dr hab. Zbigniew Puchała
Instytut Informatyki
Teoretycznej i Stosowanej PAN
ul. Bałtycka 5, 44-100 Gliwice

Gliwice, 25 maj 2023 r.

# Recenzja rozprawy doktorskiej mgra Marka Winczewskiego „Fundamental Limitations within the Selected Cryptographic Scenarios and Supra-Quantum Theories"

## Uwagi wstępne

Forma recenzowanej rozprawy obejmuje 326 stron, praca jest napisana w języku angielskim i składa się z wprowadzenia, rozdziału podsumowującego wyniki, perspektyw, bibliografii oraz pięciu publikacji. Tytuł pracy oddaje jej zawartość, a przyjęty układ pracy jest właściwy. Praca zawiera zbiór artykułów naukowych, których doktorant jest współautorem:

[A] Omer Sakarya, Marek Winczewski, Adam Rutkowski, Karol Horodecki. *Hybrid quantum network design against unauthorized secret-key generation, and its memory cost.* Phys. Rev. Research 2, 043022 (2020).

[B] Siddhartha Das, Stefan Bäuml, Marek Winczewski, Karol Horodecki. Universal *Limitations on Quantum Key Distribution over a Network.* Phys. Rev. X 11, 041016 (2021).

[C] Karol Horodecki, Marek Winczewski, Siddhartha Das. *Fundamental limitations on device-independent quantum conference key agreement.* Phys. Rev. A 105, 022604 (2022). With erratum in Phys. Rev. A 107, 029902 (2023).

[D] Marek Winczewski, Tamoghna Das, Karol Horodecki. *Limitations on device independent key secure against nonsignaling adversary via the squashed nonlocality.* Phys. Rev. A 106, 052612 (2022).

[E] Marek Winczewski, Tamoghna Das, John H. Selby, Karol Horodecki, Paweł Horodecki, Łukasz Pankowski, Marco Piani, Ravishankar Ramanathan. *Complete extension: the non-signaling analog of quantum purification.* Preprint arXiv:1810.02222. Published online 2018. Accepted for publication in Quantum 27.01.2023.

Do rozprawy dołączono oświadczenia współautorów wyżej wymienionych prac, z których można jednoznacznie wywnioskować, iż doktorant miał kluczowy wpływ na uzyskane w nich wyniki.

# Przedmiot rozprawy

Zbiór artykułów, będący częścią rozprawy doktorskiej, skupia się na określeniu górnych ograniczeń dotyczących ilości osiągalnego bezpiecznego klucza kryptograficznego w różnych scenariuszach kryptograficznych, zarówno kwantowych, jak i supra-kwantowych. Autorzy prac składających się na dysteracje, badają różne paradygmaty bezpieczeństwa, zarówno dwuosobowe, jak i wieloosobowe, w reżimach jednorazowych oraz asymptotycznych. Skoncentrowano się na scenariuszach uzgadniania klucza sekretnego, klucza konferencyjnego zależnego i niezależnego od urządzenia, a także na uzgadnianiu klucza sekretnego w obecności adwersarza ograniczonego jedynie brakiem sygnalizacji. W ramach badań autorzy odkryli nowy typ ataku przekierowującego na kwantowy Internet i przedstawili środek zaradczy oraz jego skuteczność. Ponadto, wyprowadzono ograniczenia górne dla wydajności układów kwantowych i repeaterów klucza kwantowego, a także ograniczenie dolne dla pojemności uzgadniania sekretnego klucza w sieci kwantowej, szczególnie w przypadku sieci złożonej z dwukierunkowych kanałów kwantowych. Opisano również nową miarę nielokalności, zwana ściśniętą nielokalnością (*squashed nonlocality*), oraz zbadano analogie między niesygnalizującymi i kwantowymi scenariuszami uzgadniania klucza kryptograficznego. Przyglądając się szerszej perspektywie, autorzy wskazują, że ich wyniki mają znaczenie nie tylko techniczne, ale również dotykają fundamentalnych kwestii związanych z teorią kwantową, umożliwiając dogłębne badanie tego tematu zarówno od wewnątrz, jak i od zewnątrz teorii kwantowej.

Głównym rezultatem artykułu [A] jest propozycja środka zaradczego przeciwko potencjalnemu zagrożeniu w kwantowo zabezpieczonym Internecie, gdy prywatne dane są udostępniane przez serwery wzajemnie anonimowym zarejestrowanym użytkownikom. Autorzy sugerują, że zastąpienie kanałów komunikacyjnych stanami maksymalnie splątanymi, choć jest obiecującym pomysłem na bezpieczną komunikację na dużych odległościach, jest niepotrzebne i może otworzyć luki w zabezpieczeniach dla określonej klasy serwerów. Analiza pokazuje, że aby uniknąć możliwości zamiany splątania, należy przechowywać co najmniej dwa razy więcej

pamięci w porównaniu ze standardowymi projektami sieci opartymi na repeaterach kwantowych.

Praca [B] dotyczy scenariuszy dystrybucji tajnych kluczy w scenariuszach dwu- i wieloosobowych za pośrednictwem sieci kwantowej. Główny wynik techniczny składa się z ograniczenia metakonwersji na przepustowość jednokrotnego uzgadniania klucza konferencyjnego multipleksowego kanału kwantowego. Z wyżej wymienionego wyniku autorzy uzyskują szereg słabych, jak również silnych odwrotnych ograniczeń użytecznych dla wielu zastosowań multipleksowego kanału kwantowego. Uzyskane wyniki działają w reżimie nieasymptotycznym, czyli skończonej liczby użyć kanału, a więc potencjalnie mają szerokie znaczenie praktyczne.

Głównym rezultatem artykułu [C] jest wyznaczenie kilku ogólnych górnych ograniczeń na szybkość generowania klucza kryptograficznego, który jest bezpieczny przeciwko kwantowemu adwersariuszowi w scenariuszu *device independent* dla uzgadniania klucza konferencyjnego. Ograniczenia te obejmują różne podejścia, w tym ograniczenia oparte na zredukowanych miarach splątania i wieloczęściowych monotonach tajności.

W pracy nukowej [D] głównym rezultatem jest systematyczna analiza górnych granic dla kluczy *device independent*, które są bezpieczne przed ogólnym przeciwnikiem działającym w ramach teorii niesygnalizującej. Jednym z rezultatów w tej pracy jest systematyczna eksploracja górnych granic szybkości generowania tajnego klucza w scenariuszu niezależnym od urządzenia sygnalizacyjnego. Autorzy ustanawiają bezpośredni związek między scenariuszem Secret Key Agreement (SKA) a NSDI, konstruując ograniczenia w scenariuszu NSDI w oparciu o monotony tajności ze scenariusza SKA. Wprowadzają pojęcie "ściśniętej nielokalności" jako obliczalną granicę, a także identyfikują inne miary nielokalności. Badania te otwierają nowe możliwości dla ściślejszych górnych granic i dalszego badania relacji między scenariuszami SKA i NSDI. Kolejnym rezultatem jest metoda konstruowania nowych miar nielokalności oraz udowodnienie kilku ważnych własności takich jak monotoniczność, wypukłość czy addytywność.

Głównym rezultatem pracy [E] jest zaproponowanie bardziej ogólnie stosowalnego postulatu zwanego postulatem całkowitego rozszerzenia jako zamiennika postulatu puryfikacji w wyprowadzaniu mechaniki kwantowej z zasad teorii informacji. Nowy postulat zapewnia istnienie rozszerzenia systemu fizycznego, które może wygenerować każde inne rozszerzenie, otwierając nowe ścieżki badań nad ogólnymi teoriami, które spełniają CEP. Badane są implikacje CEP i pokazane, że prowadzi to do niemożności zobowiązania bitowego.

# Ocena końcowa i wnioski

Zbiór artykułów składających się na rozprawę doktorską mgra Marka Winczewskiego „Fundamental Limitations within the Selected Cryptographic Scenarios and Supra-Quantum Theories" dotyczy ważnego zarówno poznawczo, jak i aplikacyjnie problemu oraz stanowi wartościowe osiągnięcie naukowe Autora. Praca wnosi istotne wyniki w dziedzinie bezpieczeństwa kryptograficznego w różnych scenariuszach, zarówno kwantowych, jak i supra-kwantowych. Autor skupiają się na analizie paradygmatów bezpieczeństwa, w tym uzgadniania klucza sekretnego i konferencyjnego, zarówno zależnego, jak i niezależnego od urządzenia, oraz uwzględnia obecność adwersarza niesygnalizującego.

Wyniki przedstawione w dysertacji mają znaczenie zarówno techniczne, jak i fundamentalne, i otwierają nowe możliwości badawcze w dziedzinie teorii kwantowej i teorii informacji. Prace dostarczają istotnych wniosków dotyczących bezpieczeństwa kryptograficznego w kontekście różnych scenariuszy, a także zapewniają nowe spojrzenie na zagadnienia związane z teorią kwantową.

Doktorant do rozwiązania postawionych problemów użył właściwych metod. Oryginalnymi osiągnięciami badawczymi Autora są:

- Odkrycie nowego typu ataku przekierowującego na kwantowy Internet i przedstawienie skutecznego środka zaradczego.
- Wprowadzenie nowej miary nielokalności, zwanej "ściśniętą nielokalnością" (squashed nonlocality), oraz badanie jej właściwości i związków z innymi miarami nielokalności.
- Ustanowienie bezpośredniego związku między scenariuszem Secret Key Agreement a scenariuszem Non-Signaling Device-Independent w celu konstrukcji ograniczeń bezpieczeństwa klucza kryptograficznego.
- Wyznaczenie ograniczeń górnych dla wydajności układów kwantowych, takich jak powtarzacze klucza kwantowego i repeaterów, w celu poprawy efektywności komunikacji kwantowej na dużych odległościach.
- Zaproponowanie postulatu całkowitego rozszerzenia jako ogólniejszej alternatywy dla postulatu puryfikacji w wyprowadzaniu mechaniki kwantowej z zasad teorii informacji.

Jest to wkład mgra Marka Winczewskiego w rozwój dyscypliny naukowej – nauki fizyczne. Rozległość przeprowadzonej analizy uzasadniają stwierdzenie, że Autor posiada wiedzę teoretyczną, zdolności koncepcyjne oraz umiejętności do rozwiązywania naukowych problemów badawczych.

**Uważam że przedstawiona rozprawa spełnia wymogi ustawowe stawiane pracom doktorskim w dziedzinie nauk ścisłych i przyrodniczych w dyscyplinie nauki fizyczne i wnoszę o przyjęcie jej przez Radę Dyscypliny Nauki fizyczne Uniwersytetu Gdańskiego w Gdańsku, oraz o dopuszczenie do publicznej obrony.**

dr hab. Zbigniew Puchała