STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Piotr GAWRON, Krzysztof GROCHLA
Instytut Informatyki Teoretycznej i Stosowanej PAN

KWANTOWA DYSTRYBUCJA KLUCZY W SIECIACH OPTYCZNYCH+

Streszczenie. W artykule jest przedstawiona jedna z podstawowych metod kwantowej dystrybucji klucza – protokół BB84. Wyjaśnione są niezbędne podstawy informatyki kwantowej oraz omówione są metody implementacji przy zastosowaniu technik optycznych.

Słowa kluczowe: komputery kwantowe, kwantowa dystrybucja klucza.

QUANTUM KEY DISTRIBUTION IN OPTICAL NETWORKS

Summary. In article is presented one of basic method of quantum key distribution – BB84 protocol. Basics of qunatum computer science are explained. Methodes of implenetation with use of optical technics are discused.

Keywords: quantum computers, quantum key distribution.

1. Wstęp – komputery kwantowe, kwantowa teoria informacji

Powstanie idei komputerów kwantowych [12] [13] [14] oraz opublikowanie algorytmów Shora [1] i Grovera [2] zmieniło podejście do informatyki. Informacja, przedmiot badań tej dziedziny nauki, jest fizyczna i jako taka musi być na pewnym poziomie abstrakcji traktowana. W informatyce klasycznej stosuje się prawa fizyki statystycznej, gdyż liczba cząstek reprezentująca bit informacji jest duża z punktu widzenia mikroświata. Jednakże ciągła miniaturyzacja prowadzi do tego, iż zostanie osiągnięta granica, poniżej której trzeba będzie skorzystać z dokładniejszego modelu opisu mikroświata, a mianowicie mechaniki kwantowej. Powstały modele obliczeń uwzględniające fizyczną naturę informacji.

+Praca wykonana w ramach projektu KBN nr 7 T11C 017 21

W niniejszym artykule przedstawimy ideę kwantowej dystrybucji klucza pod względem teoretycznym oraz praktycznych realizacji.

Nazwa protokołu wywodzi się od jego twórców Gilles'a Brassarda i Charlsa Bennetta, których tematem badań jest głównie kwantowa teoria informacji [8].

2. Podstawy algorytmu BB84 — podstawy informatyki kwantowej

Podstawową jednostką informatyki kwantowej jest qubit. Pojedynczy qubit może być przedstawiony jako dwustanowy układ kwantowy o spinie jedna-druga. Do opisu takiego układu stosuje się zbiór wektorów z przestrzeni $\mathbb{C}^2$, których długość unormowana jest do jedności. Dodatkowo zakładamy, że wektory różniące się tylko o czynnik fazowy, w sensie fizycznym reprezentują ten sam stan.

Aby przedstawić działanie protokołu BB84 [8], musimy omówić podstawowe wybrane własności układów kwantowych.

Dowolny układ kwantowy [3] [5], w szczególności jednoqubitowy, może znajdować się w dowolnej superpozycji stanów bazowych:

$$|\psi\rangle = \sum_i c_i |c_i\rangle, \; gdzie \sum_i |c_i|^2 = 1, c_i \in \mathbb{C} \;\; oraz \; |c_i\rangle \in \mathbb{C}^{2^n} \tag{1}$$

W informatyce kwantowej stosuje się bazy ortonormalne. Dla prezentacji protokołu BB84 wystarczy wprowadzenie dwóch baz:

kanonicznej — $\left\{ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ i

diagonalnej — $\left\{ |+\rangle = \frac{\sqrt{2}}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, |-\rangle = \frac{\sqrt{2}}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$.

Qubit jest opisywany przez unormowaną do jedności kombinację liniową wektorów bazowych: $|\psi\rangle = a|0\rangle + b|1\rangle$, gdzie $a, b \in \mathbb{C} \; i \; |a|^2 + |b|^2 = 1$. Upraszczając, możemy powiedzieć, że w wyniku pomiaru otrzymujemy jeden ze stanów bazowych, przy czym prawdopodobieństwo otrzymania każdego z nich wynosi odpowiednio: $|a|^2 \, dla \, |0\rangle$ i $|b|^2 \, dla \, |1\rangle$*. Jeżeli dokonujemy pomiaru w danej bazie stanu, który jest jej wektorem bazowym, to w wyniku otrzymujemy ten sam wektor bazowy. Jeżeli dokonujemy pomiaru stanu $|+\rangle$ lub $|-\rangle$ w bazie kanonicznej, to w wyniku otrzymamy z prawdopodobieństwem

*Autorzy zdają sobie sprawę z uproszczenia, jakiego tu się dopuszczają, jednakże takie przedstawienie jest tutaj wystarczające. Dokładny opis tego zagadnienia można znaleźć w [3] i [5].

½ stan $|0\rangle$ lub $|1\rangle$. Odpowiednio, jeżeli w bazie diagonalnej mierzymy stan $|0\rangle$ lub $|1\rangle$, to otrzymujemy z równym prawdopodobieństwem ½ stan $|+\rangle$ lub $|-\rangle$.

Twierdzenie 1. (O nieklonowaniu) Nie jest możliwe skopiowanie stanu kwantowego. Czyli nie jesteśmy w stanie zduplikować nieznanego nam pojedynczego stanu. Sytuacja wygląda kompletnie, inaczej jeżeli mamy dużą ilość identycznych stanów. Wtedy przez serię pomiarów możemy znaleźć pewne przybliżenie nieznanego nam stanu. Dowód twierdzenia można znaleźć np. w [3].

Powyższe dwie własności mechaniki kwantowej leżą u podstaw teoretycznych protokołu BB84. Zmiana stanu w wyniku pomiaru i niemożność kopiowania stanów kwantowych daje pewność wykrycia podsłuchu podczas wymiany klucza.

3. Zmodyfikowany protokół BB84

Celem wykorzystania protokołu BB84 jest bezpieczna dystrybucja klucza, rozumianego jako ciąg bitów 0 i 1, pomiędzy dwoma osobami: Alicją i Bobem. Osoba, która chce podsłuchać komunikację, jest tradycyjnie nazywana Ewą. Dystrybucja klucza polega na wymianie losowego ciągu bitów, który następnie może zostać wykorzystany do szyfrowania danych przesyłanych klasycznym kanałem komunikacyjnym. Możliwe metody szyfrowania, to: dokonanie operacji XOR bit po bicie lub zastosowanie któregoś z symetrycznych algorytmów szyfrujących typu DES [4].

Do realizacji protokołu BB84 wykorzystywany jest niezabezpieczony kanał kwantowy – czyli taki, który daje możliwość przesyłania qubitów, oraz niezabezpieczony klasyczny kanał transmisyjny, czyli taki, którym przesyłane są informacje w postaci ciągu bitów. W szczególności kanał kwantowy może być realizowany poprzez transmisję światłowodową lub transmisję fotonów w powietrzu. Kanał klasyczny – to dowolna sieć komputerowa,np: oparta na przewodach miedzianych lub światłowodach. Kanał niezabezpieczony – to taki, do którego dostęp mogą mieć osoby trzecie i mogą one swobodnie manipulować sygnałami, tzn. odczytywać je, a nawet zmieniać. O komunikacji przez taki kanał mówimy, że jest publiczna.

Kroki protokołu:

1. Alicja wysyła sekwencję qubitów, z których każdy jest w losowo i niezależnie wybranym stanie: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$.
2. Dla każdego qubitu Bob wybiera losowo i niezależnie bazę (kanoniczną lub diagonalną), w której będzie dokonywał pomiaru.
3. Bob zapisuje wyniki pomiarów i bazy, w których zostały one dokonane.
4. Bob wysyła do Alicji klasycznym jawnym kanałem informacyjnym bazy, w których został dokonany pomiar.

5. Alicja przekazuje Bobowi informację, których pomiarów dokonał w dobrej bazie.
6. Alicja i Bob dzielą dane na dwie części względem zgodności użytych baz.

Możemy zauważyć, że średnio w połowie przypadków została użyta zła baza. Przez złą bazę pomiaru rozumiemy taką, że dla Alicji i Boba są one różne. W takim przypadku dane muszą zostać odrzucone, gdyż wynik pomiaru w złej bazie jest całkowicie losowy. Wynika z tego natychmiastowy wniosek, że sprawność protokołu BB84 nie przekracza 50%. Można też zauważyć, że jeżeli nie zaistniały przekłamania i nikt nie ingerował w proces transmisji, to pozostałe 50% qubitów zmierzonych przez Boba posiada ten sam stan, jaki został nadany przez Alicję. Zatem, są one kandydatami do surowego klucza, czyli wymagają one jeszcze dalszego przetworzenia.

7. Alicja i Bob wybierają pewien wspólny podzbiór qubitów spośród tych, które zostały zmierzone w zgodnych bazach i jawnie je porównują, qubity te są oczywiście odrzucone jako że zostały ujawnione. W przypadku idealnym, jeżeli nie nastąpił podsłuch informacji, to porównanie powinno dać całkowicie zgodne wyniki. Jednakże w rzeczywistości w wyniku niedoskonałości kwantowego kanału informacyjnego porównanie to może wykazać różnice pomiędzy stanami nadanymi przez Alicję i zmierzonymi przez Boba.

Istnieje wiele metod, które dają możliwość eliminacji błędów transmisji w kanale kwantowym. Polegają one na wymianie częściowej informacji, poprzez kanał klasyczny pomiędzy Alicją i Bobem, o posiadanych ciągach bitów.

Najprostsze metody ataku, czyli strategie działania Ewy:

1. Ewa może wpiąć się do kwantowego kanału transmisji i przechwytywać wszystkie qubity nadesłane przez Alicję, dokonywać na nich pomiaru i następnie odsyłać do Boba. Taka technika podsłuchu jest bardzo łatwa do zdemaskowania, gdyż nieznając bazy, w której zostały nadane qubity, Ewa doprowadza do zmiany stanów qubitów, co jest łatwe do wykrycia dla Alicji i Boba po wymianie klucza.
2. Drugą techniką, jaką może zastosować Ewa, jest wyłapywanie tylko niektórych fotonów w ten sposób udając niedoskonałość kanału kwantowego. Metoda ta może przynieść wydobycie pewnej ilości informacji z transmisji, jednakże techniki zwane wzmocnieniem prywatności [6] chronią w pewnej mierze przed takim atakiem.
3. Trzecia metoda, jaką może zastosować Ewa, jest wykorzystanie niedoskonałości nadajnika Alicji. W rzeczywistości, nie mamy pewności nadania tylko jednego qubitu, gdyż urządzenie nadające może wysłać kilka identycznych stanów (w tym wypadku np. koherentnych fotonów), co może spowodować, że Ewa będzie w stanie wydzielić jeden foton i go zmierzyć, nie operując na pozostałych.
4. Czego natomiast Ewa nie może zrobić, to skopiować stanu qubitu i zmierzyć kopię, gdyż tego zabrania twierdzenie o nieklonowniu.

Bezpieczeństwo kwantowej dystrybucji klucza zapewnia sama natura mikroświata, a nie jak w metodach klasycznych, np. algorytmie RSA**, przekonanie o czasochłonności pewnych operacji matematycznych.

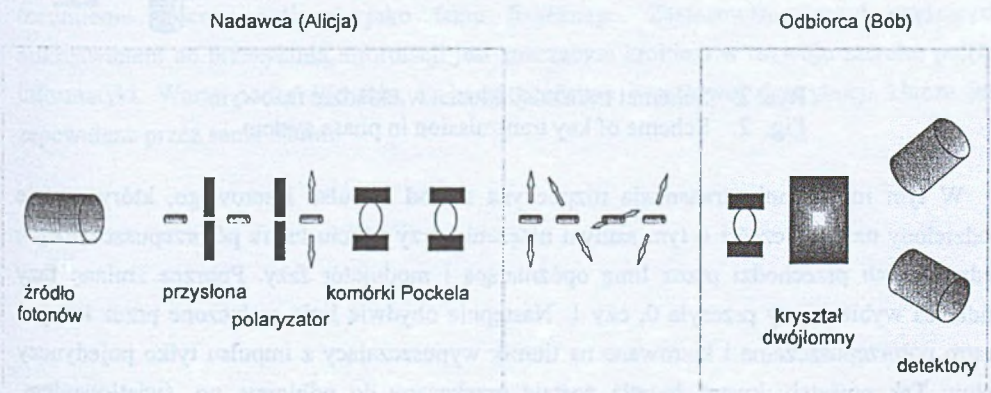
4. Realizacje

4.1. Metody kodowania klucza

Dotychczasowe eksperymenty były dokonywane z wykorzystaniem fotonów jako nośnika qubitów. Podejście to jest zrozumiałe jako że optyka kwantowa jest dobrze rozwinięta pod względem teoretycznym i zastosowań.

Istnieję dwa podejścia realizujące qubity na pojedynczych fotonach. Pierwsze z nich bazuje na polaryzacji, drugie na przesunięciu fazowym. Poniższa tabela podaje przykładowe metody kodowania stanów na wartościach własności obserwowalnych fotonu.

stan	*polaryzacja*	*przesunięcie w fazie*
$\|0\rangle$	↑	0°
$\|1\rangle$	→	45°
$\|+\rangle$	↗	90°
$\|-\rangle$	↘	135°

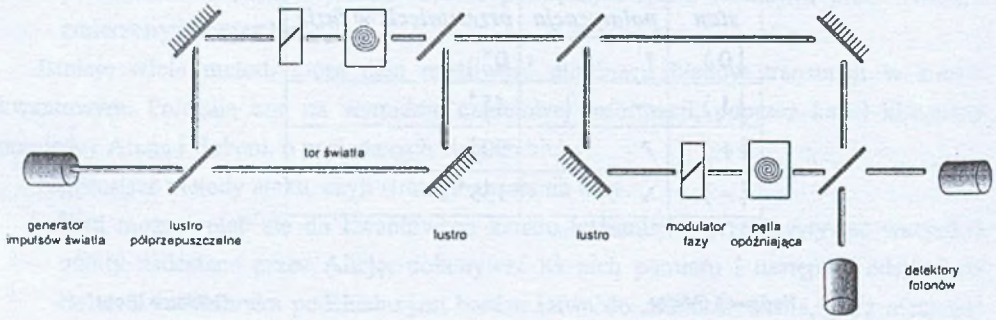


Rys. 1. Schemat transmisji klucza w układzie polaryzacyjnym
Fig. 1. Scheme of key transmission in polarisation system

**nazwa pochodzi od inicjałów nazwisk autorów: R. L. Rivesta, A. Shamira i L. M. Adlemana

W transmisji z wykorzystaniem polaryzacji nadawca rozpoczyna od wygenerowania fotonu (źródło fotonów, przysłona). W kolejnym kroku jego polaryzacja jest ustalana na pionową (polaryzator). Następnie przy użyciu komórek Pockela lub innych urządzeń do zmiany polaryzacji światła polaryzacja zostaje obrócona o 0, 45, 90 lub 135 stopni. Foton jest przekazywany do odbiorcy poprzez niezabezpieczony kanał transmisyjny (np. przy użyciu światłowodu lub w powietrzu) z zachowaniem polaryzacji. Odbiorca wybiera, czy obraca polaryzację o 45 stopni, czy nie poprzez włączanie kolejnej komórki Pockela. Dzięki temu może wybrać, w jakiej bazie dokonuje pomiaru. Następnie foton zostaje skierowany na kryształ dwójłomny (np. kalcyt), który w zależności od polaryzacji kieruje go do jednego z dwóch detektorów (najczęściej dioda lawinowa).

Wadą transmisji opartych na polaryzacji światła jest duża trudność w transmisji fotonu bez zmiany polaryzacji, co uniemożliwia stosowanie tej techniki przy większych odległościach. Wykorzystano ją podczas pierwszych doświadczalnych prób kwantowej dystrybucji klucza w laboratoriach IBM, jednak obecnie częściej zastosowanie znajduje metoda modulacji fazy [11].



Rys. 2. Schemat transmisji klucza w układzie fazowym
Fig. 2. Scheme of key transmission in phase system

W tym rozwiązaniu transmisja rozpoczyna się od impulsu laserowego, który zostaje podzielony na dwie części o tym samym natężeniu przy użyciu lustra półprzepuszczalnego. Jedna z nich przechodzi przez linię opóźniającą i modulator fazy. Poprzez zmianę fazy nadawca wybiera, czy przesyła 0, czy 1. Następnie obydwie linie są łączone przez kolejne lustro półprzepuszczalne i kierowane na tłumik wypuszczający z impulsu tylko pojedynczy foton. Tak powstały kwant światła zostaje przekazany do odbiorcy, np. światłowodem. Odbiorca rozdziela otrzymany sygnał znowu na dwie ścieżki. Na jednej z nich są umieszczone linia opóźniająca i modulator fazy, dzięki któremu odbiorca ustala, w jakiej bazie odczytuje każdy z qubitów. Na kolejnym etapie obydwie linie są łączone i kierowane do detektorów. W zależności, w którym z nich pojawi się foton, odbiorca zlicza 0 lub 1.

Zarówno przy modulacji fazy, jak i polaryzacji po przesłaniu klucza następuje uzgodnienie pomiędzy odbiorcą i nadawcą baz wykorzystanych do transmisji każdego z qubitów (krok 5 algorytmu opisanego w poprzednim rozdziale), czyli ustalenie, które bity można wykorzystać do konstrukcji klucza.

4.2. Eksperymentalne realizacje transmisji kwantowych

Pierwsze eksperymenty prezentujące zastosowanie kwantowej kryptografii wykonano na początku lat 90 ubiegłego wieku w laboratoriach IBM. Była to transmisja na dystansie 30 cm w powietrzu. Większość późniejszych doświadczeń wykonano z użyciem światłowodów jako medium transmisyjnego. W 1993 roku przeprowadzono transmisje na dystansie ponad 1 km kodując informacje przy użyciu polaryzacji fotonów [10].

Największy dystans – 67 km - został osiągnięty przez uczonych z Uniwersytetu w Genewie, wykorzystujących modulacje fazy. Do transmisji wykorzystano światłowód telekomunikacyjny pomiędzy Genewą i Lozanną i na takim dystansie osiągnięto prędkość 12,9 kbit/s. Na podstawie tych doświadczeń stworzono firmę produkującą urządzenia do kwantowej dystrybucji kluczy [9] podłączane do komputera za pomocą portu USB***.

5. Podsumowanie

Kwantowa dystrybucja jest pierwszym dość powszechnym wdrożeniem kwantowych systemów informatyki. Dziedzina ta rozwija się od około dwudziestu lat, wpływając na rozumienie procesu obliczeń jako faktu fizycznego. Zastosowanie reguł rządzących mikroświatem do przesyłania informacji jest znaczącym krokiem w rozwoju szeroko pojętej informatyki. Warto podkreślić fakt, iż bezpieczeństwo kwantowej dystrybucji klucza jest zapewniane przez samą Naturę.

***Universal Serial Bus

Literatura

1. Shor P. W.: Algorithms for quantum computation: Discrete logarithms and factoring. 1994.
2. Grover L.K.:A fast quantum mechanical algorihtm for database search. ACM Press, New York 1996. arXiv: quant-ph/9506034.
3. Nielsen M. A. Chuang I. L.: Quantum Computation and Quantum Information. Cambridge University Press, 2001.
4. Data Encryption Standard (DES), Federal Information Processing Standards Publication, 1999. FIPS PUB 46-3.
5. Preskill J. Lecture Notes for Physics 229: Quantum Information and Computation. California Istitute of Technology, 1998, http://www.theory.caltech.edu/people/preskill/ph229,
6. Ardehali M. Brasard G. Chau H. F. Lo H-K.: Eficient Quantum Key Distribution. Networked Systems Department, HP Laboratories Bristol. HPL-98-29, 1998.
7. Brassard G. Salvail L.: Secret-Key Reconciliation by Public Discussion, Lecture Notes in Computer Science, 1994. http://citeseer.nj.nec.com/brassard94secretkey.html.
8. Bennett C. H., Brassard G.: Quantum cryptography: public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175 — 179, 1984.
9. http://www.idquantique.com/qkd.html,
10. Muller A., Breguet J., Gisin N.: "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km", Europhys. Lett., 23 (6), pp. 383-388 (1993),
11. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H.: "Quantum key distribution over 67km with a plug&play system", New Journal of Physics 4 (2002).
12. Bugajski S., Klamka J., Węgrzyn S.: "Foundations of quantum computing", Part I, Archiwum Informatyki Teoretycznej i Stosowanej, tom 13, zeszyt 2, 2001, ss. 97-142.
13. Bugajski S., Klamka J., Węgrzyn S.: "Foundations of quantum computing", Part II, Archiwum Informatyki Teoretycznej i Stosowanej, tom 14, zeszyt 4, 2002, ss. 83-106.
14. Klamka J., Węgrzyn S.: "Quantum computing", Archiwum Informatyki Teoretycznej i Stosowanej, tom 12, zeszyt 3, 2000, ss. 235-246.

Recenzent: Prof. dr hab. inż. Jerzy Klamka

Wpłynęło do Redakcji 11 kwietnia 2003 r.

Abstract

In the article we present algorithm of secure cryptographical key distribution using photons and methods of quantum mechanics. In the first chapter a short introduction to quantum computing is presented. The following two chapters describe the BB84 algorithm in classical and modified form. This method allows to transmit information (usually the cryptographic key) through non-secure quantum channel with certainty, if anyone overheard it.

Bits of information are coded on one of four qubit states, from two orthogonal bases. The receiver randomly choses in which base decode each qubit. Then through classical (non-quantum) channel he tells the sender what bases he used. If both the sender and the receiver chosed the same bases the bit is assumed to be well transmitted. The possibilities of attack on such form of communication are discussed in the last paragraph of third chapter.

The physical realization of this kind of communication can be made using photons and one of two coding techniques: phase and polarization modulation. In the fourth chapter we present schemes of equipment needed to both of them. Experiments have proved that transmission can be made over long distances – up to 67km.

Adresy

Piotr GAWRON: Polska Akademia Nauk, Instytut Informatyki Teoretycznej i Stosowanej, ul. Bałtycka 5, 44-100 Gliwice, Polska, gawron@iitis.gliwice.pl .

Krzysztof GROCHLA: Polska Akademia Nauk, Instytut Informatyki Teoretycznej i Stosowanej, ul. Bałtycka 5, 44-100 Gliwice, Polska, kil@iitis.gliwice.pl .