Kryptografia kwantowa

Krzysztof Maćkowiak

CONFidence 2006

Plan referatu

- Wprowadzenie, podstawowe pojęcia
- Algorytm Grovera
- Algorytm Shora
- Algorytm Bennetta-Brassarda
- Algorytm Bennetta
- Praktyczne zastosowanie
  - Komputery kwantowe
  - Przesyłanie klucza w praktyce
  - Transakcje finansowe
  - Kwantowa sieć komputerowa
  - Rozwiązania komercyjne dostępne na rynku
  - Inne podejście do tematu

Wprowadzenie

Kot Erwina Schrödingera

Wprowadzenie

Początki teorii obliczeń kwantowych:

- 1982 – Richard Faynman – przy symulacji układu kwantowego składającego się z *R* cząsteczek na zwykłym komputerze, nie da się uniknąć wykładniczego wzrostu czasu obliczeń wraz ze wzrostem *R*.
- 1985 – David Deutsch – propozycja kwantowego modelu obliczeń oraz opis uniwersalnego komputera kwantowego.
- Bernstein i Vazirani opracowują model kwantowej uniwersalnej maszyny Turinga.
- 1994 – Peter Shor – kwantowe algorytmy rozkładu liczb na czynniki pierwsze oraz znajdowania logarytmów dyskretnych w czasie wielomianowym.

Wprowadzenie

Podstawowe pojęcia:

- **Qubit (bit kwantowy)** – dwuwymiarowa przestrzeń Hilberta, która posiada ustaloną bazę obliczeniową $B=\{|0>, |1>\}$.

  Stan pojedynczego bitu kwantowego stanowi wektor:

  $$c_0 |0> + c_1 |1>,$$

  gdzie:

  c_0 i c_1 nazywane są amplitudami stanów bazowych oraz zachodzi $|c_0|^2 + |c_1|^2 = 1$.

  Klasyczny bit przyjmuje dwie wartości {0,1} a dowolną informację możemy zapisać w postaci ciągu bitów. Różnica pomiędzy bitem a qubitem polega na tym, że qubit jest dowolną superpozycją stanów bazowych.

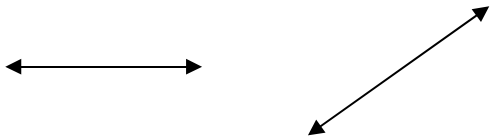
Wprowadzenie

Podstawowe pojęcia:

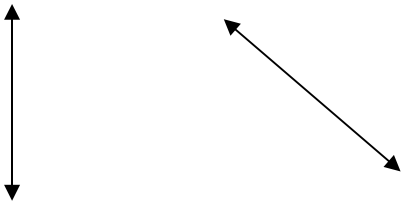
- **Problem pomiaru** – w świecie makroskopowym pomiar ma charakter pasywny, czyli nie zmienia stanu mierzonego układu. W świecie kwantowym pomiar jest aktywny, tzn. zmienia stan badanego układu.
- **Foton** – fala elektromagnetyczna, w której pole elektryczne i magnetyczne drgają prostopadle do siebie i do kierunku rozchodzenia się fali.
- **Polaryzacja** – kierunek drgania pola elektrycznego. Z wykorzystaniem laserów można emitować pojedyncze fotony i poddawać je również polaryzacji przez zastosowanie odpowiednich filtrów.

Wprowadzenie

Alfabet:



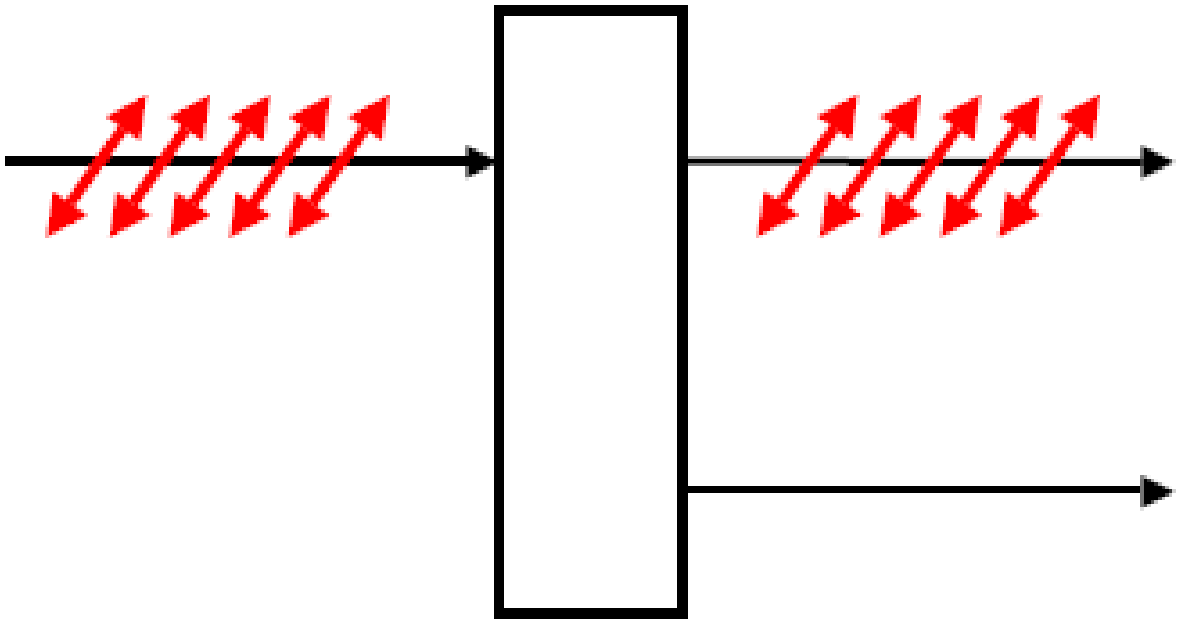
= 0



= 1

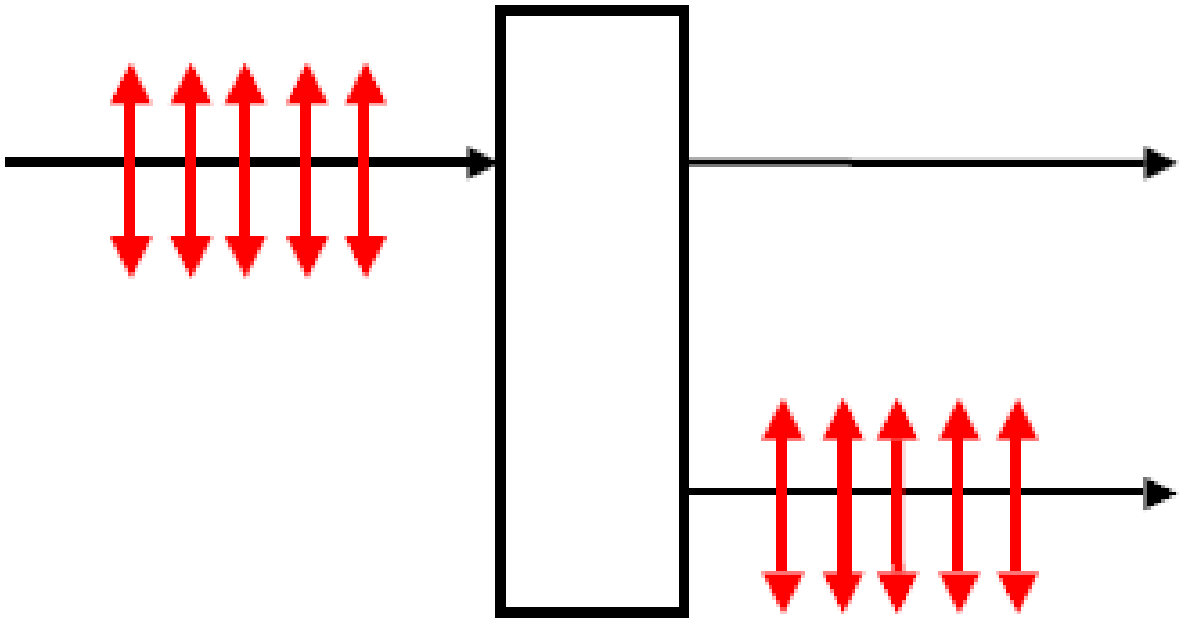
Wprowadzenie

Baza prosta – fotony spolaryzowane **poziomo**:



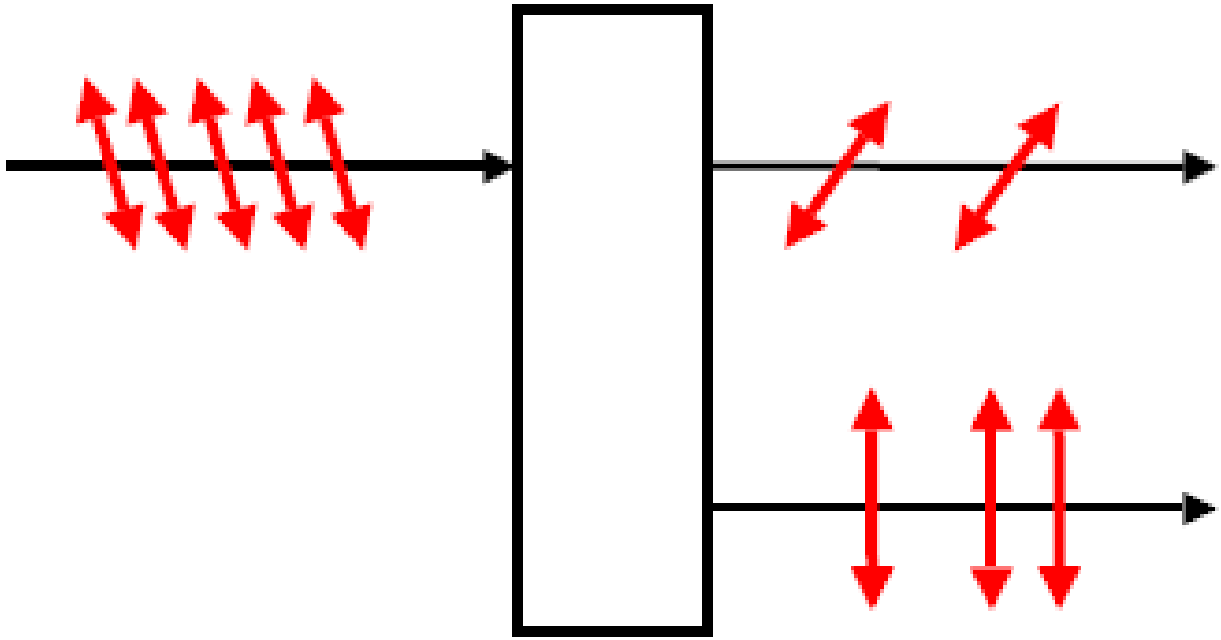
Wprowadzenie

Baza prosta – fotony spolaryzowane **pionowo**:



Wprowadzenie

Baza prosta – fotony spolaryzowane **ukośnie**:



Wprowadzenie

Bazę ukośną uzyskujemy obracając kryształ o kąt -45°.

Charakterystyka bazy ukośnej:

- Polaryzacja pozioma -> Polaryzacja ukośna -45° (135°) lub 45° (z prawdopodobieństwem równym 1/2)
- Polaryzacja pionowa -> Polaryzacja ukośna -45° (135°) lub 45° (z prawdopodobieństwem równym 1/2)
- Polaryzacja ukośna -45° (135°) -> Polaryzacja ukośna -45° (135°)
- Polaryzacja ukośna 45° -> Polaryzacja ukośna 45°

Wprowadzenie

Baza prosta zapewnia pewny pomiar fotonów spolaryzowanych pionowi i poziomo.

Baza ukośna zapewnia pewny pomiar fotonów spolaryzowanych ukośnie.

Z zasady nieoznaczoności Heisenberga wynika, że nie możemy połączyć pomiarów polaryzacji prostej z polaryzacją ukośną, w celu uzyskania pewnego pomiaru wszystkich fotonów.

Kryptoanaliza

Algorytm Grovera – algorytm poszukiwania danego elementu w nieposortowanym *N*–elementowym zbiorze.

Algortym Shora – algorytm faktoryzacji (rozkładu liczb na czynniki pierwsze).

Algorytm Grovera (1997)

Algorytm poszukiwania danego elementu w nieposortowanym N-elementowym zbiorze.

Liczba wymaganych operacji proporcjonalna do $\sqrt{N}$.

Złożoność tradycyjnych algorytmów wyszukiwania to średnio $N/2$ kroków.

Przyspieszenie kwadratowe.

Problem wyszukiwania sprowadza się do wyznaczenia na drodze przekształceń unitarnych odpowiedniego indeksu określającego dany element w zbiorze.

Przykład:

Zbiór $N=10^{16}$

Klasyczne komputery – tysiąc lat.

Komputery kwantowe – kilka minut.

Algorytm Shora (1994)

Kryptografia asymetryczna:

- problem logarytmu dyskretnego,
- problem faktoryzacji.

Najszybszy algorytm faktoryzacji wymaga czasu w przybliżeniu: $\exp [1.9(\ln N)^{1/3}(\ln\ln N)^{2/3}]$.

Faktoryzacja liczby 400-cyfrowej z zastosowaniem tego algorytmu zajęłaby około 10^{10} lat.

Złożoność algorytmu Shora - (lnN)3.

Rozłożenie na czynniki pierwsze liczby składającej się z 129 cyfr zajęłoby na komputerze kwantowym z zegarem 100 MHz kilka sekund, natomiast złamanie klucza składającego się z 400 cyfr niewiele ponad minutę.

Algorytm Shora (1994)

Liczba, którą chcemy poddać faktoryzacji – $N=15$.

Wybieramy liczbę losową $1<X<N-1$ względnie pierwszą z N (NWD(N,X)=1). Załóżmy $X=2$.

W rejestrze kwantowym złożonym z N qubitów można przechowywać 2^N liczb. Komputer kwantowy wykonuje operacje na całym rejestrze czyli na wszystkich 2^N liczbach jednocześnie.

Należy przygotować rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15:

$$|A\rangle=1/4(|0\rangle+|1\rangle+|2\rangle+\ldots+|13\rangle+|14\rangle+|15\rangle).$$

Co można zapisać jako:

A		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Algorytm Shora (1994)

Następnie wykonujemy operacje X^A mod N a wyniki umieszczamy w rejestrze B. Komputer kwantowy dzięki równoległości obliczeń wykonują tą operację w jednym kroku.

A		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

B		1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

Wartości w rejestrze B są wartościami okresowymi a okres w tym przypadku wynosi $r=4$. Jeżeli wartość okresu jest nieparzysta należy wybrać inną wartość X. Jeżeli r jest parzyste, tak jak w naszym przypadku obliczamy:

$P = X^{r/2} - 1$ lub $P = X^{r/2} + 1$ i sprawdzamy czy P jest dzielnikiem N.

Algorytm Shora (1994)

W naszym przypadku mamy:

$$r=4,$$

$$P=24/2-1=3$$

lub

$$P=24/2+1=5.$$

Sprawdźmy:

$$15/3 = 5$$

$$15/5 = 3$$

Kryptografia

Przez kryptografię kwantową rozumiemy kwantową dystrybucję klucza kryptograficznego.

W celu zapewnienia całkowicie bezpiecznego kanału łączności wystarczy połączyć kwantową dystrybucję klucza z całkowicie bezpiecznym szyfrem Vernama.

Szyfr Vernama – XOR z kluczem spełniającym 3 warunki:

- jednorazowy,
- losowy,
- długość klucza przynajmniej tak długa jak długość wiadomości.

Przykładowe algorytmy kryptografii kwantowej:

- **Algorytm Bennetta-Brassarda,**
- **Algortym Bennetta,**
- Algorytm Ekerta.

Algorytm Bennetta-Brassarda (1984)

Obsada:

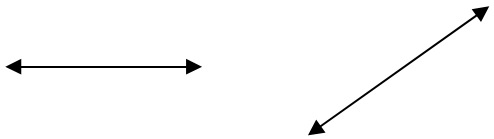
Renata

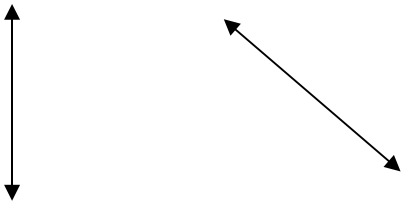
Andrzej

Roman

Algorytm Bennetta-Brassarda (1984)

Alfabet:

 = 0

 = 1

Algorytm Bennetta-Brassarda (1984)

Renata i Andrzej korzystają z kanału kwantowego np. światłowodu.

Renata wysyła Andrzejowi fotony o wybranej losowej polaryzacji. Odpowiadają one zgodnie z przyjętym alfabetem wartościom 0 i 1.

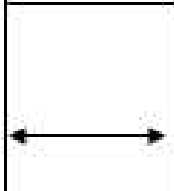
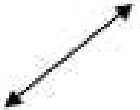
Andrzej mierzy polaryzację każdego fotonu i może w tym przypadku wybrać albo bazę prostą (+) albo ukośną (X).

Wyniki pomiaru są przez Andrzeja notowane.

W następnym kroku Andrzej korzystając z kanału publicznego informuje Renatę, jak ustawiał swój analizator dla poszczególnych fotonów.

Renata wskazuje, które ustawienia były pewne. Dla tych pewnych ustawień Andrzej dokonuje zamiany wybranych fotonów na wartości 0 oraz 1.

Otrzymany ciąg stanowi klucz kryptograficzny.

	0	1	1	0	1	0
						
	X	X	+	+	X	+
						
Zgodność	NIE	TAK	TAK	TAK	TAK	NIE
	-	1	1	0	1	-

Algorytm Bennetta-Brassarda (1984)

Średnio 50 % bitów zarejestrowanych przez Andrzeja to bity pewne.

Pozostałe 50 % niepewnych bitów zostaje odrzuconych, z czego 25% to bity prawidłowe mimo złego wyboru bazy a 25% to bity nieprawidłowe.

Algorytm Bennetta-Brassarda (1984)

Średnio 50 % bitów zarejestrowanych przez Andrzeja to bity pewne.

Pozostałe 50 % niepewnych bitów zostaje odrzuconych, z czego 25% to bity prawidłowe mimo złego wyboru bazy a 25% to bity nieprawidłowe.

Czy nie można podsłuchać transmisji?

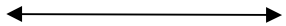
	0	1	1	0	1	0
	↔	↘↖	↕	↔	↘↖	↗↙
	+	+	+	+	+	+
	↔	↔	↕	↔	↕	↕
	X	X	+	+	X	+
	↘↖	↗↙	↕	↔	↘↖	↔
	NIE	TAK	TAK	TAK	TAK	NIE
	-	0	1	0	1	-

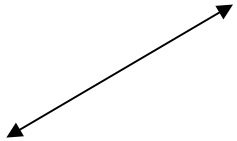
Każdy podsłuch zaburza przekaz. Przy dłuższych ciągach wystarczy sprawdzić 10% wygenerowanego klucza. 25% wykrytych niezgodności świadczy o podsłuchu transmisji.

Algorytm Bennetta (1992)

Protokół bezpiecznej wymiany klucza oparty na dwóch nieortogonalnych stanach kwantowych.

Załóżmy, że Renata korzysta z dwóch nieortogonalnych stanów kwantowych następującej postaci:

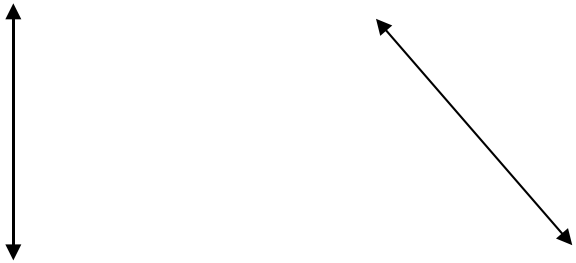
 = 0

 = 1

Algorytm Bennetta (1992)

Renata wysyła Andrzejowi fotony o wybranej losowej polaryzacji z dwóch polaryzacji określonych w założonym alfabecie. Odpowiadają one zgodnie z przyjętym alfabetem wartościom 0 i 1.

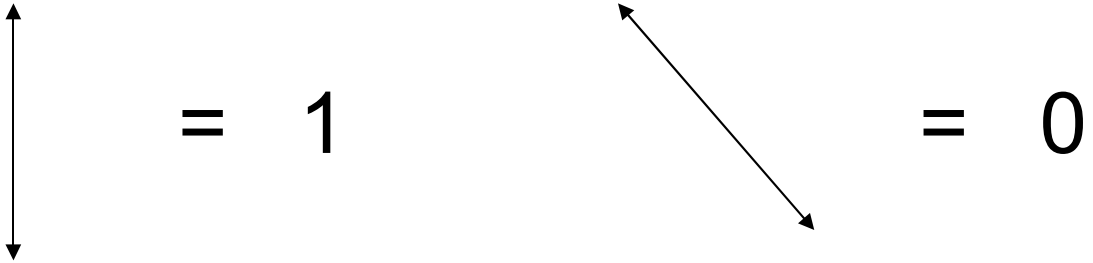
Andrzej dokonuje pomiaru w stanach ortogonalnych (prostopadłych) do stanów wybranych przez Renatę:



Algorytm Bennetta (1992)

Andrzej za każdym razem wybiera jeden z tych stanów i mierzy polaryzację w tym stanie.

W przypadku, gdy wybrał on polaryzację ortogonalną do polaryzacji wybranej przez Renatę, nie zarejestruje on fotonu. W przeciwnym razie z prawdopodobieństwem 1/2 zarejestruje on foton. Następnie przyporządkowuje mu wartość zgodną z poniższym alfabetem:



Algorytm Bennetta (1992)

W kolejnym kroku jawnym kanałem Andrzej przekazuje Renacie informacje, dla których fotonów udało mu się dokonać rejestracji. Nie podaje jednak jakie polaryzacje zmierzył. Renata i Andrzej przechowują ciąg bitów, dla których Andrzej zarejestrował foton.

Ciąg ten stanowi klucz kryptograficzny.

	0	1	1	0	1	0
	↔	↗	↗	↔	↗	↔
Zarejestrowany foton?	↘	↘	↕	↕	↕	↘
	**TAK**	**NIE**	**NIE**	**NIE**	**TAK**	**TAK**
	0	-	-	-	**1**	**0**

W przypadku, gdy nastąpi próba podsłuchu, spowoduje to błędy w kluczu, które zostaną wykryte przez Renatę i Andrzeja.

Komputery kwantowe

Teoria

Układ kwantowy złożony z N qubitów może występować w 2^N różnych stanach kwantowych reprezentowanych przez N-elementowe ciągi binarne.

Do opisu układu kwantowego złożonego z N qubitów potrzeba 2^N liczb.

Superpozycja stanów kwantowych poszczególnych qubitów oznacza, ze układ N qubitów może istnieć w wielu stanach kwantowych jednocześnie i w tym samym czasie można równolegle dokonywać operacji kwantowych na każdym ze stanów.

Komputer kwantowy, mający do dyspozycji 500 qubitów, miałby moc obliczeniową większą niż superkomputer zawierający tyle procesorów, ile jest cząstek elementarnych we wszechświecie!

Komputery kwantowe

Praktyka

Prototypy komputerów kwantowych:

- 1998 – Berkley – 2 qubity,
- 1999 – IBM – 3 qubity,
- 2000 – IBM – 5 qubitów,
- 2001 – IBM, Uniwersytet Stanford – 7 qubitów.

Komputery kwantowe

2000 – IBM – 5 qubitów

Qubity pełniły rolę pamięci i procesora.

Zasada działania tego komputera opierała się na kierunku obrotu tzw. spinie elektronów w powłokach atomu. Dodatni spin cząsteczki odczytujemy jako "1", kiedy jest ujemny - jako "0". Wykorzystywane są tutaj również stany superpozycji tzn. takie, gdzie spin może być jednocześnie dodatni i ujemny. Oznacza to, że taka cząsteczka posiada jednocześnie stan "0" i "1" oraz cały nieskończony ciąg wartości pomiędzy tymi stanami.

Fakt obserwacji tego zjawiska zmienia właściwości cząstek.

Prototyp wykorzystano do rozwiązania problemu znalezienia okresu funkcji.

Komputery kwantowe

2001 – IBM, Uniwersytet Stanford – 7 qubitów

Komputer kwantowy stanowił zsyntezowany związek chemiczny – perfluorobutadienylowy kompleks żelaza.

Na komputerze kwantowym uruchomiono algorytm Shora w celu rozkładu liczby 15. Związek chemiczny poddany został działaniu fal radiowych tak, by zmiana polaryzacji atomów odpowiadała krokom w algorytmie Shora, a wyniki rejestrowano używając metod znanych w spektroskopii magnetycznego rezonansu jądrowego.

Przesyłanie klucza w praktyce

W 1989 roku naukowcy z IBM skonstruowali prototypowe urządzenie realizujące protokół Benetta-Brassarda. Urządzenie to umożliwiło przesłanie fotonów na odległość 32 cm i pozwalało przesłać do 10 bitów/sek.

Obecnie istnieją rozwiązania umożliwiające przesyłanie fotonów na odległość 20 km w otwartej przestrzeni oraz do 150 km z wykorzystaniem światłowodów. Ze względu na brak możliwości podsłuchu bez wprowadzania błędów nie ma możliwości zastosowania w praktyce przekaźników, które umożliwiałyby przedłużenie odległości transmisji.

System transmisji zaproponowany przez NIST umożliwia transmisję miliona bitów na sekundę (bps). Wynik taki osiągnięto przy transmisji na odległość około 730 m.

Transakcje finansowe

Pierwsza transakcja finansowa, bezpieczeństwo, której gwarantowała kryptografia kwantowa, została przeprowadzona w kwietniu 2004 roku przez dwie austriackie instytucje bankowe (magistrat Wiednia i bank Austria Creditanstalt). Transmisja 3000 Euro odbyła się na dystansie 500 metrów.

W systemie tym wykorzystano pary splecionych fotonów. Jeden z fotonów przesyłany był z banku do magistratu przez światłowód. Na miejscu obserwowana była polaryzacja przesłanego fotonu. W dużym uproszczeniu, w przypadku par splątanych fotonów, zmiana stanu (spinu) jednego z nich powoduje jednoczesną zmianę stanu drugiego. Splecenie cząsteczek kwantowych zapewnia bezpieczeństwo transmisji, gdyż każda próba przechwycenia fotonów w czasie przysłania skutkuje natychmiast efektami, które widoczne są dla obydwu stron uczestniczących w komunikacji.

Sieć komputerowa

Pierwsza sieć komputerowa, w której dane szyfrowane są kwantowo uruchomiono na Uniwersytecie Cambridge. Sieć połączona została z Harvard University oraz Boston University Photonics. Pierwszy pakiet danych w sieci Quantum Net (Qnet) przesłał Chip Elliott, szef grupy inżynierów BBN Technologies z Cambridge. Projekt był finansowany przez DARPA (Defense Advanced Research Projects Agency). Informacje w sieci Qnet przesyłane są przez standardowy światłowód a ich bezpieczeństwo gwarantują klucze szyfrujące określone przez wymianę serii pojedynczych, spolaryzowanych fotonów.

Rozwiązania komercyjne

Rozwój badań nad kryptografią kwantową zaowocował pojawieniem się gotowych rozwiązań na rynku. Swoje rozwiązania zaproponowali znani producenci sprzętu komputerowego jak NEC czy Toshiba a także mniej znane firmy jak ID Quantique.

Rozwiązania komercyjne

Firma ID Quantique we współpracy z firmą Magiq stworzyły urządzenie QPN Security Gateway, które było jednym z pierwszych urządzeń dostępnych na rynku, zabezpieczających dane z wykorzystaniem kryptografii kwantowej. Koszt urządzenia wahał się w granicach 50000 – 100 000 USD.

Rozwiązania komercyjne

Aktualnie ID Quantique oprócz systemu do wymiany klucza proponuje urządzenia szyfrujące, które łączą kryptografię kwantową (wymiana klucza) oraz kryptografię tradycyjną (algorytm AES – szyfrowanie), jak również kwantowe generatory liczb losowych.

Clavis

Vectis

Inne rozwiązania

W ostatnim czasie Profesor Laszlo Kish z Teksasu zaproponował system bezpiecznej komunikacji o wiele prostszy niż kryptografia kwantowa.

Zaproponował on, aby wykorzystać klasyczne prawa fizyki oraz rezystory. Podstawą teoretyczną działania systemu jest drugie prawo Kirchoffa.

W proponowanym systemie dwie komunikujące się strony, Alice i Bob są połączone za pomocą zwykłego, dwużyłowego przewodu, tworząc obwód zamknięty.

Każde z nich dysponuje dwoma rezystorami - na przykład o opornościach 10 Ω i 1000 Ω.

Każda ze stron podłącza do przewodu w jednym momencie tylko jeden z rezystorów.

Inne rozwiązania

Możemy otrzymać zatem trzy możliwe układy:

- 10 + 10 – łączna oporność wyniesie 20 Ω,
- 1000 + 1000 – łączna oporność wyniesie 2000 Ω,
- 10 + 1000 – łączna oporność wyniesie 1010 Ω.

Podłączanie rezystorów jest losowe i odbywa się cyklicznie, według taktów zegara. Każda ze stron za każdym taktem mierzy opór łącza.

Opór = 20 Ω lub 2000 Ω traktujemy jako bezużyteczny.

Jeśli zaś opór wyniósł 1010 Ω, to wiadomo tylko, że jedna ze stron podłączyła 10 Ω a druga 1000 Ω. Jednak Alice i Bob wiedzą dokładnie kto podłączył jaki rezystor. Każdy taki takt może być wykorzystany do przekazania jednego bitu.

W praktyce podsłuch jest możliwy, poprzez włączenie się do obwodu i przyłożenie napięcia do każdej ze stron, ale z pierwszym odkrytym w ten sposób bitem podsłuchujący zostanie zdemaskowany.


Standard
GET KEN
AND WIN
05-006
Andy Davey

Dziękuję za uwagę