów napisów i składu matematyki, zapisu 30 000 zamiast $30k$, precyzyjnego opisu osi, czytelniejszego rozmieszczenia legend,

zachowania napisów jako tekstu z osadzonym fontem oraz sprawdzenia wykresów w druku i w skali szarości.

15. Na s. 95 opis wzoru (5.30) odwołuje się do obserwabli $M^{0,j}$ i $M^{1,k}$, które nie występują w wyświetlonym wzorze. Pojawiają się w nim projektory $\Pi_n^{0,j}$ i $\Pi_n^{1,k}$. Należy ujednolicić wzór i jego opis.
16. Na s. 100–103 podpisy rysunków 5.15–5.17 mówią o „two measures of randomness”, chociaż każdy z tych rysunków przedstawia jedną miarę. W tabeli 5.3 wartości 1,003841 i 1,003749 opisano jako „exactly 1”. Bez podania tolerancji numerycznej nie uzasadnia to ścisłego wniosku o jednoznaczności ani samotestowaniu.
17. Na s. 108–114 wyniki rozdziału 6 przedstawiono jako dolne granice dyskor-du. Tymczasem dla

$$D_{\min}(b) = \min_{\rho, M: B(\rho, M)=b} D(\rho)$$

każdy znaleziony punkt spełnia $D(\hat{\rho}) \geq D_{\min}(b)$. Wynik heurystycznej optymalizacji bez certyfikatu globalności jest więc górnym oszacowaniem nieznanego minimum, a nie dolną granicą dyskor-du obowiązującą wszystkie zgodne stany. Autor uczciwie opisuje algorytm *basin-hopping*, około 50 prób na wyrażenie i lokalne minima dla CHSH, I_1 oraz łańcuchowych nierówności Braunsteina–Cavesa z trzema i pięcioma ustawieniami (BC_3 i BC_5). Zastrzeżenie nie występuje więc wyłącznie przy BC_5 . Nie zmienia to kierunku nierówności.

Ogólnie wyniki na tych stronach są przedstawione momentami chaotycznie co powoduje trudność w zrozumieniu jaka faktycznie funkcja była optymalizowana.

18. Na s. 115 zapis „In Section 4” powinien brzmieć „In Chapter 4”. Na s. 116 omówienie eksperymentalnej wykonalności kwantowego darwinizmu i przenoszenia informacji do środowiska jest następnie powtórzone niemal tymi samymi słowami.

Usterki redakcyjne nie przesądzają o wartości wyników, lecz błędny kierunek niektórych oszacowań, brak certyfikatu globalności i założenie symetrycznego kanału w rozdziale 4 są problemami merytorycznymi, a nie wyłącznie typograficznymi. Przed archiwizacją lub publikacją rozprawy zalecam zatem pełną korektę językową i typograficzną oraz ponowną weryfikację wzorów (3.1), (4.12)–(4.17), (5.13), (5.27), (6.6) i wzorów dodatków.

Ocena końcowa i wnioski

Rozprawa doktorska mgr inż. Roberta Okuły pt. „*Quantifying Quantum Information: Relationships between measures in Quantum Cryptography*” dotyczy ważnego poznawczo i aplikacyjnie problemu certyfikacji bezpieczeństwa i losowości w kryptografii kwantowej oraz zawiera oryginalne wyniki naukowe. Znaczna część rezultatów została poddana recenzji czasopismowej, co stanowi dodatkowe potwierdzenie ich wartości.

Przeprowadzone analizy pokazują, że mgr inż. Robert Okuła posiada rozległą wiedzę teoretyczną z zakresu informacji kwantowej oraz bardzo dobrze opanowany warsztat numeryczny obejmujący programowanie półokreślone, hierarchię NPA i nieliniową optymalizację heurystyczną. Podniesione uwagi wymagają odpowiedzi, a w kilku przypadkach korekty interpretacji wyników, nie niwelują jednak zakresu wykonanej pracy, jej oryginalności ani wartości poznawczej.

Pomimo uwag podniesionych w niniejszej recenzji uważam, że przedstawiona rozprawa spełnia wymogi ustawowe stawiane rozprawom doktorskim w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie informatyka techniczna i telekomunikacja. Wnoszę o przyjęcie rozprawy oraz o dopuszczenie mgr inż. Roberta Okuły do dalszych etapów postępowania doktorskiego.

dr hab. inż. Łukasz Paweła



Elektrycznie podpisany przez:

Łukasz Paweła

Data:
2026-7-24 11:51:29