# Kryptografia kwantowa

Przemysław Ciok

29 lipca 2002

## 1 Idea kryptografii kwantowej

Kryptografia kwantowa jest nową, wielce interesującą dziedziną kryptografii. Co ciekawe, w odróżnieniu od wielu zagadnień mechaniki kwantowej, doczekała się już praktycznej realizacji.

Kryptografia kwantowa zapewnia możliwość całkiem bezpiecznej komunikacji - to znaczy niemożliwej do podsłuchania przez osoby trzecie.

### 1.1 Przesyłanie informacji

#### 1.1.1 Podstawowe zagadnienie kryptologii

Podstawowe zagadnienie kryptologii wiąże się z przesyłaniem informacji. Alicja przekazuje informacje do Boba. Kanał jest publiczny, więc istnieje niestety możliwość podsłuchu przez osoby trzecie (Ewa). **Kryptografia** zajmuje się zapisywaniem informacji w sposob zrozumiały tylko dla odbiorcy posiadającego **klucz** tak aby osoba podsłuchująca nie była w stanie jej zrozumieć. W zależności od zastosowanego algorytmu **kodowania** istnieje jednak mniej lub bardziej realne zagrożenie złamania szyfru przez osobę podsłuchującą.

#### 1.1.2 Absolutnie bezpieczny algorytm

Istnieją algorytmy które są niemożliwe do złamania, jak chociażby szyfr Vernama (ang. *one-time pad*). Alicja koduje informację (ciąg bitów) za pomocą klucza (rownież ciąg bitów) w ten sposób, że bity na poszczególnych pozycjach dodaje modulo 2 i tak uzyskany kryptogram wysyła Bobowi. Ten z kolei może odzyskać informację, dodając modulo 2 otrzymany ciąg bitów i klucz. Jeżeli klucz jest conajmniej tak długi jak przesyłana informacja, oraz jest całkowicie przypadkowy to szyfr ten jest nie do złamania. Jedyna możliwość to odgadnięcie klucza, czyli wygenerowanie $2^n$

możliwych kluczy. Oczywiście raz użyty klucz nie może być wykorzystany ponownie. Problemem jednak pozostaje uzgodnienie klucza pomiędzy stronami. To jest prawdziwy "słaby punkt" tego algorytmu.

### 1.1.3 Inne metody

Są oczywiście inne metody, np. stosujące klucz prywatny i publiczny. Takie algorytmy opierają się jednak na idei istnienia *funkcji jednostronnych* dla których znalezienie argumentu gdy znamy wartość jest obliczeniowo trudne. Przykładowo: algorytm *RSA*, opierający się na problemie faktoryzacji liczb, przy odpowiednio duzych liczbach oraz dzisiejszej mocy obliczeniowej tradycyjnych komputerów jest praktycznie nie do złamania. Jednak w przypadku znalezienia efektywnego algorytmu faktoryzacji tych liczb szyfr taki staje się bezużyteczny. W istocie, istnieje taki algorytm (algorytm *Schora*) który wymaga zastosowania komputera kwantowego. Prace nad skonstruowaniem takiego komputera ciągle trwają, ale jest całkiem prawdopodobne że już niedługo będzie możliwe łamanie dzisiaj "bezpiecznych" szyfrów.

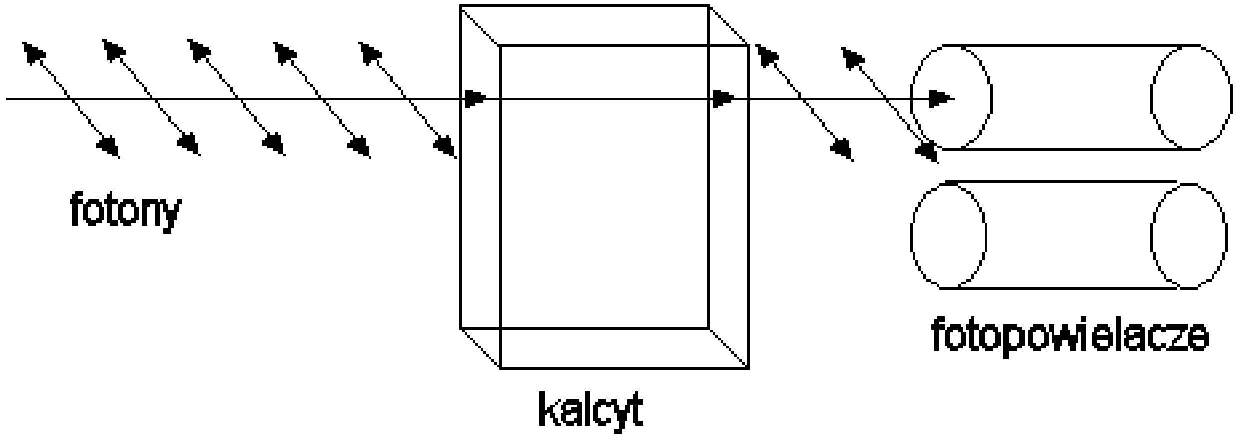
### 1.1.4 Kwantowe generowanie klucza

Znana jest jednak stuprocentowo bezpieczna metoda uzgadniania klucza. Co ciekawe, również to rozwiązanie bazuje na dokonaniach mechaniki kwantowej. W dalszej części przedstawię podstawowe pojęcia, przykładowe protokoły oraz opiszę zastosowane już implementacje.

## 1.2 Fotony, ich polaryzacja oraz jej pomiary

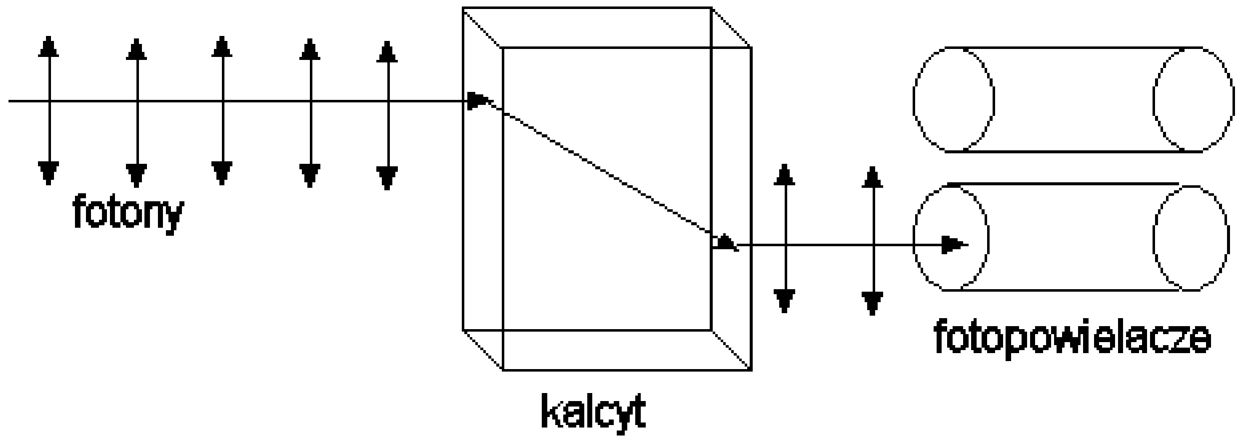
*Fotony* są to najmniejsze możliwe porcje, czyli *kwanty* swiatła. W istocie każdy foton jest falą elektromagnetyczną, w której pola elektryczne i magnetyczne drgają prostopadle do siebie i do kierunku rozchodzenia się fali. *Polaryzacja* to kierunek drgania pola elektrycznego, zwykle światlo składa się z wielu fotonow o różnych polaryzacjach. Trzeba dodać także, iż współczesna fizyka umożliwia emitowanie pojedynczych fotonów oraz nadawanie im odpowiedniej polaryzacji poprzez odpowiednie filtry. Możliwy jest także pomiar polaryzacji nadchodzących fotonow za pomocą specjalnego analizatora. Przykładowo, kryształ mający wlasciwość *dwójłomności*, np. kryształ kalcytu nadaje światłu jeden z dwóch współczynników załamania, w zależności od polaryzacji nadchodzących fotonów. To, czy foton ulegnie odchyleniu, czy też nie, mozna oczywiście rejestrować poprzez fotopowielacze zmieniające światło w impuls elektryczny. Tak więc możliwe jest używanie fotonów przy przesyłaniu informacji (wysyłanie i odbieranie).

### 1.2.1 Polaryzacja pozioma




Rysunek 1: polaryzacja pozioma

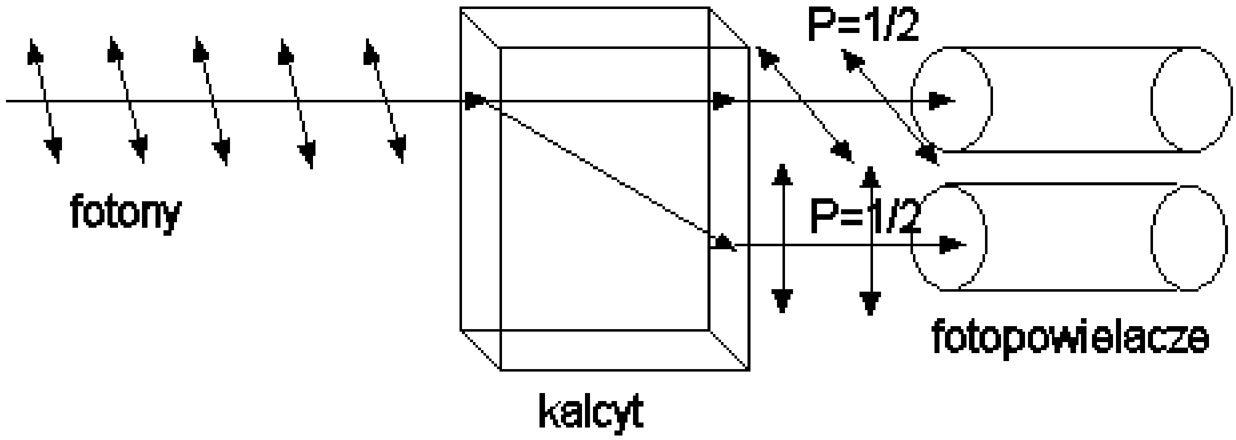
Poziomo (0°) spolaryzowane fotony przechodzą przez kryształ kalcytu bez zmiany kierunku propagacji. Zostaną więc wychwycone w górnym fotopowielaczu.




Rysunek 2: polaryzacja pionowa

### 1.2.2 Polaryzacja pionowa

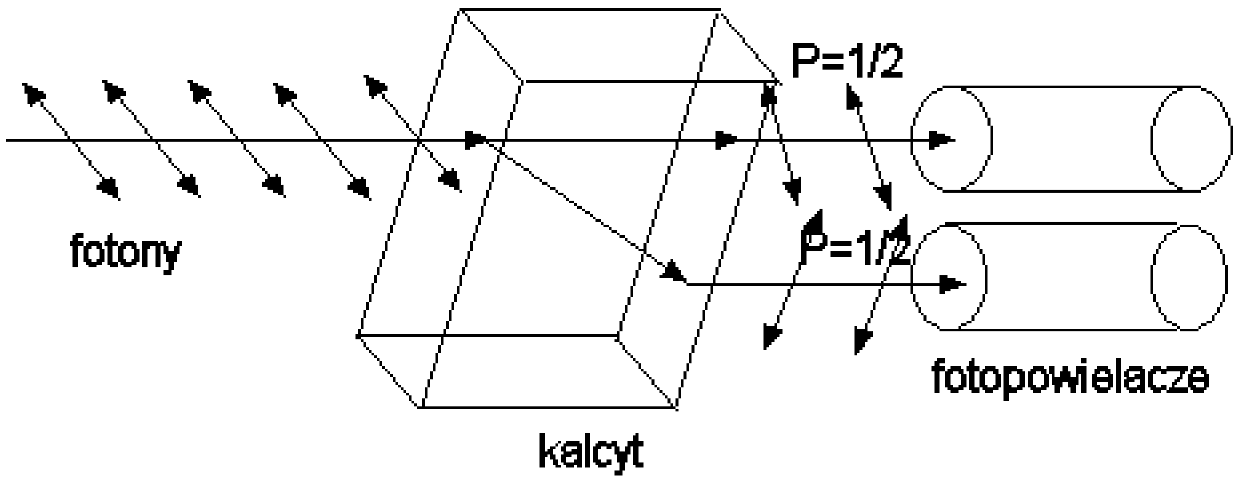
Pionowo (90°) spolaryzowane fotony będą natomiast odchylane przy przechodzeniu przez kryształ. W wyniku tego zostaną utrwalone w dolnym fotopowielaczu.




Rysunek 3: polaryzacja ukośna

### 1.2.3 Polaryzacja ukośna

Co się stanie w przypadku polaryzacji ukośnej? Otóż fotony rozdzielą się na dwie wiązki. Zajmijmy się pojedynczym fotonem. Zgodnie z prawami mechaniki kwantowej, trafi on do górnego fotopowielacza z prawdopodobieństwem równym $cos^2\alpha$ gdzie $\alpha$ jest kątem polaryzacji względem kierunku poziomego, a do dolnego z prawdopodobieństwem $1-\cos^2\alpha$ czyli $\sin^2\alpha$. Szczególnie interesujący jest przypadek gdy foton spolaryzowany jest pod kątem $45°$ lub $135°$, wtedy prawdopodobieństwa te sa równe i wynoszą $1/2$. Przy polaryzacji $45°$ średnio połowa fotonów trafi do każdego z fotopowielaczy. W przypadku pojedynczego fotonu na podstawie informacji o tym, który fotopowielacz go zarejestrował, nie możemy więc w żadnym stopniu określić czy cząstka ta była spolaryzowana pod kątem $45°$ czy może $135°$ , obie te sytuacje są jednakowo prawdopodobne.




Rysunek 4: obrót krysztalu o 45°

### 1.2.4 Sytuacja po obróceniu kryształu

Co się stanie natomiast gdy obrócony (o 45°) zostanie kryształ kalcytu? Wtedy przy przechodzniu przez niego to fotony spolaryzowane pod kątem 45° lub 135° nie zmienią swojej polaryzacji aczkolwiek fotony spolaryzowane pod kątem 45° zostaną odchylone i trafią do dolnego powielacza. Natomiast fotony spolaryzowane pod katem 90° i 0° (ta sytuacja została przedstawiona na rysunku nr. 4) będą trafiać do każdego z fotopowielaczy z prawdopodobieństwem równym 1/2. Oznacza to że przy tak ustawionym krysztale kalcytu, jeżeli wiemy że foton został spolaryzowany na jeden z dwóch sposobów: pionowo bądź poziomo, to obie te możliwości są jednakowo prawdopodobne niezależnie od tego który fotopowielacz zarejestruje nadchodzący foton.

#### 1.2.5 Niewspółmierzalność bazy prostej i ukośnej

"Standardowe" ustawienie kryształu (gdy możemy rejestrować kierunki polaryzacji 0° oraz 90°) tworzy tzw. **bazę prostą**. Pomiary w tej bazie nie dają żadnej informacji o polaryzacji ukośnej (45° lub 135°) w stosunku do osi kryształu. Można natomiast rejestrować je w tzw. **bazie ukośnej** (która odpowiada kryształowi obróconemu o 45°). W takiej bazie z kolei nie możemy odczytać żadnej informacji o polaryzacji prostej (0° bądź 90°). Polaryzacja prosta i polaryzacja ukośna są więc **niewspółmierzalne**. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy do czynienia z **zasadą nieoznaczoności Heisenberga**, ten interesujący aspekt mechaniki kwantowej został wykorzystany do konstrukcji algorytmów umożliwiających stuprocentowo bezpieczne przekazywanie klucza.

# 2 Protokoły kryptografii kwantowej

Przestawię teraz przykładowe protokoły kryptografii kwantowej

## 2.1 BB84

Protokół ten został zaproponowany przez Benett'a i Brassard'a w roku 1984. Opiera się na pomiarze polaryzacji przychodzących fotonów w ortogonalnych bazach, zastosowanie mają opisane wcześniej dwie bazy: prosta oraz ukośna.

### 2.1.1 Alfabety kwantowe

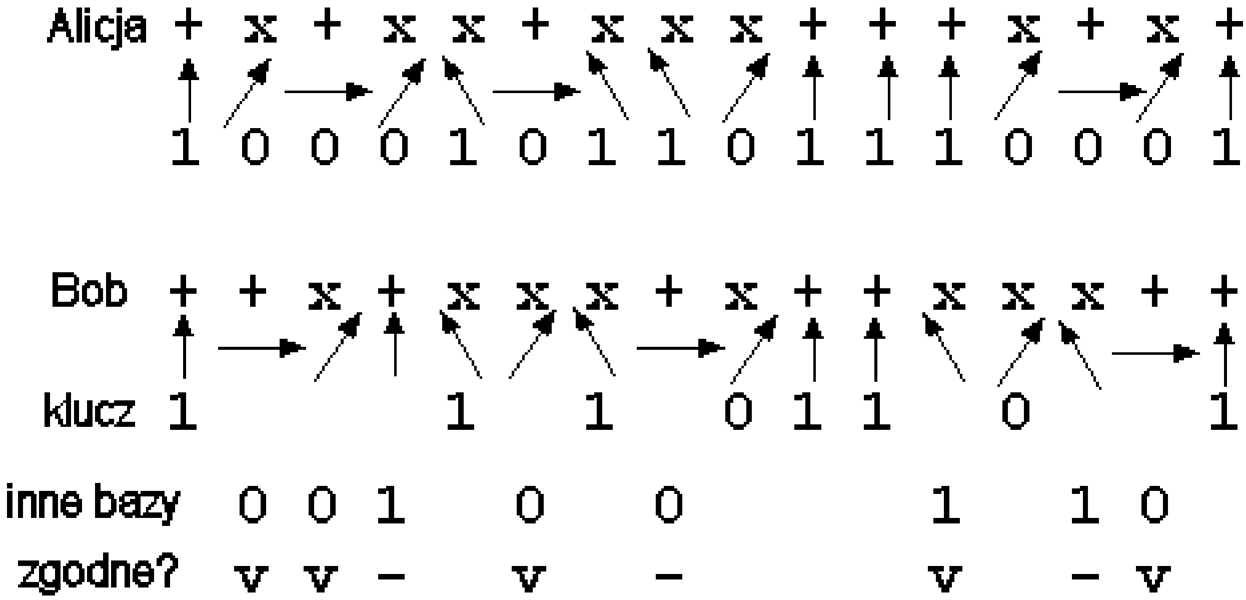
Mając dwie bazy, możemy stworzyć dwa alfabety, dla bazy prostej kątowi 0° czyli poziomej polaryzacji odpowiada 0, natomiast pionowej czyli kątowi 90° - bit 1. W bazie ukośnej natomiast polaryzacji pod kątem 45° odpowiada bit 0, a 135° - 1.

### 2.1.2 Opis protokołu

1. Alicja wybiera losowo jedną z dwóch baz, a następnie jedną z dwóch ortogonalnych polaryzacji w wybranej bazie i wysyła do Boba foton o takiej polaryzacji. Zgodnie z przyjętymi założeniami dotyczącymi alfabetów, wysyłane fotony odpowiadają ciągowi bitów.

2. Bob wybiera losowo bazę prosta lub ukośną i wykonuje pomiar polaryzacji fotonu.

3. Bob, za pomocą publicznego kanalu, informuje Alicję jakiej bazy używał, zaś Alicja informuje go czy była to baza właściwa czy też nie.




Rysunek 5: przesyłanie klucza z uzyciem BB84

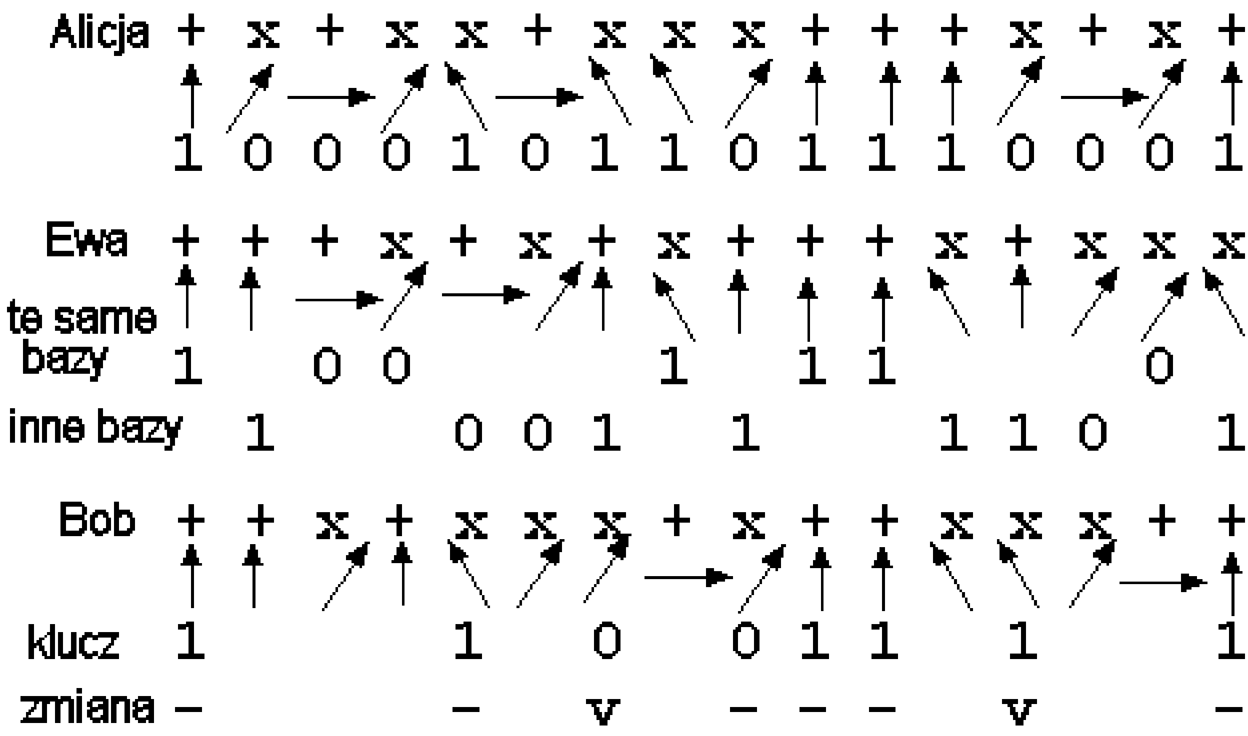
4. Alicja i Bob przechowują wyniki, dla których Bob użył właściwej bazy. Przypisując tym wynikom wartości 0 i 1 (zgodnie z przyjetymi alfabetami) oboje otrzymaja taki sam ciąg zer i jedynek. Jest to losowy ciąg który może slużyć jako klucz kryptograficzny.

### 2.1.3 Przykład

Na rysunku nr. 6 zaznaczone są użyte przy wysyłaniu i pomiarach bazy (+ - baza prosta, x - baza ukośna) oraz polaryzacje fotonów. Po przesłaniu całej wiązki, Alicja ogłasza publicznie, jakie bazy zostały wykorzystane przy wysyłaniu poszczególnych fotonów. W przypadku fotonów, dla których Bob używał tej samej bazy, wiadomo że bity są pewne (polaryzacja musi się zgadzac) i mogą posłużyć jako klucz kryptograficzny. W przypadku niezgodności baz, Bolek moze otrzymać jeden z dwóch możliwych wyników pomiaru z prawdopodobieństwem 1/2. Część otrzymanych bitów będzie więc przekłamana (średnio połowa, na rysunku zacznaczone poprzez -), dlatego oczywiście pomiary przy różniących się bazach nie są brane pod uwagę.

### 2.1.4 Obecność osoby podsłuchujacej

Co się natomiast stanie, gdy ktoś bedzie chciał podsłuchać transmisję? Ewa musi się za każdym razem zdecydować na jedną z dwóch baz, wybierając ją losowo. Musi




Rysunek 6: obecność osoby podsłuchujacej

jednak przesłać foton dalej, używając wybranej przez siebie bazy. Jeżeli jest ona zgodna z bazą wybraną przez Alicję, nic się nie dzieje. Jednak jeżeli Ewa wybrała inną bazę, Bob może z prawdopodobieństwem 1/2 otrzymać jedną z dwóch możliwych polaryzacji. Czyli średnio w połowie przypadków uzyska inną wartość niż ta, która była wysłana przez Alicję. Można więc wykryć obecność podsłuchującego - wystarczy wybrać losowo pewną liczbę bitów klucza i publicznie porównać ich wartości. Średnio 25% będzie się różniło (na rysunku bity zaznaczone przez v), o ile rzeczywiście ktoś podsłuchuje przekaz. Wtedy należy rozpocząc od nowa całą procedurę uzgadniania klucza. Mechanika kwantowa nie dopuszcza możliwości **pasywnego**, czyli nie wpływającego na stan układu, podsłuchu. Retransmisja musi wprowadzić przekłamania. Prawa fizyki gwarantują więc bezpieczeństwo tego algorytmu! Podsłuch musi być **aktywny** co gwarantuje jego wykrycie.

## 2.2 B92

Protokół B92 został zaproponowany przez Bennett'a w roku 1992. Również opiera się na pomiarze polaryzacji przychodzących fotonów, ale tym razem każda ze stron posługuje się dwoma nieortogonalnymi stanami kwantowymi.

### 2.2.1 Alfabet kwantowy

Alicja wysyła fotony o dwóch możliwych polaryzacjach: $0°$ , bądź $45°$ przypisując im odpowiednio wartości binarne 0 i 1.

### 2.2.2 Opis protokołu

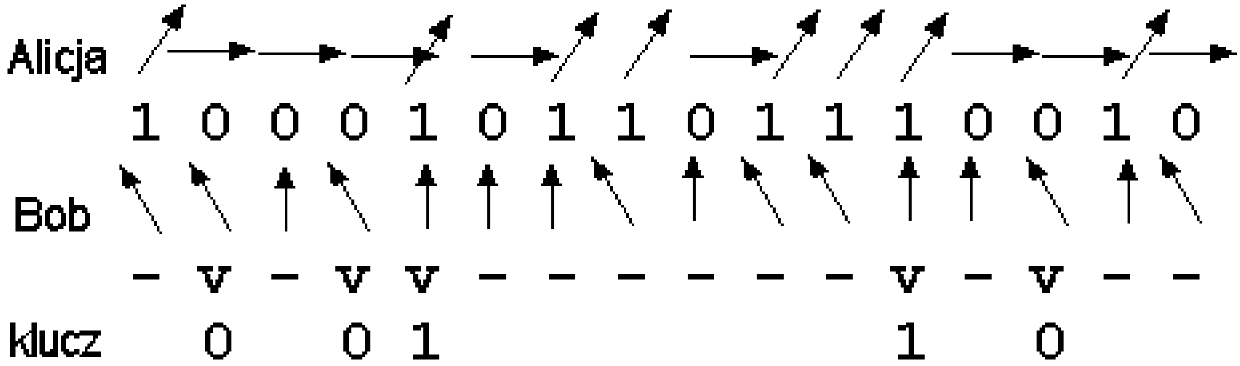
1. Alicja wybiera losowo jedną z dwóch polaryzacji i przesyła do Boba foton tak spolaryzowany. Zgodnie z przyjętym alfabetem oznacza to ciąg zer i jedynek.
2. Bob wybiera jeden ze stanów: $90°$ lub $135°$ i mierzy polaryzację w takim stanie. Jeżeli wybierze polaryzację ortogonalną do wybranej przez Alicję, to nie zarejestruje fotonu. W drugim przypadku zarejestruje foton z prawdopodobieństwem 1/2. W przypadku zarejestrowania fotonu o polaryzacji $90°$ przypisuje mu wartość binarną 1, a jeżeli będzie on spolaryzowany pod kątem $135°$ , to 0. Bob uzyska więc bit o wartości przypisanej mu przez Alicję.
3. Bob, za pomocą publicznego kanału, informuje Alicję dla których bitów zarejestrował foton (oczywiście nie zdradza publicznie, jaką polaryzację zmierzył).
4. Alicja i Bob przechowują bity na tych pozycjach, dla których Bob zarejestrował foton. Jest to losowy ciąg, który może być zastosowany jako klucz kryptograficzny.

### 2.2.3 Przykład

Na rysunku nr. 7 zaznaczone są zastosowane przez Alicję przy wysyłaniu polaryzacje fotonów, oraz pozycje dla których Bob zarejestrował foton (miał na to szanse z prawdopodobieństwem 1/2, o ile nie zastosował przy mierzeniu stanu ortogonalnego z polaryzacją wysłanego przez Alicję fotonu).

### 2.2.4 Obecność osoby podsłuchującej

Obecność Ewy, a więc osoby podsłuchujacej jest łatwa do wykrycia . Ewa losowo wybiera jeden z dwóch stanów, potem przy retransmisji powstają jednak przekłamania. Porównanie wartości dla pewnej wybranej liczby bitów wykaże więc różnicę średnio w 25% przypadków. możliwość wykrycia podsłuchu oznacza ze algorytm ten jest bezpieczny i uzgodniony ciąg może zostać wykorzystany jako klucz kryptograficzny.




Rysunek 7: przesyłanie klucza z użyciem BB84

### 2.3 Ekert, EPR

Protokół zaproponowany w 1991 roku przez Ekerta opiera się na zjawisku EPR (*Einstein-Podolsky-Rosen*). Generowana jest sekwencja par cząstek związanych nierownością Bella (są to tak zwane pary EPR). Bob i Alicja badają polaryzację tych cząstek. Próba odczytania ich przez Ewę i ponownego wysłania powoduje przekłamania przy pomiarze (możliwe naruszenie korelacji układu) i umożliwia wykrycie tego przez zainteresowane strony. Jeżeli transmisja nie zostanie podsłuchana, Alicja i Bob będą w stanie na podstawie swoich pomiarów określić klucz.

### 2.4 Inne protokoły

Istnieje wiele różnych protokołów kryptografii kwantowej. Do kodowania może być np. używana faza fotonu, a nie jego polaryzacja. Ciągle powstają nowe protokoły kryptografii kwantowej.

## 3 Kryptografia kwantowa w praktyce

### 3.1 Kryptografia kwantowa: Początki

Pierwsze prototypowe urządzenia realizujące protokół *Benetta i Brassarda* ujrzały światło dzienne na przełomie lat 80 i 90tych XX wieku. Zostały one skonstruowane przez naukowców z laboratorium IBM, firmy która bardzo intensywnie zajmuje się zagadnieniami mechaniki kwantowej. Parametry transmisji nie były może imponujące: odległość 32cm, 10 bitów/sek, ale liczył się głównie sam fakt implementacji dotychczas pozostającego w sferze teoretycznej protokołu.

## 3.2 Kryptografia kwantowa: Teraźniejszość

Obecnie jest możliwe przesyłanie fotonów, za pomocą swiatłowodów, na odległości do kilkudziesięciu kilometrów. Prace i udane eksperymenty są prowadzone przez naukowców w specjalnych laboratoriach m.in. w Genewie (maksymalna uzyskana odległość: 23 km) czy Los Alamos (48 km). Możliwe jest także przesyłanie fotonów bezpośrednio w powietrzu, udało się nawiązać zaszyfrpwane połączenie na odległość nawet 10 kilometrow (jeszcze niedawno, dwa lata temu, udawało się to osiągnąc jedynie na odległośc 1,6 km).

## 3.3 Kryptografia kwantowa: Przyszłość

Jeżeli chodzi o przesyłanie fotonów bezpośrednio w powietrzu, uwzględniając rozrzedzenie powietrza na dużych wysokościach, możliwe powinno być nawet przekazywanie zaszyfrowanych kwantowo informacji do satelitów znajdujących się na niskiej orbicie okołoziemskiej. Za pomocą światłowodów także nie będzie możliwe przesyłanie fotonów na zbyt duże odległości. Maksymalna odległość szacowana jest na około 100 km, przy dzisiaj znanych rozwiązaniach technologicznych. Przesłanie fotonów na dluższym dystansie wymagałoby już zastosowania przekaźników, a więc retransmisji co prowadziłoby do przekłamań. Można oczywiście wyobrazić sobie zastosowania dla których jest to odłegość wystarczająca, np. komunikacja między oddziałami banku w obrębie jednej aglomeracji, bądź też agencjami rządowymi. Plotka głosi nawet, iż w Stanach Zjednoczonych istnieje już połączenie kwantowe pomiędzy Białym Domem a Pentagonem.