Gdańsk, 28 czerwca 2018 r.

mgr Edgar Alexis Aguilar Lozano
Instytut Fizyki Teoretycznej i Astrofizyki
Uniwersytet Gdański

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Device Independent and Semi Device Independent Protocols for Quantum Information Processing

Niniejsza rozprawa doktorska poświęcona jest badaniom sprzętowo-niezależnych (ang. Device Independent, DI) i quasi-sprzętowo-niezależnych (ang. Semi Device Independent, SDI) protokołów i ich zastosowaniom w przetwarzaniu kwantowej informacji. Kluczową cechą protokołów DI jest to, że zaangażowane strony nie muszą przyjmować żadnych założeń dotyczących wewnętrznych mechanizmów ich urządzeń. W szczególności nie muszą ufać źródłu, które dostarcza układy poddawane przez strony pomiarom, jak i samym aparaturom pomiarowym. Scenariusz ten jest idealny w zastosowaniach kryptograficznych, w których dwie strony chcące ustanowić tajny klucz nie ufają dostawcy swoich urządzeń lub mają powody, by sądzić, że istnieje podsłuch w kanale kwantowym. Podobnie scharakteryzować można protokoły SDI: strony nie przyjmują żadnych założeń opisujących urządzenia, z wyjątkiem ograniczania na wymiar wykorzystywanych systemów fizycznych (lub równoważnie, ograniczania na pojemność kanału kwantowego). Podejście SDI jest mniej rygorystyczne (a więc mniej bezpieczne), tym niemniej niezwykle cenne przy testowaniu doświadczalnie osiągalnych własności w eksperymentach przygotowania i pomiaru. Ze względu na bardzo ograniczone założenia, protokoły SDI umożliwiają uzyskanie bezprecedensowego poziomu bezpieczeństwa, co wyjaśnia dużą liczbę przeprowadzanych badań eksperymentalnych i teoretycznych. Rozprawa ta jest w istocie teoretyczna, choć część badań została przeprowadzona z myślą o laboratoryjnej weryfikacji rezultatów (która została uwieńczona sukcesem).

W szczególności wykorzystano zbiór protokołów DI służących powielaniu losowości, wraz z ugruntowanymi protokołami DI używanymi w dystrybucji klucza kwantowego, w celu zweryfikowania podstawowych założeń potrzebnych do zagwarantowania prywatności. Jako że generatory liczb losowych nie spełniają warunku DI, konieczność posiadania dostępu do tych urządzeń została zakwestionowana. Zaproponowano protokół ustanawiający tajny klucz między dwiema stronami w sposób zgodny z ideą DI.

Ponadto, przeanalizowano protokół typu SDI zwany kodem losowego dostępu (ang. Random Access Code, RAC) i znaleziono jego kilka zastosowań. Jedno z nich polega na dostarczaniu testów statystycznych do uwiarygodniania wysokiej jakości stanów kwantowych wytworzanych w laboratorium. Pomysł ten został wdrożony w eksperymencie fotonicznym, w którym potwierdzono dysponowanie 1024-wymiarowym stanem fotonicznym. Drugie zastosowanie to konstrukcja jawnego algorytmu do wykluczania istnienia danej liczby wzajemnie zrównoważonych baz (ang. Mutually Unbiased Bases) w przestrzeni o określonym wymiarze.