Kryptografia kwantowa

mgr inż. Krzysztof Maćkowiak

Konferencja CONFidence 2006

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

1. Wprowadzenie

Rozwój fizyki w XX wieku zmienił dotąd niezachwiany pogląd na świat oparty na pracach Newtona oraz Galileusza. Z jednej strony teoria względności Alberta Einsteina z drugiej strony mechanika kwantowa umożliwiająca modelowanie zjawisk zachodzących w mikroświecie. W celu przybliżenia zjawisk zachodzących w świecie kwantowym warto przybliżyć proste doświadczenie Erwina Schrödingera przeprowadzone pod koniec lat dwudziestych ubiegłego wieku.
Do szczelnego pudła wkładamy kota, źródło promieniotwórcze emitujące średnio jedną cząstkę na godzinę oraz detektor, który w chwili wykrycia cząstki uwolni trujący gaz. Po zamknięciu pudła i odczekaniu godziny mamy 50% prawdopodobieństwo, że kot jest martwy, i takie samo, że jest żywy. Tak się nam przynajmniej wydaje. Opierając się jednak na zasadach mechaniki kwantowej otrzymujemy coś innego - przed otwarciem pudła kot jest jednocześnie i żywy, i martwy! Znajduje się w tzw. superpozycji wszystkich możliwych stanów. Dopiero otwarcie pudła i sprawdzenie jego zawartości redukuje układ do jednego stanu - kot wyskakuje przerażony z pudła albo zostaje w nim martwy. Wielu uczonych wyjaśnia to istnieniem wielu równoległych wszechświatów. Hipotetyczny kot Schrödingera żyje w tej połowie wszechświatów, w których przeprowadzono eksperyment, a w drugiej połowie wszechświatów jest martwy! Istnienie swego rodzaju "cieni" wszechświatów równoległych można dostrzec w niektórych zjawiskach fizycznych. Przykładem są prążki interferencyjne powstające podczas przechodzenia światła przez dwie szczeliny. Eksperymenty dowiodły, że nawet pojedyncze fotony zachowują się tak, jakby przechodziły przez obie szczeliny jednocześnie. I tak robią - w jednym wariancie wszechświata przechodzą przez pierwszą, a w drugim przez drugą szczelinę.
Za początki teorii obliczeń kwantowych uznać można wczesne lata osiemdziesiąt XX wieku. W roku 1982 Richard Feynman stwierdził, iż przy symulacji układu kwantowego składającego się z R cząsteczek na zwykłym komputerze, nie da się uniknąć wykładniczego wzrostu czasu obliczeń wraz ze wzrostem R. Rozwiązaniem tego problemu byłaby budowa maszyny działającej zgodnie z prawami fizyki kwantowej. W 1985 roku Deutsch jako pierwszy zaproponował w pełni kwantowy model obliczeń oraz opis uniwersalnego komputera kwantowego. Kolejnym krokiem dokonanym przez Bernsteina i Vaziraniego było opracowanie modelu uniwersalnej kwantowej maszyny Turinga, umożliwiającej symulację dowolnej kwantowej maszyny Turinga w czasie wielomianowym. Przełomem w procesie popularyzacji obliczeń kwantowych był rok 1994, kiedy to Peter Shor przedstawił algorytmy kwantowe pozwalające na rozkład liczb na czynniki pierwsze oraz znajdowanie logarytmów dyskretnych w czasie wielomianowym.
Budowa i wykorzystanie komputerów kwantowych stwarza nadzieję na znaczną redukcję czasu obliczeń dla wielu problemów mających zastosowanie w praktyce jak np. przeszukiwanie baz danych czy też faktoryzacja dużych liczb. Sekretem tego jest kwantowa równoległość obliczeń. W maszynie kwantowej informacja reprezentowana jest przez stany kwantowe, będące wektorami w przestrzeni Hilberta a obliczenia dokonywane są na superpozycji tych stanów. Tak możliwości kształtują się w teorii. Praktyka jednak za teorią w tej kwestii nie nadąża. Dotąd nie udało się zbudować komputera kwantowego dużej mocy obliczeniowej a główny problem polega na spełnieniu sprzecznych warunków. Otóż z jednej strony komputer kwantowy musiałby być odseparowany od otoczenia w celu zapobiegnięcia zakłóceniom, z drugiej strony natomiast nie może być on całkowicie odizolowany od świata zewnętrznego, gdyż w trakcie wykonywania obliczeń powinna istnieć możliwość wpływania na ich przebieg. Dopiero rozwój prac nad problemem kwantowej korekcji błędów może doprowadzić do budowy komputera kwantowego o znaczącej mocy obliczeniowej.

2. Podstawowe pojęcia

Bit kwantowy (qubit) – dwupoziomowy układ kwantowy, inaczej dwuwymiarowa przestrzeń Hilberta H_2. Przestrzeń ta posiada ustaloną bazę obliczeniową B={|0>, |1>}, która składa się z dwóch stanów bazowych |0> oraz |1>.

Stan pojedynczego bitu kwantowego – 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.

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.

Osoba nadająca sygnał odpowiednio obracając polaryzatorem może dowolnie zmieniać kierunek każdego fotonu. Osoba odbierająca przekaz posiada przykładowo kryształ kalcytu odgrywający rolę analizatora. Kryształ kalcytu ma właściwość dwójłomności tzn. współczynnik załamania w tym krysztale zależy od kierunku polaryzacji światła. Gdy foton spolaryzowany jest ukośnie trafi do górnego fotopowielacza (zamienia światło na impuls elektryczny) z prawdopodobieństwem równym $\cos^2\alpha$, gdzie α jest kątem polaryzacji względem kierunku poziomego a do dolnego z prawdopodobieństwem $1-P = \sin^2\alpha$. Dla kąta 45° obydwa prawdopodobieństwa wynoszą ½. Dlatego jeżeli trafi do nas foton spolaryzowany pionowo to mamy jedynie pewność, że nie był to foton spolaryzowany poziomo.

Baza prosta (pewny pomiar fotonów spolaryzowanych pionowo i poziomo):

Wejście	**Wyjście**
Polaryzacja pozioma	Polaryzacja pozioma
Polaryzacja pionowa	Polaryzacja pionowa
Polaryzacja ukośna	Polaryzacja pionowa lub pozioma (z prawdopodobieństwem równym ½)

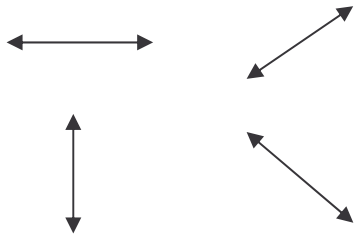
Baza ukośna (kryształ obrócony o kąt -45° (135°):

Wejście	Wyjście
Polaryzacja pozioma	Polaryzacja ukośna -45° (135°) lub 45° (z prawdopodobieństwem równym ½)
Polaryzacja pionowa	Polaryzacja ukośna -45° (135°) lub 45° (z prawdopodobieństwem równym ½)
Polaryzacja ukośna -45° (135°)	Polaryzacja ukośna -45° (135°)
Polaryzacja ukośna 45°	Polaryzacja ukośna 45°

Przykładowy zestaw pomiarowy mógłby się składać z emitera fotonów, kryształu oraz dwóch detektory fotonów.

Z zasady nieoznaczoności Heisenberga wynika, że nie możemy połączyć pomiarów polaryzacji prostej (pionowa i pozioma) z polaryzacją ukośną.

Załóżmy następujący alfabet:



= 0

= 1

Superpozycję dwóch stanów:

$$|\Psi> = 1/\sqrt{2}(|0>_1 |1>_2 + |1>_1 |0>_2)$$

Indeks wskazuje na numer qubitu. Superpozycja dwóch stanów układu dwóch qubitów oznacza, że pierwszy qubit znajduje się w stanie |0> a drugi w stanie |1> i jednocześnie pierwszy qubit znajduje się w stanie |1> a drugi w stanie |0>. Pomiar wykonany na jednym z qubitów natychmiast ustala stan drugiego, nawet jeśli są one oddalone od siebie o lata świetlne. Superpozycję dwóch stanów układu dwóch qubitów nazywamy często splątaniem. Termin ten został wprowadzony przez Schrödingera.

Twierdzenie o nieklonowaniu – nie można skopiować dowolnego stanów qubitów. Z wykorzystaniem bramek możemy kopiować jedynie stany bazowe.

Teleportacja stała się możliwa dzięki zastosowaniu niezwykłych własności stanów splątanych, na które po raz pierwszy zwrócili uwagę Albert Einstein, Borys Podolski i Nathan Rosen. Dysponując splątaną parą cząstek, stan pewnej cząstki źródłowej można teleportować wykonując kilka prostych działań. W tym celu wystarczy wykonać połączony pomiar wspólnego stanu jednej ze splątanych cząstek i cząstki źródłowej, a następnie przesłać wynik pomiaru do portu docelowego, gdzie stan cząstki źródłowej odtwarzany jest w stanie drugiej cząstki ze splatanej pary na podstawie otrzymanej informacji.

Teleportacja w praktyce

Anton Zeilinger w 1997 roku wspólnie ze swoimi współpracownikami zaprezentował eksperymentalnie możliwość teleportacji stanów fotonowych.

W roku 2004 Rainer Blatt wraz z grupą z Uniwersytetu w Innsbrucku dokonał teleportacji stanów kwantowych jonów wapnia w pułapce jonowej. W tym samym roku David Wineland dokonał teleportacji stanów kwantowych jonów berylu w pułapce jonowej.

3. Algorytm Grovera

Algorytm Grovera (1997) rozwiązuje problem szukania danego elementu w nieposortowanym, N-elementowym zbiorze, wykonując zaledwie liczbę operacji proporcjonalną do $\sqrt{N}$. Algorytm klasyczny wymaga w najgorszym przypadku przejrzenia wszystkich N elementów. Przez zastosowanie tego algorytmu uzyskujemy zatem przyspieszenie kwadratowe.

W 1997 roku Grover zaproponował kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych. Problem polega na wyszukaniu w nieuporządkowanym zbiorze danych zawierającym N elementów określonego elementu d_j. Przykładowo, może to być wyszukanie w spisie telefonów danego numeru telefonu nie znając nazwiska abonenta. Klasyczne algorytmy poszukiwań potrzebuje średnio $N/2$ kroków na wyszukanie danej informacji w zbiorze danych zawierającym N elementów. Algorytm kwantowy zaproponowany przez Grovera jest w tym przypadku bardziej efektywny i potrzebuje średnio $\sqrt{N}$ kroków na wyszukanie właściwego elementu w zbiorze składającym się z N elementów.
Każdy element zbioru, w którym prowadzimy poszukiwania ma określony indeks i. Zatem problem wyszukiwania sprowadza się w zasadzie do wyznaczenia na drodze przekształceń unitarnych odpowiedniego indeksu określającego dany element w zbiorze. Inaczej mówiąc, należy wyznaczyć operację unitarną:

$$U|i\rangle = \begin{cases} |i\rangle \text{ jeżeli } i=j \\ -|i\rangle \text{ jeżeli } i\neq j \end{cases}$$

gdzie j jest indeksem poszukiwanego elementu.

O efektywności algorytmu Grovera najlepiej świadczy następujący przykład.
W zagadnieniach klasycznej kryptografii przy dekodowaniu nieznanych szyfrów występuje konieczność wyszukiwania zadanych elementów w zbiorze zawierającym około $N = 10^{16}$ nieuporządkowanych elementów. Najszybszy z istniejących klasycznych komputerów wykonałby taka czynność w czasie około tysiąca lat. Natomiast komputer kwantowy wykorzystujący przedstawiony powyżej algorytm wyznaczyłby poszukiwany element zbioru w ciągu kilku minut.
Algorytm Grovera może być uogólniony i zastosowany do jednoczesnego poszukiwania kilku wybranych elementów w nieuporządkowanym zbiorze danych, oraz do wyszukiwania największego lub najmniejszego elementu w zbiorze.

4. Algorytm Shora

Koncepcja kryptografii z kluczem jawnym zaproponowana została przez Whitfielda Diffiego i Martina Hellmana oraz niezależnie, przez Ralpha Merkle'a. Zaproponowali oni by klucz składał się z pary kluczy – szyfrującego i deszyfrującego a wyznaczenie klucza deszyfrującego z klucza szyfrującego byłoby niemożliwe. Dzięki temu mimo opublikowania klucza szyfrującego (publicznego), szyfrogram zaszyfrowany tym kluczem nadal pozostaje dobrze zabezpieczony. Kryptografia asymetryczna opiera się najczęściej na zastosowaniu jednego z dwóch problemów: problemu logarytmu dyskretnego oraz problemu faktoryzacji czyli rozłożenia liczby na czynniki pierwsze. Najbardziej popularnym algorytmem kryptografii asymetrycznej jest algorytm RSA. Jego bezpieczeństwo opiera się na faktoryzacji. Warto sobie zadać pytanie czy jest on jednak bezpieczny?

Najszybszy obecnie algorytm faktoryzacji liczb wymaga czasu równego w przybliżeniu $\exp[1.9(\ln N)^{1/3}(\ln\ln N)^{2/3}]$. Faktoryzacja liczby 400-cyfrowej z zastosowanie takiego algorytmu zajmowałaby około 10^{10} lat. Przy zastosowaniu algorytmu Shora złożoność obliczeniowa rozkładu liczby N wynosi w przybliżeniu $(\ln N)^3$, czyli rozłożenie na czynniki pierwsze liczby składającej się ze 129 cyfr zajęłoby na komputerze kwantowym z zegarem 100MHz zaledwie kilka sekund, podczas gdy złamanie klucza składającego się z 400 cyfr niewiele ponad minutę.

Zasada działania algorytmu Shora

Załóżmy, że mamy liczbę N=15, którą chcemy poddać faktoryzacji, czyli rozkładowi na czynniki pierwsze. Wybieramy liczbę losową $1<X<N$-1 względnie pierwszą z N (NWD(N,X)=1) powiedzmy niech to będzie X=2.

Rejestr dwuqubitowy:
$|A\rangle = 1/\sqrt{2}\ (|0\rangle + |1\rangle) * 1/\sqrt{2}\ (|0\rangle + |1\rangle) = ½\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = ½\ (|0\rangle + |1\rangle + |2\rangle + |3\rangle)$.
Rejestr dwuqubitowy przechowuje z jednakowymi amplitudami jednocześnie cztery liczby.

Klasycznie na przechowanie czterech liczb potrzebujemy czterech rejestrów dwubitowych – każda liczba umieszczana jest wtedy w innym rejestrze. Gdybyśmy dysponowali rejestrem kwantowym złożonym z N qubitów, to moglibyśmy przechować w takim rejestrze 2^N liczb. Komputer kwantowy wykonuje operacje na całym rejestrze, czyli na wszystkich 2^N liczbach jednocześnie. Zjawisko to nazywane jest kwantowym parallelizmem.

Przygotujmy 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

Wykonujemy następnie operację X^A mod N i wyniki umieszczamy w rejestrze B. Komputer kwantowy dzięki równoległości obliczeń wykonuje taką 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

Jak widać wartości w rejestrze *B* są wartościami okresowymi a okres wynosi w tym przypadku r=4. Komputer kwantowy potrafi szybko znaleźć okres funkcji. Jeżeli okaże się, że *r* jest wartością nieparzystą, wybieramy inną wartość *X* i zaczynamy obliczenia od początku. Natomiast jeżeli *r* jest parzyste jak w naszym przykładzie, obliczamy $P=X^{r/2}-1$ lub $P=X^{r/2}+1$ i sprawdzamy czy *P* jest dzielnikiem *N*. W naszym przypadku r=4 i $P=2^{4/2}-1=3$ lub $P=2^{4/2}+1=5$.

15/3=5
15/5=3

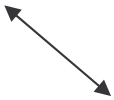
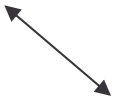
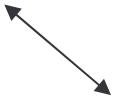
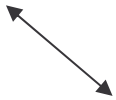
ODNIEŚLIŚMY SUKCES ☺

5. Algorytm Bennetta-Brassarda

Przez kryptografię kwantową rozumiemy kwantową dystrybucję klucza kryptograficznego. Pierwszym i najbardziej znanym algorytmem zapewniającym bezpieczną dystrybucję klucza kryptograficznego jest algorytm Bennetta-Brassarda. Poniżej przedstawione zostały podstawowe zasady działania tego algorytmu.

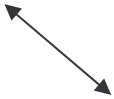
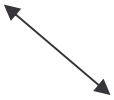
Alice i Bob korzystają z kanału kwantowego np. światłowodu. Alice wysyła Bobowi fotony o wybranej losowej polaryzacji. Odpowiadają one zgodnie z przyjętym alfabetem wartościom 0 oraz 1.
Bob mierzy polaryzację każdego fotonu i może w tym przypadku wybrać albo bazę prostą (+) lub ukośną (X). Wyniki pomiaru są przez Boba notowane. W następnym kroku Bob korzystając z kanału publicznego informuje Alice, jak ustawiał swój analizator dla poszczególnych fotonów. Alice wskazuje, które ustawienia były pewne (dla fotonów poziomych i pionowych – baza prosta, dla fotonów ukośnych – baza ukośna). Dla tych pewnych ustawień Bob dokonuje zamiany wybranych fotonów na wartości 0 oraz 1. Otrzymany ciąg stanowi klucz kryptograficzny.

Przykład:

Losowy ciąg (Alice)	0	1	1	0	1	0
Fotony (Alice)						
Analizator (Bob)	X	X	+	+	X	+
Otrzymane fotony (Bob)						
Zgodność	NIE	TAK	TAK	TAK	TAK	NIE
Otrzymany klucz (Bob)	-	**1**	**1**	**0**	**1**	-

Można określić, że średnio 50 % bitów zarejestrowanych przez Boba to bity pewne. Pozostałe 50 % niepewnych bitów zostaje odrzuconych, z czego 25% to bity prawidłowe mimo złego wyboru bazy a 25% to bity nieprawidłowe.

Wiemy w jaki sposób przekazać klucz kryptograficzny. Ale czy jest to bezpieczne – co by się stało jakby transmisja była podsłuchiwana?

Losowy ciąg (Alice)	0	1	1	0	1	0
Fotony (Alice)						
Analizator (Ewa)	+	+	+	+	+	+
Otrzymane fotony (Ewa)						
Analizator (Bob)	X	X	+	+	X	+
Otrzymane fotony (Bob)						
Zgodność	NIE	TAK	TAK	TAK	TAK	NIE
Otrzymany klucz (Bob)	-	**0**	**1**	**0**	**1**	-

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

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

6. Algorytm Bennetta

Algorytm ten został zaproponowany przez Charlesa Bennetta w roku 1992. Podobnie jak w przypadku algorytmu Bennetta-Brassarda wykorzystywany jest on jako protokół bezpiecznej wymiany klucza i oparty jest na dwóch nieortogonalnych stanach kwantowych.

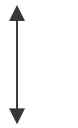
Załóżmy, że Alice korzysta z dwóch nieortogonalnych stanów kwantowych następującej postaci:

 = 0

 = 1

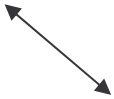
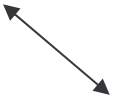
Algorytm wymiany klucza wygląda następująco:
Alice wysyła Bobowi fotony o wybranej losowej polaryzacji z dwóch polaryzacji określonych w założonym alfabecie. Odpowiadają one zgodnie z przyjętym alfabetem wartościom 0 i 1.
Bob dokonuje pomiaru w stanach ortogonalnych (prostopadłych) do stanów wybranych przez Alice:

Bob za każdym razem wybiera jeden z powyższych stanów i mierzy polaryzację w tym stanie. W przypadku, gdy wybrał on polaryzację ortogonalną do polaryzacji wybranej przez Alice, nie zarejestruje on fotonu. W przeciwnym razie z prawdopodobieństwem ½ zarejestruje foton. Następnie przyporządkowuje mu wartość zgodną z poniższym alfabetem:

 = 1

 = 0

W kolejnym kroku jawnym kanałem Bob przekazuje Alice informacje, dla których fotonów udało mu się dokonać rejestracji. Nie podaje jednak jakie polaryzacje zmierzył. Alice i Bob przechowują ciąg bitów, dla których Bob zarejestrował foton. Ciąg ten stanowi klucz kryptograficzny.

Losowy ciąg (Alice)	0	1	1	0	1	0
Fotony (Alice)						
Stany (Bob)						
Zarejestrowany foton?	**TAK**	NIE	**NIE**	NIE	**TAK**	**TAK**
Otrzymany klucz (Bob)	**0**	**-**	**-**	**-**	**1**	**0**

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

7. Praktyczne zastosowanie

7.1. Komputery kwantowe

W roku 1982 Richard Feynman stwierdził, iż przy symulacji układu kwantowego składającego się z R cząsteczek na zwykłym komputerze, nie da się uniknąć wykładniczego wzrostu czasu obliczeń wraz ze wzrostem R. Rozwiązaniem tego problemu byłaby budowa maszyny działającej zgodnie z prawami fizyki kwantowej. Matematyczne podstawy komputera kwantowego zostały opracowane przez Davida Deutscha w roku 1985.
Układ kwantowy złożony z N qubitów może występować w 2^N różnych stanach kwantowych reprezentowanych przez N-elementowe cięgi binarne. Zatem do opisu układu kwantowego złożonego z N qubitów potrzeba 2^N liczb. Istotną cechą N-qubitowego komputera kwantowego jest zjawisko zwane superpozycją stanów kwantowych poszczególnych qubitów. 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. Zatem komputer kwantowy może wykonywać olbrzymią liczbę operacji atematycznych równolegle, wykorzystując do tego celu jeden procesor kwantowy. Komputer kwantowy, mający do dyspozycji 500 qubitów, miałby moc obliczeniową większą niż superkomputer zawierający tyle procesorów, ile jest cząstek elementarnych we wszechświecie!
Qubity mają w komputerach kwantowych pełnić jednocześnie rolę dzisiejszej pamięci operacyjnej oraz jednostki obliczeniowej. Porównując architekturę komputerów kwantowych z komputerami konwencjonalnymi, obliczenia wykonywane na qubitach odpowiadałyby wykonywaniu wszystkich operacji bezpośrednio na rejestrach CPU.
Jak dotąd powstało zaledwie kilka prototypów i to dalekich od oczekiwań. Pierwszym był, opracowany w Berkley w roku 1998, system złożony z zaledwie dwóch qubitów. Rok później udało się w laboratoriach IBM utworzyć system złożony z trzech qubitów.
15 sierpnia 2000 firma IBM podała sensacyjną wiadomość o skonstruowaniu komputera kwantowego składającego się z 5 qubitów, które działały razem jako procesor i pamięć. Zasada działania tego komputera opierała się na kierunku obrotu tzw. spinie elektronów w powłokach atomu a dokładniej na specyficznej właściwości cząstek elementarnych. Mogą one mianowicie "wirować" jednocześnie w różnych kierunkach (posiadać różny spin), jednak sam fakt obserwacji tego zjawiska zmienia właściwości cząstek. Kiedy spin danej cząsteczki jest dodatni, jego stan można odczytać jako "1", kiedy jest ujemny - jako "0". Binarne ciągi zer i jedynek odpowiadają więc krótkim okresom działania i spoczynku obwodów wspomnianego komputera. 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. Eksperymentalny komputer IBM został użyty do rozwiązania typowego matematycznego problemu, mianowicie do znalezienia okresu danej funkcji. Prototyp wykonał wszystkie obliczenia w jednym etapie, natomiast zwykły komputer potrzebowałby na to wielu kolejnych cykli operacji.
W roku 2001 zbudowano komputer o siedmiu qubitach, na których w pełni zadziałał algorytm Shora. Eksperyment ten przeprowadzono w laboratoriach IBM i Uniwersytetu Stanford. Zespół naukowców zajął się rozkładem liczby 15. Przypomnijmy, że 15=3*5. Po dokładnym zbadaniu algorytmu Shora w tym konkretnym przypadku i dokonaniu optymalizacji okazuje się, że trzeba zbudować urządzenie kontrolujące 7 qubitów. Był to pierwszy w historii eksperyment jednoczesnego kontrolowania siedmiu qubitów.

Komputerem kwantowym był w tym przypadku specjalnie zsyntezowany związek chemiczny – perfluorobutadienylowy kompleks żelaza – pięć atomów fluoru i dwa atomy węgla używanych było jako qubity. Związek ten poddawano działaniu fal radiowych tak, by zmiana polaryzacji atomów odpowiadała krokom w algorytmie Shora, a wyniki rejestrowano używając metod znanych w spektroskopii magnetycznego rezonansu jądrowego. Wynik eksperymentu pokazał, że założenia algorytmu Shora są poprawne. Główną przeszkodą w skutecznym używaniu tego algorytmu dla większych wartości jest szum. Istotą algorytmu jest precyzyjne odczytanie wzmacnianych wielkości. A są one odczytywane tylko z przybliżeniem. Jeśli ma być ich bardzo wiele, to może okazać się, że nawet wzmocnione wielkości nie zostaną odróżnione od tła. Dla rozkładu liczby 15 potrzeba 7 qubitów, dla rozkładu liczby RSA-174 o blisko 600 bitach długości potrzeba byłoby ponad 1200 qubitów. Każdy z qubitów wszedłby ponad 1200 razy w interakcje z pozostałymi i żadna z interakcji nie mogłaby przeszkadzać innym. Zjawisko takiego przeszkadzania nazywa się dekoherencją i jednym ze źródeł szumu. Co więcej, w zasadzie nie wiadomo jak w ogóle zmusić odległe od siebie jony będące nośnikami qubitów do takich interakcji.
Klasyczna teoria obliczeń doskonale sobie radzi z szumem. Zgodnie z teorią informacji Shanonna zawsze można zapewnić prawie bezbłędność przekazu zapewniając odpowiednią nadmiarowość informacji. W przypadku świata kwantowego argument ten nie jest możliwy do zastosowania. Informacja nie może być skopiowana, jak już wspominaliśmy. Właściwie, to nawet wykrycie, że zaszedł błąd jest niemożliwe.

7.2. Przesyłanie klucza w praktyce

W 1989 roku naukowcy z IBM skonstruowali prototypowe urządzenie realizujące protokół Benetta-Brasarda. Urządzenie to umożliwiło przesłanie fotonów na odległość 32 cm i pozwalało przesłać do 10 bitów/sek. Początek XXI wieku to bicie rekordów w odległości przesyłania fotonów w powietrzu oraz z wykorzystaniem światłowodów. 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.
Cały czas trwają badania na rozwojem kryptografii kwantowej. Unia Europejska zainwestuje 11 mln Euro w system SECOQC (Secure Communication basad on Quantum Cryptography). Powstało również konsorcjum firm, które otrzymało od rządu australijskiej prowincji Wiktoria grant w wysokości 2,5 miliona dolarów. Pieniądze mają zostać przeznaczone na opracowanie urządzeń zdolnych do wytwarzania i używania pojedynczych fotonów do przechowywania i przesyłania informacji.

7.3 Transakcja finansowa z wykorzystaniem kryptografii kwantowej

Pierwsza transakcja finansowa, bezpieczeństwo, której gwarantowała kryptografia kwantowa, została przeprowadzona w kwietniu 2004r. przez dwie austriackie instytucje bankowe. Transakcja przeprowadzona została pomiędzy dwoma austriackimi instytucjami: magistratem Wiednia i bankiem Austria Creditanstalt. System kryptograficzny stworzył Anton Zeilinger wraz z zespołem kolegów z Uniwersytetu Wiedeńskiego oraz pracownikami austriackiej firmy ARC Seibersdorf Research. Transmisja 3000 Euro odbyła się na dystansie 500 metrów.

W systemie tym wykorzystano pary splecionych fotonów generowane światłem lasera, który przechodząc przez kryształ dzielił pojedynczy foton na dwa. Jeden z fotonów wygenerowanej pary był następnie przesyłany z banku do magistratu przez światłowód. Po dotarciu do miejsca przeznaczenia obserwowana była polaryzacja przesłanego fotonu, która gwarantowała zarówno nadawcy jak i odbiorcy identyczność przesłanych danych (zero lub jedynkę). Mechanizm ten pozwala więc stworzyć klucz szyfrujący, który może być wykorzystany do zabezpieczenia transakcji finansowych.
W dużym uproszczeniu, w przypadku par splątanych fotonów, zmiana stanu (spinu) jednego z nich powoduje jednoczesną zmianę stanu drugiego. Dzieje się to natychmiast, przy czym odległość między nimi nie ma najmniejszego znaczenia. Nie bez powodu Einstein, który zresztą nie bardzo potrafił wyjaśnić istotę splątania, nazwał to zjawisko "upiornym działaniem na odległość".
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. Natomiast losowy dobór klucza szyfrującego sprawia, że zachowując zasadę stosowania za każdym razem innego klucza szyfrującego, także transmisja przez całkowicie niezabezpieczony kanał gwarantuje zachowanie poufności przesyłanych danych.

7.4 Sieć komputerowa oparta na kryptografii kwantowej

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). Sieć składa się z sześciu serwerów. Istnieje możliwość połączenia jej z komputerami włączonymi do Internetu. W opinii twórców sieci Qnet, implementacja kolejnych węzłów sieci w bankach i instytucjach finansowych umożliwi wymianę danych przez Internet w sposób dużo bardziej bezpieczny, niż umożliwiają to obecne rozwiązania kryptograficzne. Informacje w sieci Qnet przesyłane są przez standardowy światłowód a ich bezpieczeństwo gwarantują klucze szyfrujące określone przez wymianę serii pojedynczych, spolaryzowanych fotonów.

7.5 Rozwiązania komercyjne dostępne na rynku

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. To właśnie urządzenie tej ostatniej firmy - QPN Security Gateway było jednym z pierwszych urządzeń dostępnych na rynku, zabezpieczających dane z wykorzystaniem kryptografii kwantowej. Koszt urządzenia wahał się w granicach 50 000-100 000 USD. 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.

7.6 Inne podejście do tematu

W ostatnim czasie Profesor Laszlo B. 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. 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 odbywa się cyklicznie, według taktów zegara. Istotne jest to, że wybór rezystora, który ma być podłączony musi być w każdym kroku losowy. Każda ze stron za każdym taktem mierzy opór łącza. Jeśli wyniósł on 20 Ω lub 2000 Ω (dwa takie same rezystory), to takt jest pomijany jako bezużyteczny. Jeśli zaś wyniósł 1010 Ω, to powstaje ciekawa sytuacja – z zewnątrz 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.

Podsłuchanie takiej łączności jest praktycznie niemożliwe, dlatego że podsłuchiwacz będzie tylko widzieć zmiany napięcia, odpowiadające zmieniającym się opornościom, ale nie będzie wiedział kto co podłączył. W praktyce łatwo to zmierzyć, samemu włączając się do obwodu i przykładając napięcie do każdej ze stron, ale z pierwszym odkrytym w ten sposób bitem sam zostanie zdemaskowany, podobnie jak w kryptografii kwantowej.

Kish przewidział jeszcze jedno zabezpieczenie komunikacji. Dzięki szumowi termicznemu powstającemu w rezystorach łączność może odbywać się bez dodatkowego zasilania i wtedy, z punktu widzenia podsłuchującego, taka komunikacja jest niewidzialna. Ma ona jednak poważne ograniczenie – na łączu długości 1 km można w ten sposób przesłać zaledwie 2000 bitów na sekundę.

W praktyce system ma niską przepustowość, ale jak zauważa Kish komponenty potrzebne do jego budowy są około 100 do 1000 razy tańsze niż te, z których zestawia się łącza kwantowe. Dzięki zastosowaniu przewodów wielożyłowych można łatwo stworzyć łącze o przepustowości stukrotnie większej od pojedynczego kanału. System jest również o wiele bardziej odporny na praktyczne problemy związane z jakością przewodnika i przypadkowymi zakłóceniami.

8. Podsumowanie

Rozwój badań w dziedzinie informatyki i kryptografii kwantowej napawa optymizmem. Nowe rozwiązania komercyjne i głośne doświadczenia powodują zainteresowanie tym tematem wśród dużych firm i instytucji. Prawdziwy przełom nastąpi jednak w momencie, gdy uda się zbudować komputer kwantowy składający się z dużej liczby qubitów. Fakt ten zmieni spojrzenie na informatykę i może być początkiem rewolucji w przemyśle komputerowym. Wszystkich zachęcam do śledzenia wiadomości o rozwoju tej fascynującej dziedziny nauki.

9. Literatura

Algorytmy kwantowe, M. Hirvensalo, 2004
Kryptografia kwantowa, W. Broniowski
Kryptografia kwantowa, R. Tanaś, 2002
Kwantowe systemy informatyki, S. Węgrzyn, J. Klamka, J. Miszczak, 2003
Niezwykłe cechy informacji kwantowej, M. Horodecki, 2002
Quantum Computing, S. Stupkiewicz, J. Warzecha, 2005
Quantum Cryptography: Public Key Distribution And Coin Tossing, C. Bennett, G. Brassard, 1984
Quantum Cryptography Using Any Two Nonorthogonal States, C. Bennett, 1992
Teleportacja stanów atomowych z wykorzystaniem kwantowej interferencji pól wychodzących z dwóch rezonatorów, G. Chimczak, 2005
Wprowadzenie do teorii komputerów kwantowych, O. Siedlecka