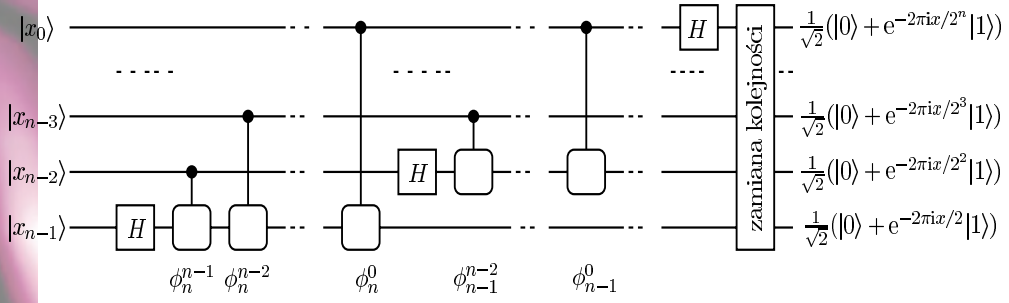


Łamanie klucza publicznego

Rozkład na czynniki pierwsze

MECHANIKA KWANTOWA 3/2

Informację koduje się i zapisuje w stanie pewnego układu fizycznego, takiego jak strony książki czy powierzchnia twardego dysku. Ale każdy układ fizyczny jest układem kwantowym, zatem informacja musi być zakodowana w stanie kwantowym. Przetwarzanie informacji, zwane także obliczaniem, jest wykonywane przez realnie istniejące urządzenia, również będące układami kwantowymi. Czyli podstaw teorii informacji jak i samej informatyki należy szukać w fizyce kwantowej. Wykład poświęcony będzie niektórym zagadnieniom dotyczących tego problemu oraz przedstawieniu wybranych paradoksów. W szczególności planuję poruszyć następujące tematy:

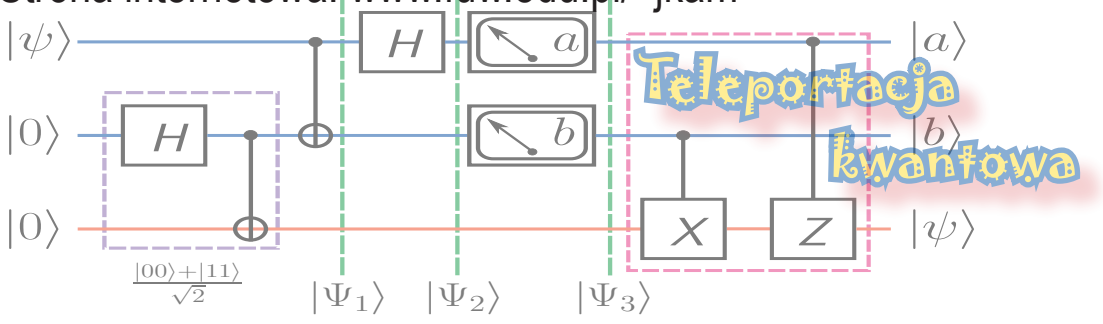
- Podstawowy aparat matematyczny mechaniki kwantowej.
- Postulaty mechaniki kwantowej i jej niektóre paradoksy, np. efekt Casimira, kwantowy efekt Zeno, kwantowy saper ...
- Całki funkcjonalne (po drogach) i zwiazek z teorią klasyczną.
- Bramki i obwody klasyczne i kwantowe. Teleportacja i destylacja stanów. Miary informacji, splątania, wierności ...
- Szyfrowanie kwantowe i najważniejsze algorytmy kwantowe:
  - Algorytm Grovera (przeszukiwania) i łamanie kluczy symetrycznych.
  - Algorytm Shora (kwantowa transformata Fouriera) i łamanie kluczy publicznych.
- Klonowanie stanów i gęste kodowanie informacji.

Celem tego wykładu jest jak najwcześniejsze zapoznanie studentów z najnowszymi osiągnięciami mechaniki kwantowej i jej związkami z teorią informacji i sterowaniem kwantowym, zwanym również inżynierią kwantową. Jest on adresowany do studentów drugiego i trzeciego roku. Wymagana jest elementarna znajomość Analizy i Algebry. Wszystkie nowe pojęcia zostaną zdefiniowane i przedyskutowane na wykładzie. **Nie wymagana jest** znajomość mechaniki kwantowej na poziomie *Mechanika Kwantowa I.*

Wszystkich zainteresowanych gorąco zapraszam, J. Kamiński

Czas: Wtorki, 15-18 Miejsce: SDT - 229 (Hoża)

Strona internetowa: www.fuw.edu.pl/~jkam



Strona intergetowa wykładu:
www.fuw.edu.pl/~jkam/Dydaktyka/MechanikaKwantowa/MechanikaKwantowa3_2_2008_2009
lub www.fuw.edu.pl/~jkam/

215274110271888970189601520131282542925777358884567598017049767677813314521885913\
567301105977349105960249790711158521430207931466520284014061994699492757040775 3=
4542789285848139407168619064973883165613714577846979325095998470925000415733535 9
*473880906038320161966338323037889519732689229210409579447413546488120284939093 67