Streszczenie

Kodowanie czasowo-fazowe pojawiło się jako obiecujące narzędzie dla technologii informacji kwantowej. Modulowanie czasu i fazy światła kwantowego pozwala generować kubity oraz wielkowymiarowe stany kwantowe, które umożliwiają implementację technologii kwantowych o zwiększonej odporności na szum. Jedną z najbardziej pożądanych technologii komunikacji kwantowej jest kwantowa dystrybucja klucza (QKD). QKD wyłoniła się jako wiodące rozwiązanie, aby sprostać rosnącemu zapotrzebowaniu na bezpieczne systemy komunikacyjne w obliczu potencjalnych zagrożeń związanych z rozwojem komputerów kwantowych.

Obecne systemy QKD oparte na kubitach zostały szeroko zademonstrowane, szczególnie z wykorzystaniem czasowo-fazowego oraz polaryzacyjnego stopnia swobody. Kodowanie czasowo-fazowe jest szczególnie atrakcyjne ze względu na kompatybilność z istniejącą infrastrukturą telekomunikacyjną, odporność na dryf polaryzacji oraz możliwość wydajnej i szybkiej implementacji. W niniejszej pracy badam korzyści wynikające z rozszerzenia kodowania czasowo-fazowego w QKD na stany o wysokiej wymiarowości w celu dalszego zwiększenia tolerancji na szumy oraz poprawy efektywności generowania kluczy.

Głównym celem pracy jest budowa systemu QKD wykorzystującego kodowanie czasowo-fazowe. Opracowałem system umożliwiający transmisję i detekcję kwantowych symboli o wysokiej wymiarowości, pozwalający na kodowanie wielu bitów informacji w pojedynczym fotonie. Głównym osiągnięciem jest eksperymentalna demonstracja zalet wysokowymiarowego kodowania, poparta teoretyczną analizą porównującą wpływ niezrównoważonych prawdopodobieństw pomiaru między bazą generacji klucza i bazą kontrolną.

W pierwszej częsci pracy oceniłem potencjał fotonicznych układów scalonych (PIC) do generowania symboli, które mogłyby być wykorzystywane w komunikacji kwantowej. Zbadałem właściwości kompoentnów umieszczonych na chipie celem sprawdzenia poprawności wykonania oraz zbadania kluczowych parametrów. Wykorzystałem zintegrowane modulatory na chipie do generacji impulsów optycznych o pożądanych właściwościach czasowo widmowych. Zweryfikowałem wyniki za pomocą przybliżonego mapowania czasu na widmo zrealizowanego za pomocą ośrodka dyspersyjnego i techniki dyspersyjnego przekształcenia Fouriera i czasowo-skorelowanego zliczania pojedynczych fotonów. Uzyskane wyniki potwierdzają możliwość zastosowania generycznych platform PIC opartych na fosforku indu na poczet QKD.

Następnie zaproponowałem nową metodę detekcji wysokowymiarowych czasowych superpozycji kwantowych, opartą na efekcie Talbota w dziedzinie czasu — odpowiedniku dobrze znanego efektu samoobrazowania obiektów periodycznych związanego z dyfrakcją w strefie bliskiego pola. Dzięki precyzyjnemu dostrojeniu parametrów czasowych oraz własności dyspersyjnych osiągnąłem mapowanie częstotliwość-czas przy znacznie niższych wymaganiach dotyczących dyspersji w porównaniu do standardowych metod. Dodatkowo przeanalizowałem wpływ strategii post-selekcji oraz szumu czasowego na poprawność rozróżniania kwantowych superpozycji.

Najważniejszym osiągnięciem niniejszej pracy jest eksperymentalna demonstracja QKD z wykorzystaniem dwuwymiarowych i czterowymiarowych superpozycji kwantowych, wykrywanych za pomocą nowo wprowadzonej metody opartej na efekcie Talbota w dziedzinie czasu. Przeprowadziłem kontrolowane testy laboratoryjne oraz rozszerzyłem walidację systemu o pomiary z wykorzystaniem infrastruktury światłowodowej Uniwersytetu Warszawskiego. W trakcie badań wykazałem, że kodowanie wysokowymiarowe zwiększa odporność na szumy oraz podnosi entropię informacji przypadającą na pojedyncze zdarzenie detekcji. Wyniki eksperymentalne zostały przeanalizowane w oparciu o dwa różne modele bezpieczeństwa — zarówno uwzględniające, jak i pomijające niezrównoważoną wydajność detekcji — ujawniając istotne różnice w osiągalnych wartościach informacyjnych generowanych kluczy. Uzyskane wyniki otwierają drogę do budowy bezpiecznych systemów QKD opartych zarówno na stanach wysokowymiarowych, jak i na kubitach.

Dalsze analizy teoretyczne mogą poprawić dokładność modelowania systemów QKD, w szczególności w scenariuszach ograniczonej skończonej kluczy kryptograficznych.