



Kraków, maj 2006

## Krzysztof Maćkowiak "Kryptografia kwantowa"

### Agenda

Rozwój badań w dziedzinie kryptoanalizy oraz wzrost mocy obliczeniowej komputerów, powoduje, iż wiele algorytmów, które uważane były za niemożliwe do złamania w krótkim czasie i miały zapewnić bezpieczeństwo na wiele dziesięcioleci jak np. standard szyfrowania symetrycznego DES, zostało w ostatnich latach skompromitowanych. Podobnie ostatnie doniesienia związane ze złamaniem algorytmu RSA o długości klucza 576 bitów (100 maszyn w 3 miesiące), praca Adi Shamira i Erana Tromera, w której autorzy przedstawiają możliwość złamania algorytmu RSA z kluczem 512-bitowym w czasie krótszym niż 10 minut z wykorzystaniem dedykowanego sprzętu o wartości 10tys USD oraz z kluczem 1024-bitowym w czasie krótszym niż rok z nakładami finansowymi rzędu 10 milionów USD a także algorytm Shora, który jest efektywnym algorytm faktoryzacji z wykorzystaniem komputerów kwantowych, nie napawają optymizmem. W przypadku kryptografii wiele nadziei pokładanych jest w komputerach kwantowych i kryptografii kwantowej.

W referacie przedstawione zostały podstawy informatyki kwantowej oraz kryptografii kwantowej. Oprócz podstaw teoretycznych i najważniejszych algorytmów, zaprezentowane zostały informacje m.in. na temat budowy komputerów kwantowych, rekordów w przesyłaniu fotonów, komputerowej sieci kwantowej oraz transferu pieniędzy z wykorzystaniem kryptografii kwantowej.

### Plan referatu:

1. Wprowadzenie
2. Podstawowe pojęcia
3. Algorytm Grovera
4. Algorytm Shora
5. Algorytm Bennetta-Brassarda
6. Algorytm Bennetta
7. Praktyczne zastosowanie
  - 7.1 Komputery kwantowe
  - 7.2 Przesyłanie klucza w praktyce
  - 7.3 Transakcja finansowa z wykorzystaniem kryptografii kwantowej
  - 7.4 Sieć komputerowa oparta na kryptografii kwantowej
  - 7.5 Rozwiązania komercyjne dostępne na rynku
  - 7.6 Inne podejście do tematu
8. Podsumowanie
9. Literatura