Streszczenie

Celem pracy doktorskiej jest opis wybranych zagadnień przetwarzania informacji kwantowej pod kątem badania ich fizycznych ograniczeń. W każdym z przypadków podejmujemy próbę wyeliminowania ich negatywnych konsekwencji. Jako przykłady ograniczeń rozważamy: relacje pomiędzy zasobami i ich ograniczone ilości, fizyczną naturę procesu generacji i detekcji fotonów, czy też ograniczenia na liczbę pomiarów, które możemy przeprowadzić.

Pierwszy rozdział opisuje rys historyczny koncentrując się głównie na tematyce, która rozwinięta zostanie w następnych rozdziałach.

Następny rozdział poświęcony jest na przypomnienie podstawowych definicji i pojęć, na których bazuje praca. Rozdział ten podzielony jest na dwie części. Pierwsza z nich poświęcona jest klasycznej teorii informacji, podczas gdy druga, koncentruje się na podstawowych własnościach zasobów kwantowych. Zakres materiału w tym rozdziale ograniczony jest do potrzeb późniejszych analiz.

Kolejne rozdziały stanowiące zasadniczą część rozprawy, w głównej mierze, opierają się na wynikach opublikowanych w następujących pracach:

[A] *Security of QKD protocols against detector blinding attacks*
arXiv:1504.00939 [quant-ph] (2015)

[B] *Activation of entanglement in teleportation*
J. Phys. A: Math. Theor. 46 435301 (2013)

[C] *Optimal pumping strength for BBM92 key distribution protocol*
Int. J. Quantum Inform. 14, 1650049 (2016)

[D] *Entanglement witnesses with variable number of local measurements*
Phys. Rev. A 88, 022304 (2013),

których jestem współautorem.

W rozdziale trzecim podjęta zostaje tematyka kwantowej dystrybucji klucza kryptograficznego, gdzie poszukiwane jest kryterium uwzględniające wydajność procesu detekcji. Rozdział rozpoczyna się od wstępu teoretycznego i opisu mechanizmu fizycznego jaki umożliwia detekcję fotonów. Opis ten jest realizowany na przykładzie detektora APD (z ang. *avalanche photo-diode*). Następnie budowany jest teoretyczny model, w którym kontrolę nad urządzeniami przejmuje

osoba trzecia. Badane są dwa rodzaje ataków: PP (przechwyć/prześlij) oraz OP (opóźniony pomiar).

W rozdziale czwartym analizowana jest natura fizycznego ograniczenia na relację pomiędzy komunikacją klasyczną a splątaniem kwantowym. Badanym zjawiskiem jest teleportacja stanów kwantowych o wymiarze przestrzeni Hilberta podukładów równym d (tzw. kuditów). Na początku opisany jest schemat i notacja wykorzystywana w dalszej części oraz zostają przywołane przydatne własności i definicje algebraiczne. Następnie przeprowadzona jest analiza średniej wierności procesu teleportacji w zależności od rodzaju narzucanych na zjawisko ograniczeń. Po tej analizie wyznaczona zostaje graniczna ilość informacji klasycznej potrzebna do aktywowania zasobów kwantowych w funkcji wymiaru d. Na końcu porównywana jest wierność zjawiska teleportacji z komunikacją klasyczną, przeprowadzaną przy użyciu kanałów o różnych charakterystykach.

W piątym rozdziale dotykamy problemu związanego z generowaniem stanów przydatnych w protokołach kryptograficznych wykorzystując zjawisko parametrycznego podziału częstości PDC (z ang. *parametric down-conversion*). Wiadomo, że przy dużej mocy lasera pompującego, kreacja wielu par fotonów staje się bardziej prawdopodobna i ma negatywny wpływ na wierność otrzymanego stanu. Pokazujemy metodę ominięcia tego negatywnego ograniczenia, która pozwala na stosunkowo dużą moc lasera pompującego, co przekłada się na większą wydajność (szybkość) w generowaniu klucza kryptograficznego.

Ostatni rozdział poświęcony jest metodzie konstruowania wydajnych kwadratowych kryteriów wykrywania splątania w stanach kwantowych. Są one idealne w sytuacjach ograniczonej liczby pomiarów, które możemy wykonać na stanie kwantowym. Metoda opatrzona jest wieloma przykładami ilustrującymi sposób działania nowego indykatora splątania.

Prace kończy podsumowanie, w którym zebrane są główne wyniki zawarte w rozprawie.