Zestawy egzaminacyjne z przedmiotu Podstawy Informatyki Kwantowej

dr hab. K. Horodecki
Instytut Informatyki, Uniwersytet Gdański

Zestawy egzaminacyjne (tylko to obowiązuje na egzamin). Losowany jest 1 zestaw z poniższych. Każdy zestaw składa się z 3 zagadnień a,b,c. Egzamin jest pisemny. Poprawny opis 1 zagadnienia daje 10 pkt. Egzamin jest zaliczony jeśli uzyska się w sumie min. 15 pkt.

1. (a) Podaj 2 z aksjomatów mechaniki kwantowej: (1) co to jest stan kwantowy oraz (2) aksjomat pomiaru.
   (b) Opisz protokół BB84 i główna zasadę jego bezpieczeństwa.
   (c) Podaj definicje podukładów dwuukładowego stanu kwantowego z przykładem obliczenia na jakimś stanie.

2. (a) Opisz protokół destylacji singletów ze stanów mieszanych 2 układowych Bennetta et al. (nie trzeba przywoływać całej tabelki działania dwóch CNOTów, wystarczy 1-2 przykłady)
   (b) Definicja stanu separowalnego (i splatanego). kryterium częściowej transpozycji dla 2x2 i 2x3 splatania stanu. Co to są stany o związanym splataniu (w tym co to są operacje Lokalne i klas. komunikacja LOKK)
   (c) Opisz protokół gęstego kodowania.

3. (a) Podaj 2 aksojmaty mechaniki kwantowej - układu złożonego i ewolucji układu niemierzonego
   (b) Opisz przykładowy atak na protokół BB84.
   (c) Udowodnij twierdzenia o nieklonowaniu, opisz na tej podstawie pomysł Wiesnera o kwantowych pieniądzach.

4. (a) Opisz protokół B92
   (b) Podaj dowód twierdzenia, że pomiar 2 stanów które nie są ortogonalne albo je narusza, albo nie daje żadnej informacji.
   (c) Podaj definicję świadka splątania oraz przykład wraz z wyjaśnieniem dlaczego jest świadkiem.

5. (a) Podaj definicje wartości średniej obserwabli kwantowej i przykład obliczenia
   (b) Opisz jakie są zawierania pomiędzy zbiorami układów lokalnych, kwantowych i niesygnalizujacych oraz które z nich łamią nierówność CHSH. Opisz nierówność CHSH i szkic jej dowodu.
   (c) Opisz protokół one-time-pad oraz wyjaśnij jak można generować klucz kwantowy mając do dyspozycji źródło stanów singletowych. Uzasadnij, że tak otrzymany klucz jest bezpieczny podając definicje dopełniania stanu dwuukładowego do stanu czystego trójukładowego.

6. (a) Opisz działanie i idee zastosowanie alg. Grovera
   (b) Opisz protokół teleportacji.
   (c) Opisz protokół E91. o jakie 2 założenia opiera się jego bezpieczeństwo ? (w tym kontekście: co to jest device independent quantum cryptography)

7. (a) Definicja entropii Shannona i von Neummanna, oraz przykład występowania entropii von Neumanna i Shannona w kontekście ważnych protokołów (np. state merging) co to jest wzajemna informacja. Diagram Venna dla entropii i na jego podstawie znane zależności miedzy wielkościami entropowymi
   (b) Podać bramki kwantowe poznane na wykładzie i ich działanie na bazie standardowej (jednego lub 2 kubitów w zależności od liczby wejść bramki). Czym różnią się od klasycznych ? Opisać algorytm Deutscha.

(c) Definicja stanów bezpiecznych, problem rozróżniania stanów za pomocą operacji LOKK oraz globalnych, pokazanie, że niektóre stany bezpieczne nie nadają się do ”key repeaters” - ”powtarzania klucza”.

8. (a) Opisz kwantowa transformatę Fouriera, oraz opisz jak działa ona i jaka ma złożoność czasowa (liczbę kwantowych bramek z których się składa)
(b) Jakie są problemy z kwantowa dystrybucja klucza i jak można się ich pozbyć za pomocą splatania (entanglement swapping oraz idea kwantowych powtarzaczy).
(c) Opisz idee algorytmu Shora rozkładu liczby na czynniki pierwsze i jego zastosowanie (bez definiowania kwantowej transformaty Fouriera) w opisie podaj obwód pod-procedury która rozwiązuje ten algorytm