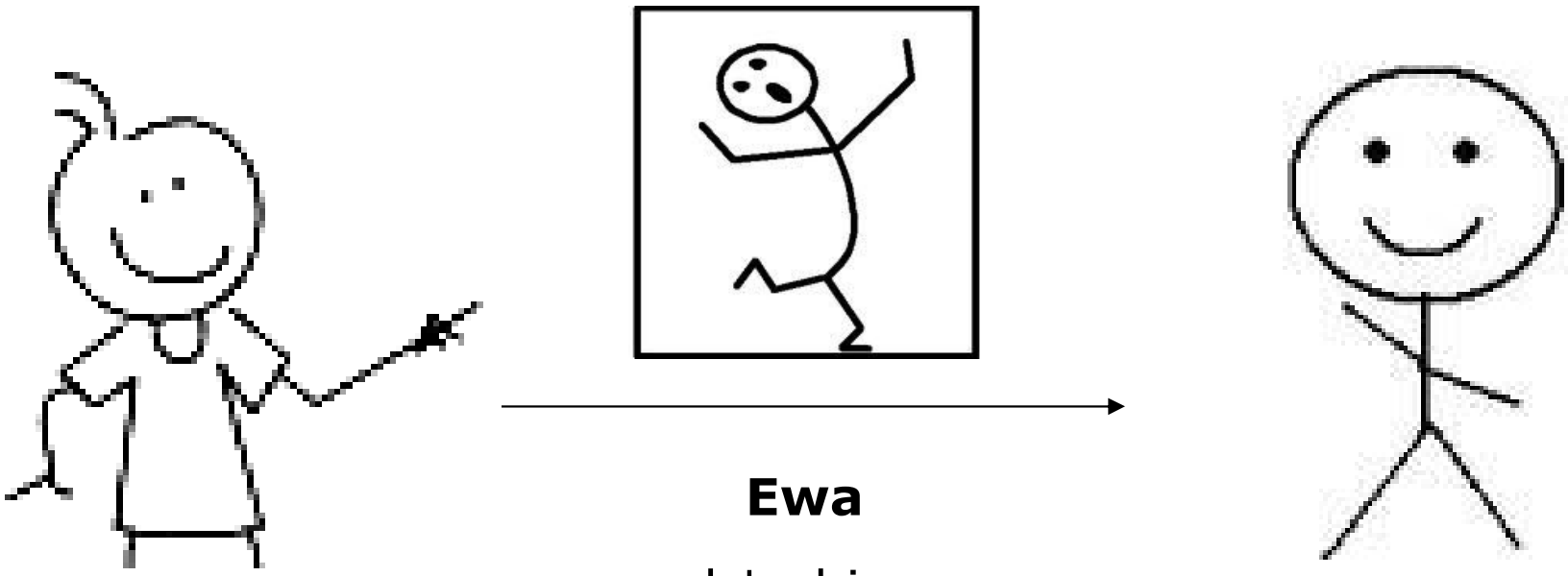
Kryptografia kwantowa

Marta Michalska

Główne postacie



Ewa

podsłuchiwacz

Alicja

nadawca informacji

Bob

odbiorca informacji

Alicja przesyła do Boba informacje kanałem, który jest narażony na podsłuch. Ewa usiłuje przechwycić informację przeznaczoną dla Boba.

Szyfrowanie

Wiadomość	1	0	1	0	0	1	1	0	1	0
Klucz	1	1	0	1	0	1	0	0	1	0
Alicja	0	1	1	1	0	0	1	0	0	0

Bob	0	1	1	1	0	0	1	0	0	0
Klucz	1	1	0	1	0	1	0	0	1	0
Wiadomość	1	0	1	0	0	1	1	0	1	0

Klucz szyfrujący powinien być:

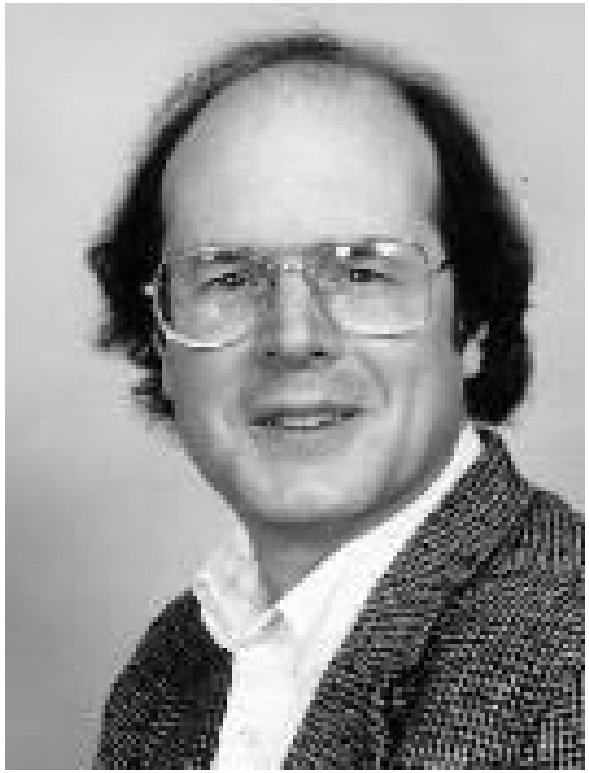
- Tak samo długi jak szyfrowana wiadomość;
- Użyty tylko raz;
- Znany wyłącznie uprawnionym osobom;
- Losowy.

Jak wygenerować taki klucz?

Kryptografia kwantowa

Jest to nowa dziedzina leżąca na pograniczu informatyki i mechaniki kwantowej zajmująca się możliwościami wykorzystania układów kwantowych do przetwarzania i przesyłania informacji.

Kryptografia kwantowa



Charles H. Bennett

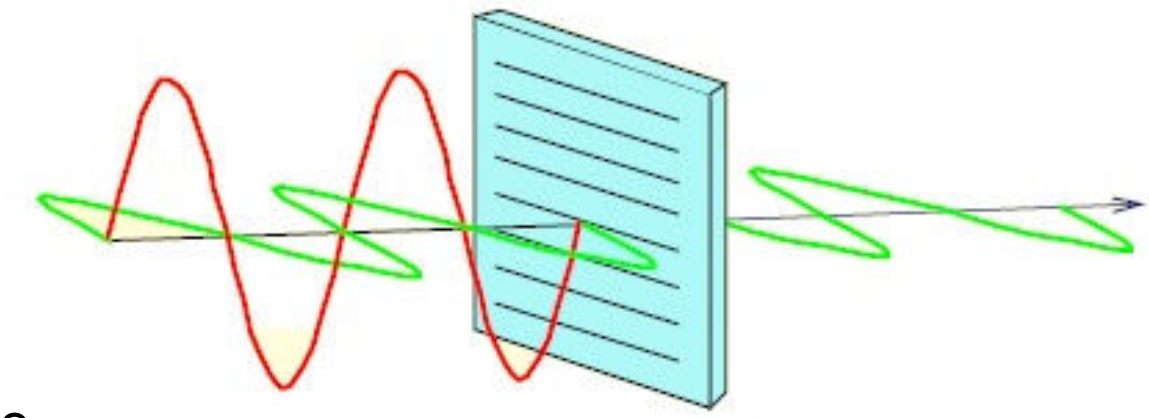
Gilles Brassard

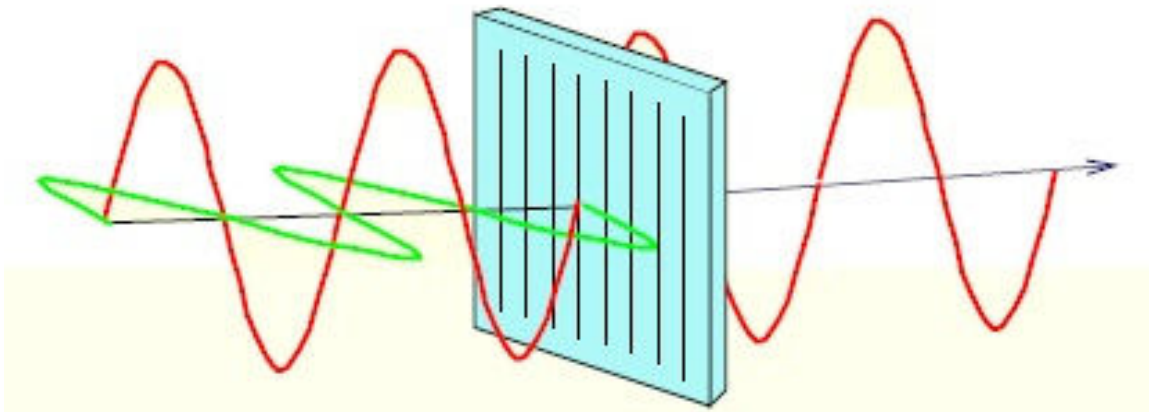
„Kryptografia kwantowa” jest chwytliwą frazą, ale nieco niedokładną.

Nie wiadomość jest szyfrowana za pomocą fizyki kwantowej, lecz raczej fizyka kwantowa gwarantuje nam bezpieczną transmisję klucza (QKD).

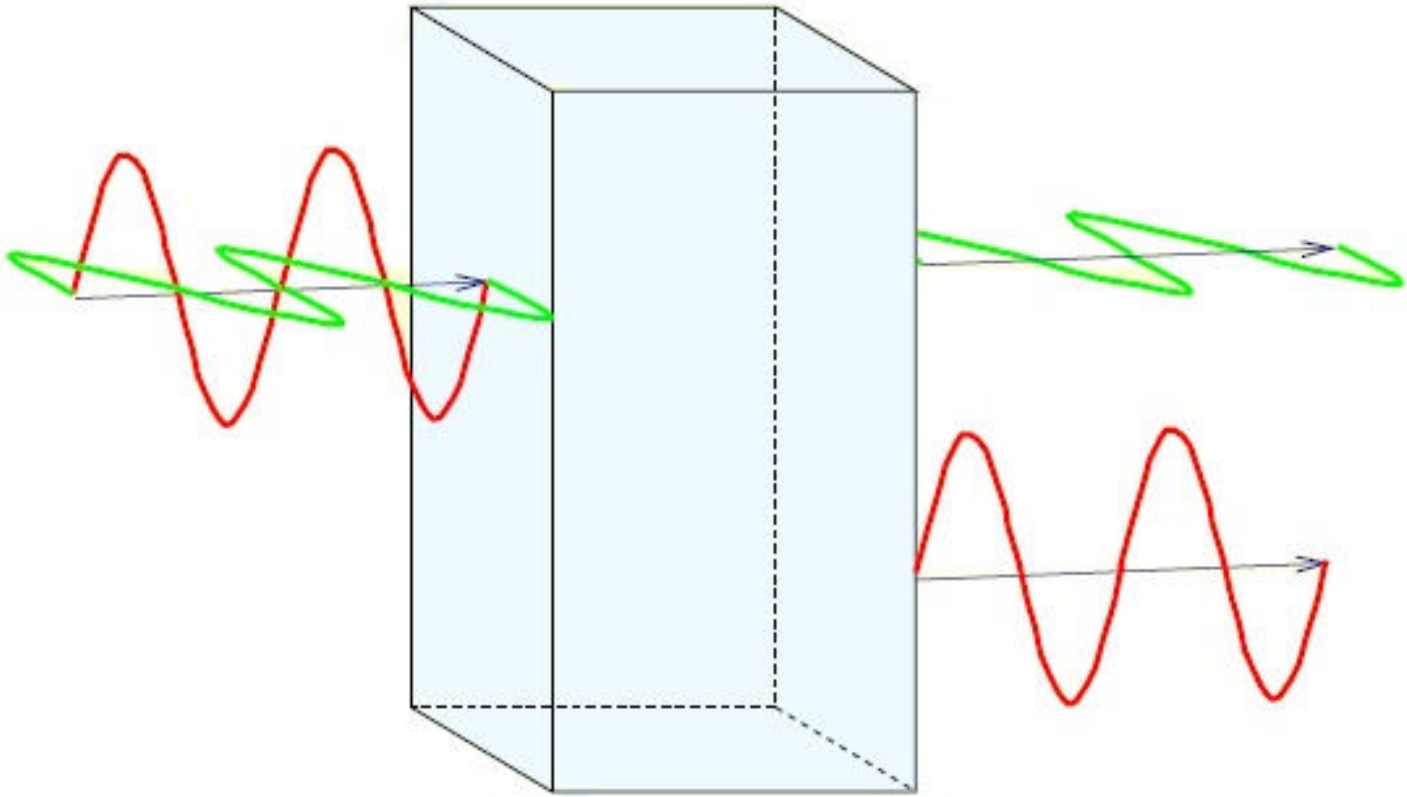
Polaryzacja światła

Polaryzator przepuszcza światło o określonej polaryzacji.



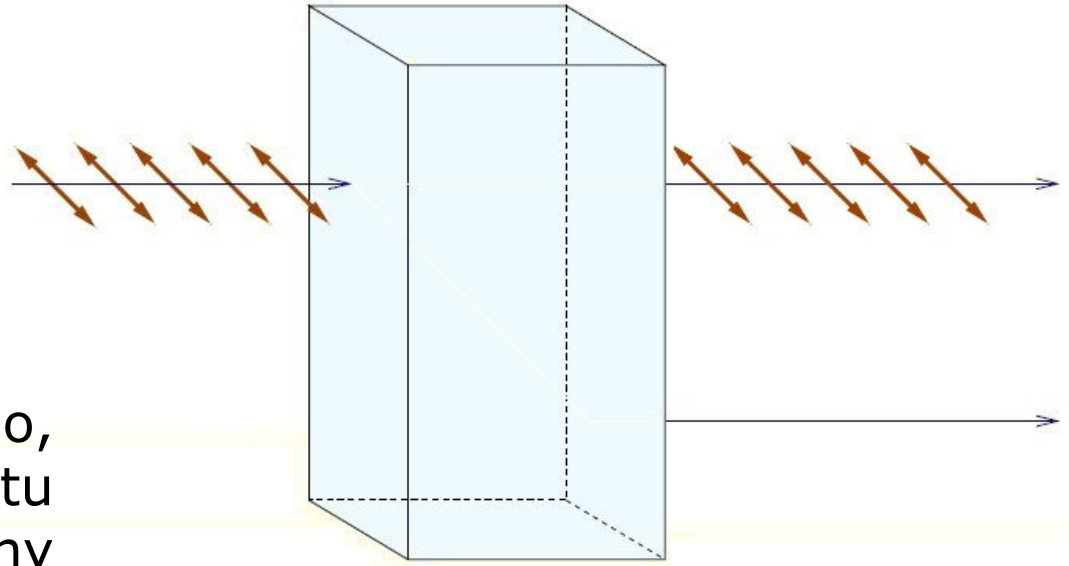


Polaryzacja światła

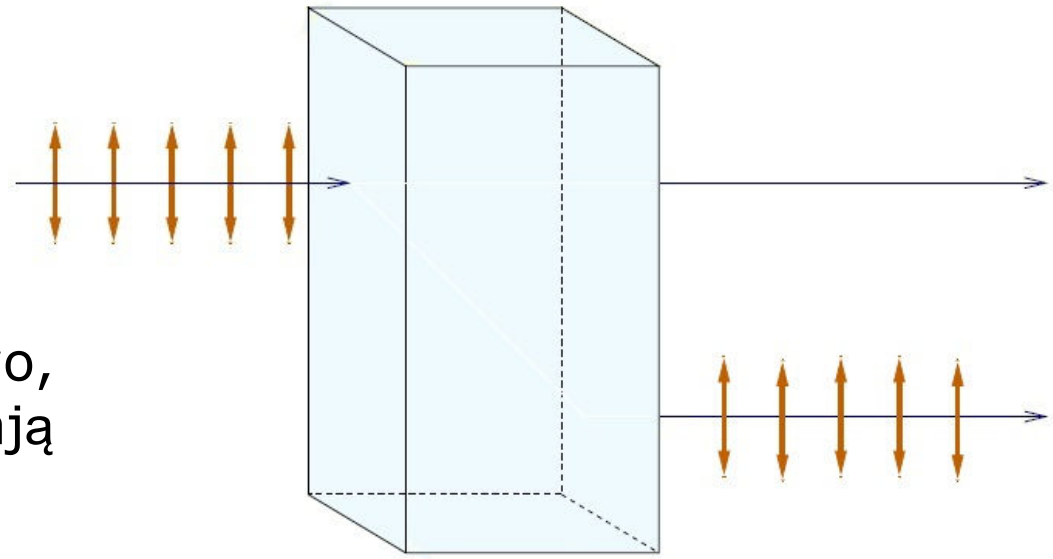


Dwójłomny kryształ kalcytu rozdziela falę świetlną na dwie składowe o wzajemnie prostopadłych polaryzacjach (promień zwyczajny i nadzwyczajny).

Polaryzacja światła

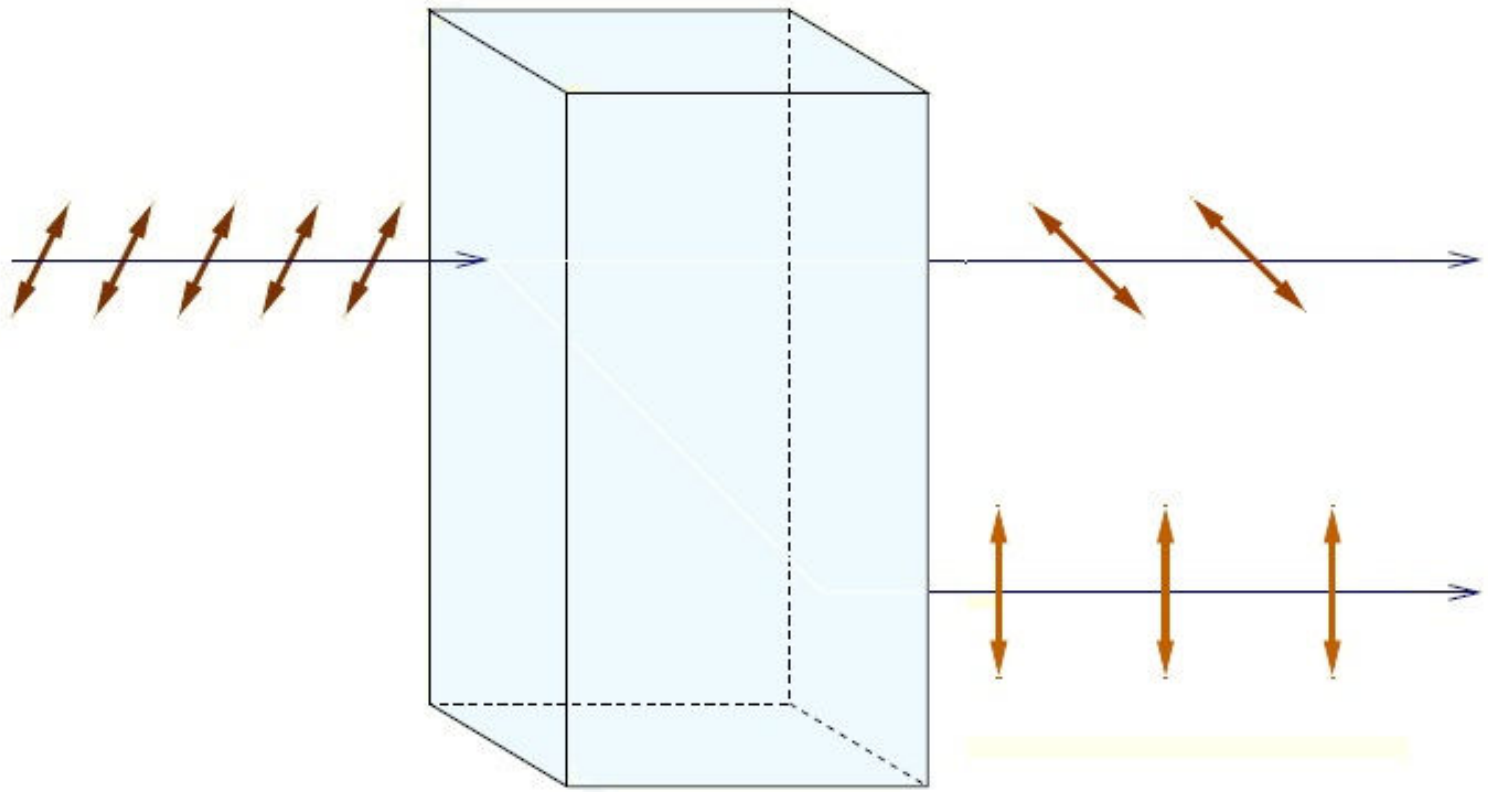


Fotony spolaryzowane poziomo, padające na kryształ kalcytu przechodzą przez niego bez zmiany kierunku – promień zwyczajny.



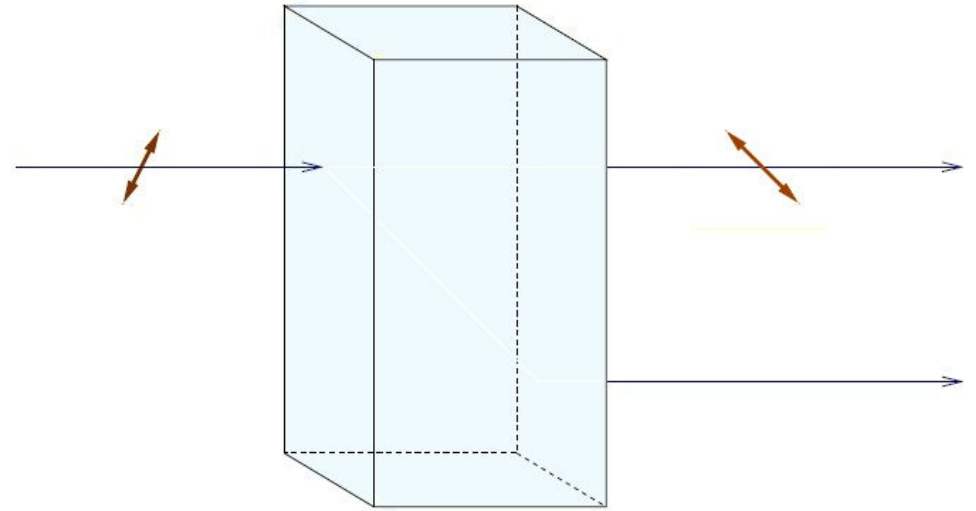
Fotony spolaryzowane pionowo, padające na kryształ kalcytu zostają odchylone – promień nadzwyczajny.

Polaryzacja światła



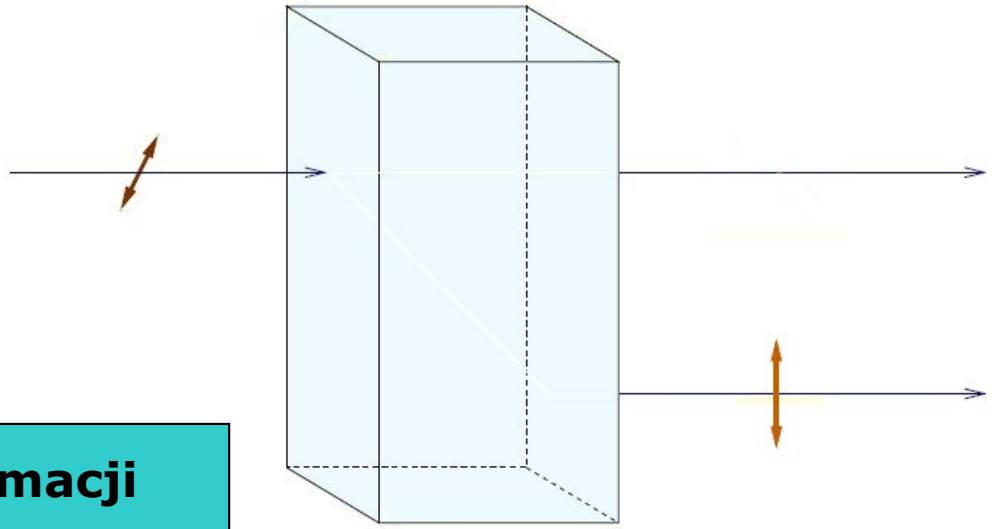
Fotony spolaryzowane ukośnie, padające na kryształ kalcytu, w sposób losowy otrzymują polaryzację poziomą lub pionową i odpowiedni kierunek propagacji.

Polaryzacja światła



Pojedynczy foton o polaryzacji ukośnej:

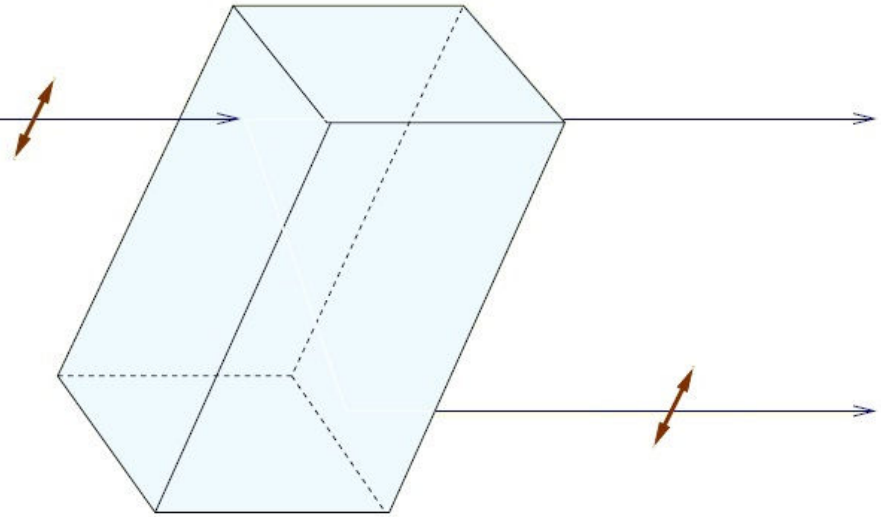
- z prawdopodobieństwem ½ znajdzie się w wiązce zwyczajnej z polaryzacją poziomą;
- z prawdopodobieństwem ½ znajdzie się w wiązce nadzwyczajnej z polaryzacją pionową.



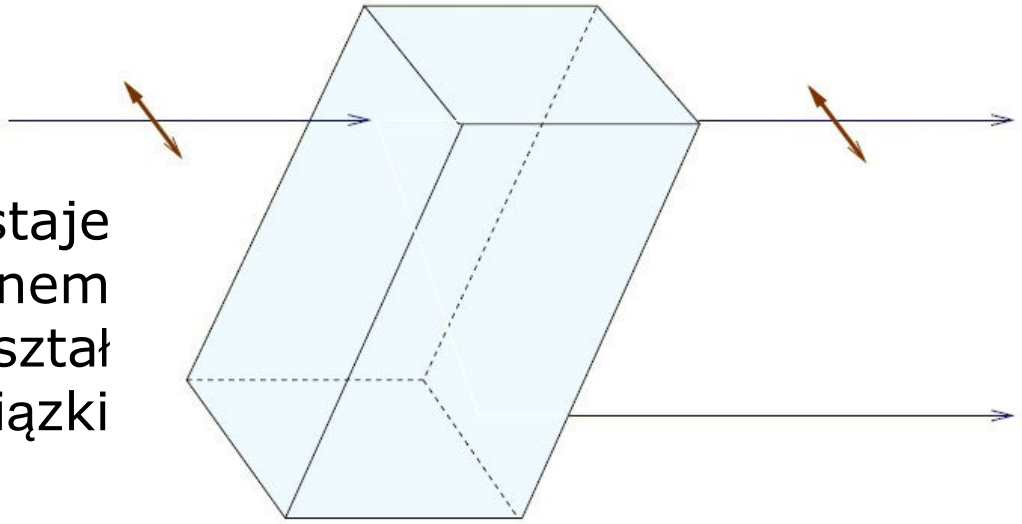
Foton nie niesie już żadnej informacji o poprzedniej polaryzacji.

Polaryzacja światła

Obracamy teraz kryształ o -45°.

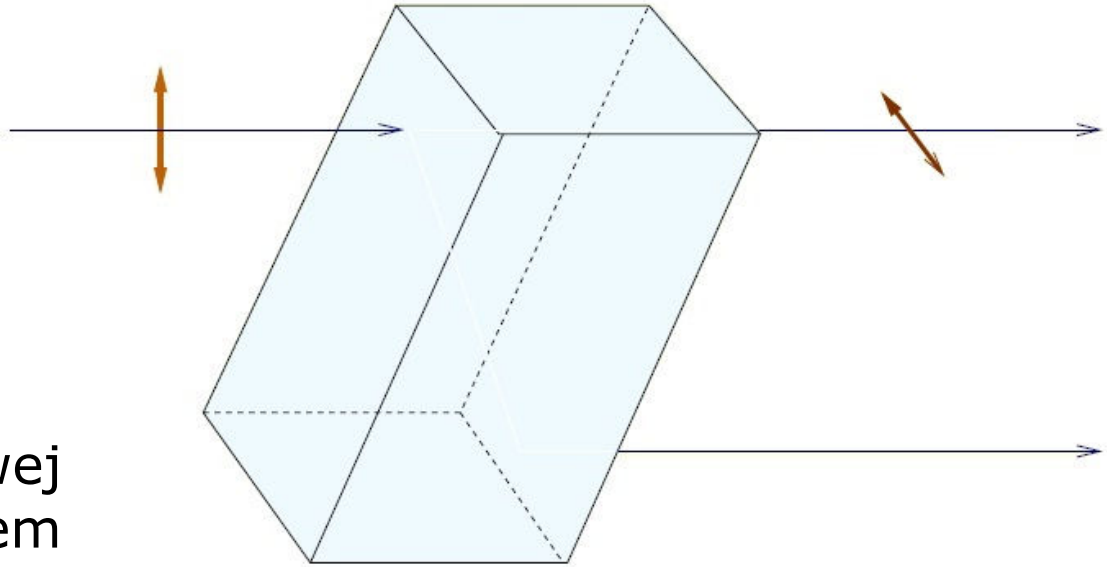


Foton o polaryzacji ukośnej -45° staje się w nowym układzie fotonem pionowym i przechodzi przez kryształ bez zmiany polaryzacji do wiązki nadzwyczajnej.

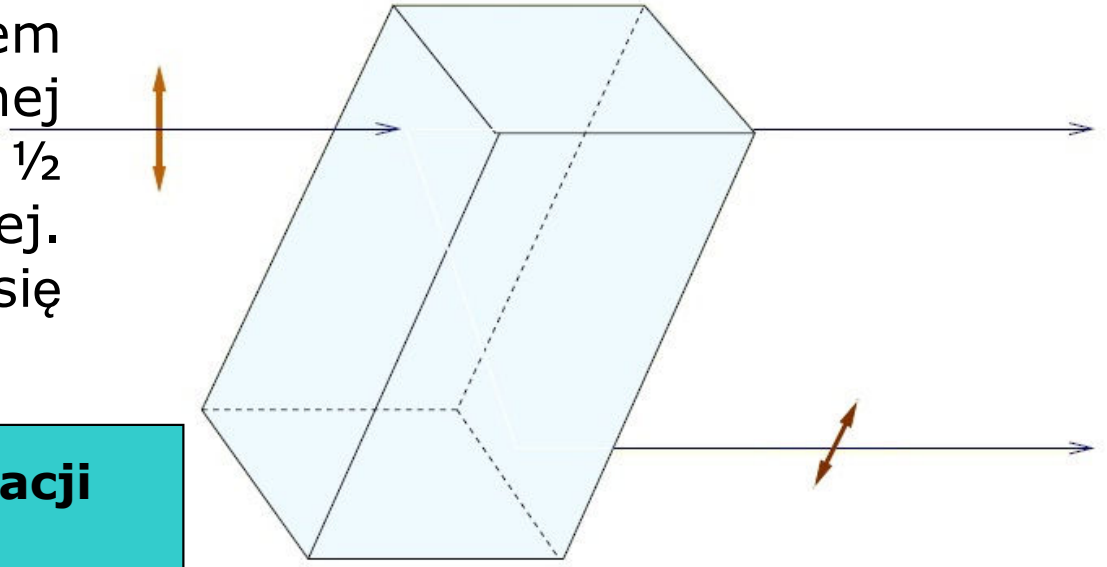


Foton o polaryzacji ukośnej 45° staje się w nowym układzie fotonem poziomym i przechodzi przez kryształ bez zmiany polaryzacji do wiązki zwyczajnej.

Polaryzacja światła

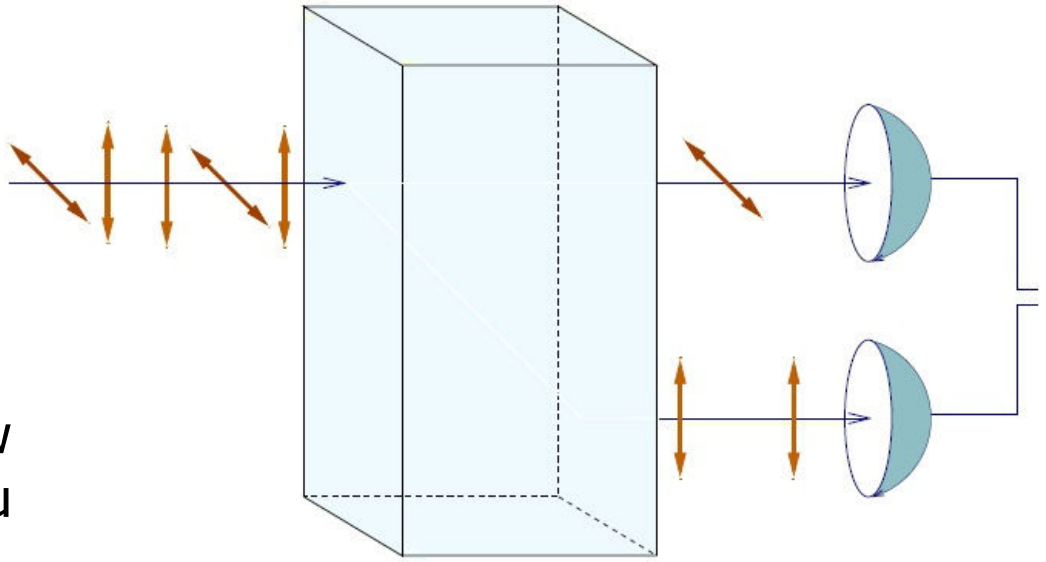


Foton o polaryzacji pionowej (poziomej) staje się fotonem ukośnym w stosunku do obróconego kryształu i z prawdopodobieństwem ½ przechodzi do wiązki zwyczajnej lub z prawdopodobieństwem ½ przechodzi do wiązki nadzwyczajnej. W obydwu przypadkach zmienia się jego polaryzacja.



Foton nie niesie już żadnej informacji o poprzedniej polaryzacji.

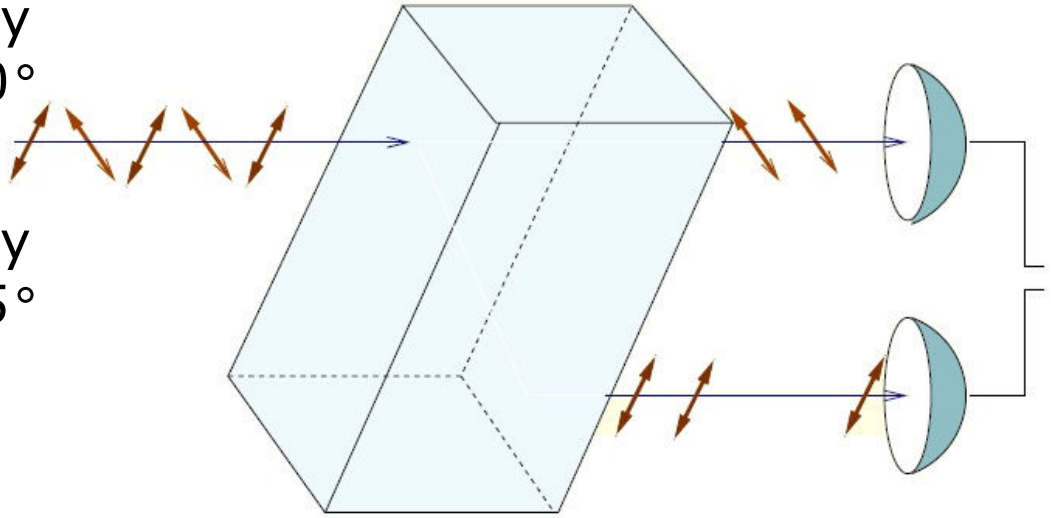
Polaryzacja światła



Dodając dwa detektory fotonów otrzymujemy przyrząd do pomiaru polaryzacji.

W bazie prostej w sposób pewny mierzymy polaryzację fotonów 0° i 90°.

W bazie ukośnej w sposób pewny mierzymy polaryzację fotonów -45° i 45°.



Zasada nieoznaczoności Heisenberga

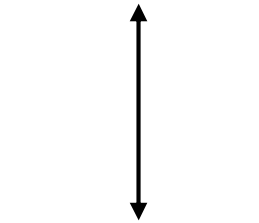
- Pomiary w bazie prostej nie dają żadnych informacji o polaryzacji ukośnej.
- Pomiary w bazie ukośnej nie dają z kolei żadnych informacji o polaryzacji prostej.
- Polaryzacja prosta i ukośna są dwiema wielkościami fizycznymi, które nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną.

Protokoły kwantowe

- Protokół Bennetta i Brassarda (BB84)
- Protokół Bennetta (B92)
- Protokół Ekerta

Alfabety kwantowe

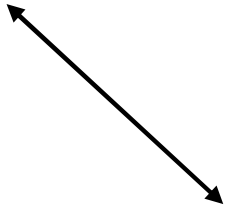
Alfabet prosty



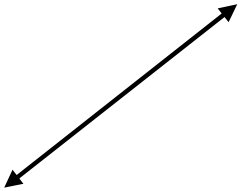
=1

=0

Alfabet ukośny



=1



=0

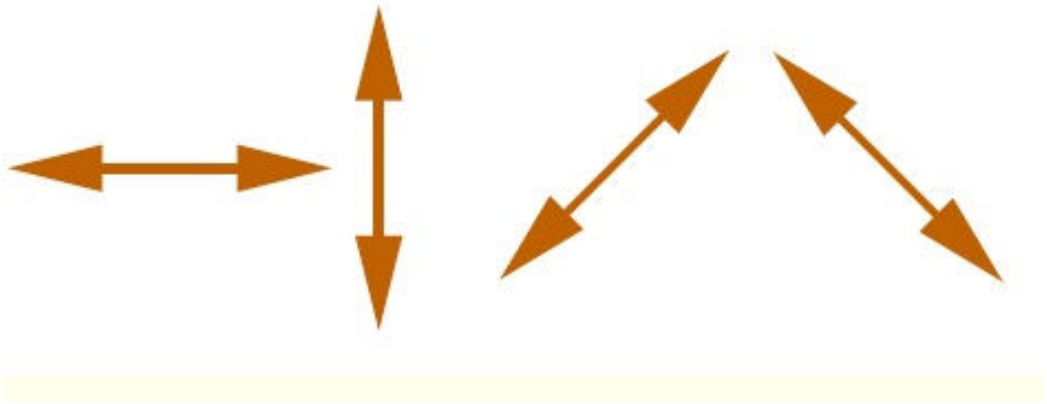
Mamy dwa różne alfabety kwantowe: prosty i ukośny. Dwie wzajemnie prostopadłe polaryzacje stanowią znaki alfabetu, którym przypisujemy wartości binarne 0 lub 1. Kodujemy w ten sposób informację, którą chcemy przesłać kanałem kwantowym.

Protokół BB84

Krok 1

Alicja wybiera w sposób losowy jedną z czterech możliwych polaryzacji i wysyła do Boba foton o takiej polaryzacji.

Ciąg fotonów stanowi ciąg 0 i 1 z dwóch alfabetów kwantowych.

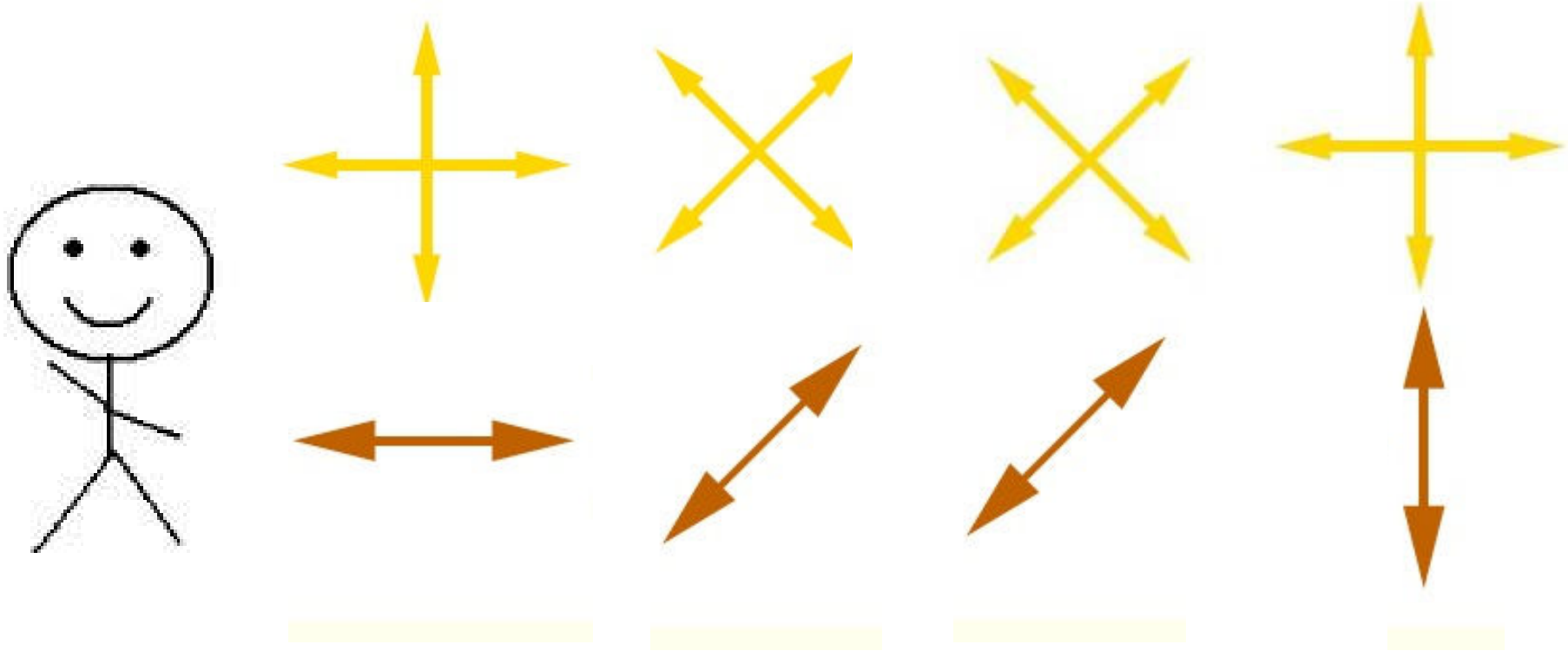


Protokół BB84

Krok 2

Bob również w sposób losowy wybiera jedną z baz: prostą lub ukośną i dokonuje w niej pomiaru polaryzacji fotonu, który dostał od Alicji.

Bob notuje wyniki pomiarów zachowując je w tajemnicy.

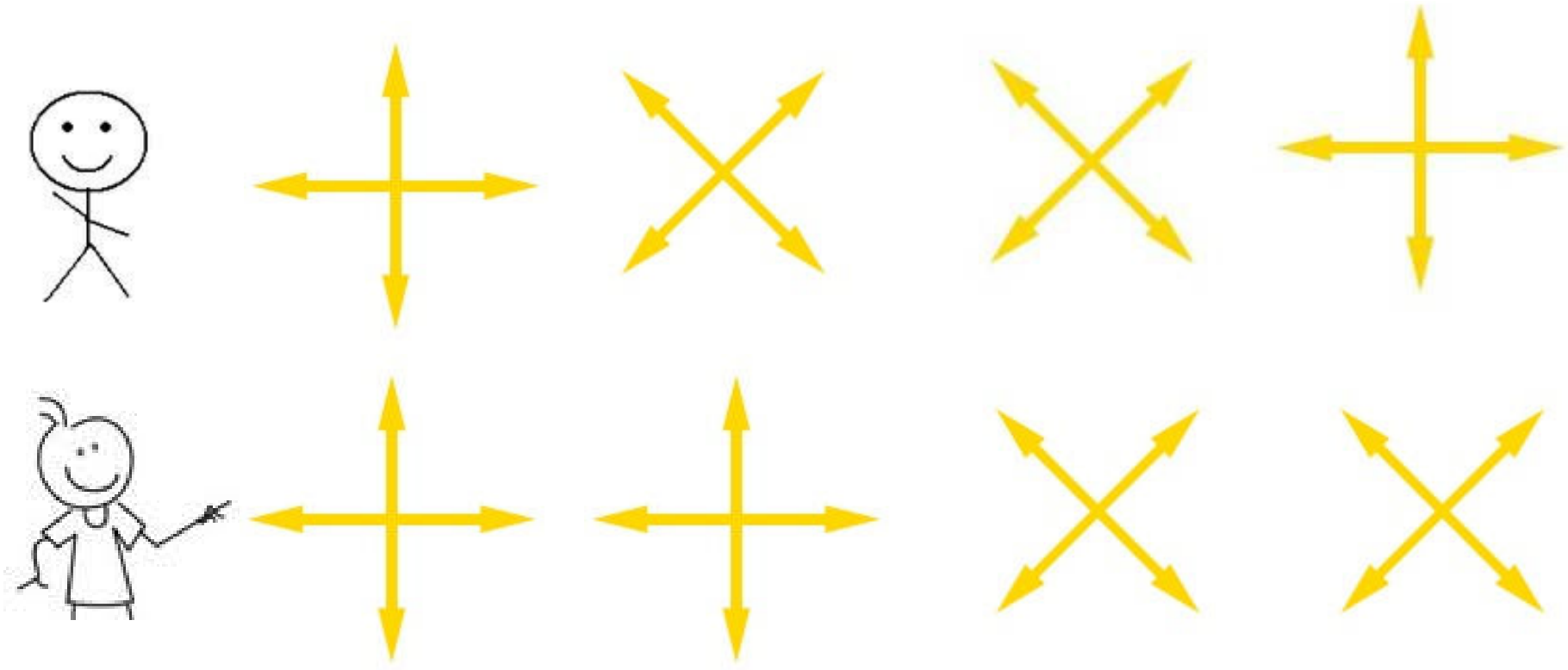


Protokół BB84

Krok 3

Bob publicznie informuje Alicję jakiej bazy użył do wykonania każdego z pomiarów. Nie podaje jakie otrzymał wyniki.

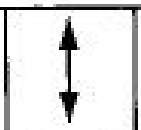
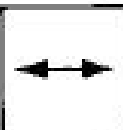
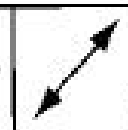
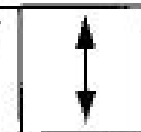
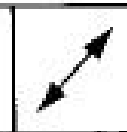
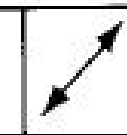
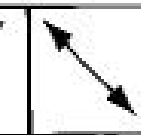
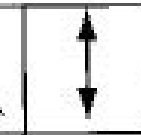
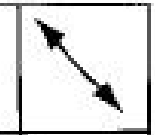
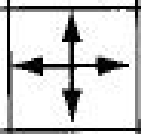
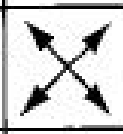
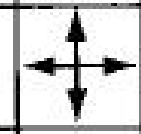
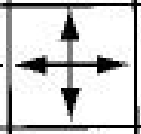
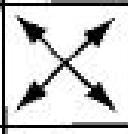
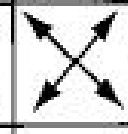
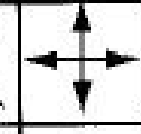
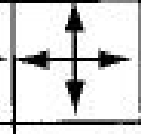
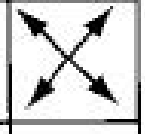
Alicja informuje, również publicznie, Boba czy dokonany przez niego wybór bazy był słuszny czy nie.



Protokół BB84

Krok 4

Alicja i Bob przechowują wyniki pomiarów, dla których Bob użył właściwej bazy. Wyniki tych pomiarów zapisują w postaci binarnej.

Alice's polarizers									
sequence of bits	1	0	0	1	0	0	1	1	1
Bob's analyzers									
Bob's measurements	1	1	0	1	0	0	1	1	1
retained bits	1	–	–	1	0	0	–	1	1

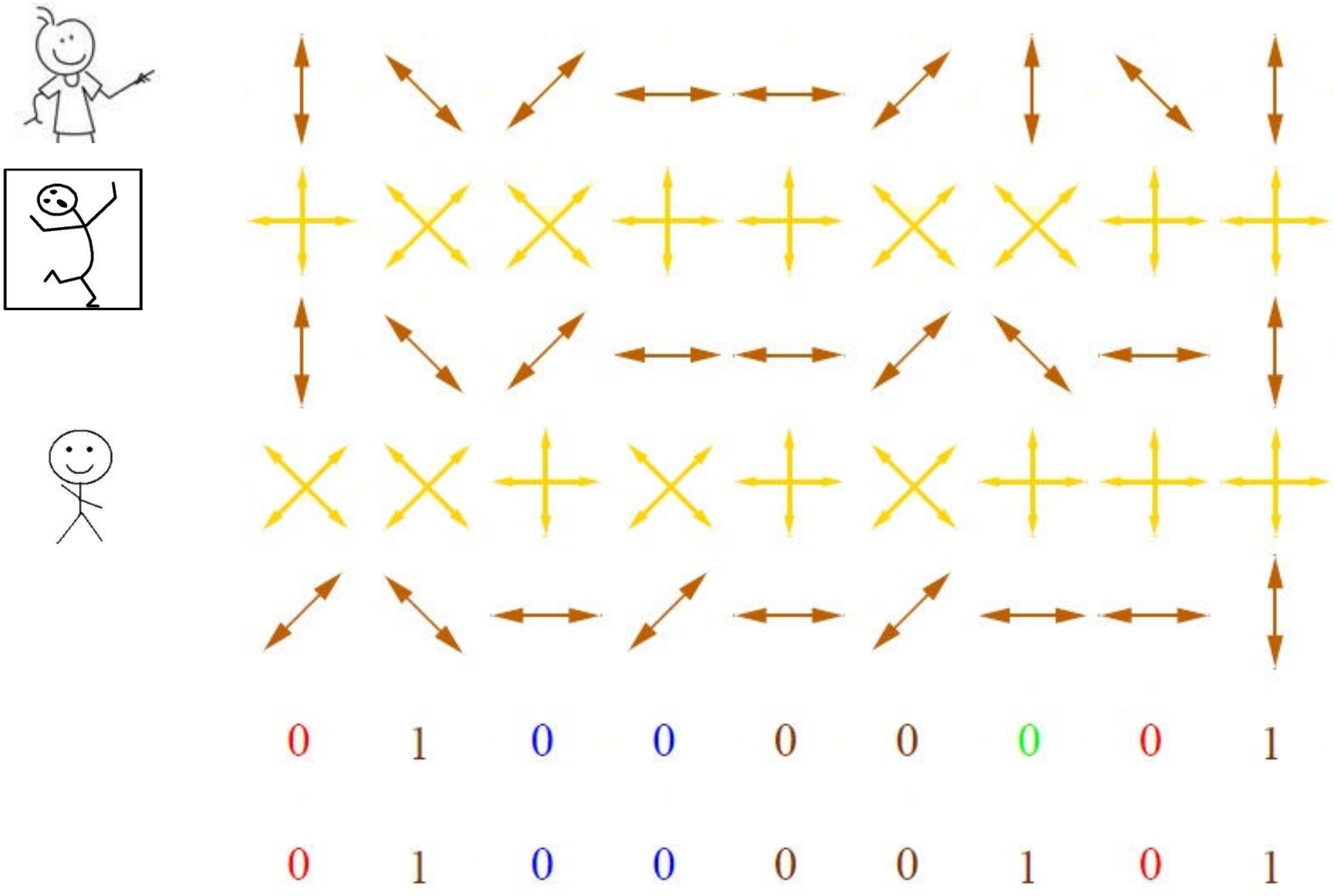
Ewa podsłuchuje

Protokół BB84

- Ewa podsłuchuje dokonując pomiaru polaryzacji fotonu wysłanego przez Alicję w losowo wybranej bazie.
- Po zarejestrowaniu polaryzacji wysyła foton o takiej samej polaryzacji do Boba.
- Ewa zmienia niektóre bity – wprowadza błędy w przekazie.

Ewa podsłuchuje

Protokół BB84



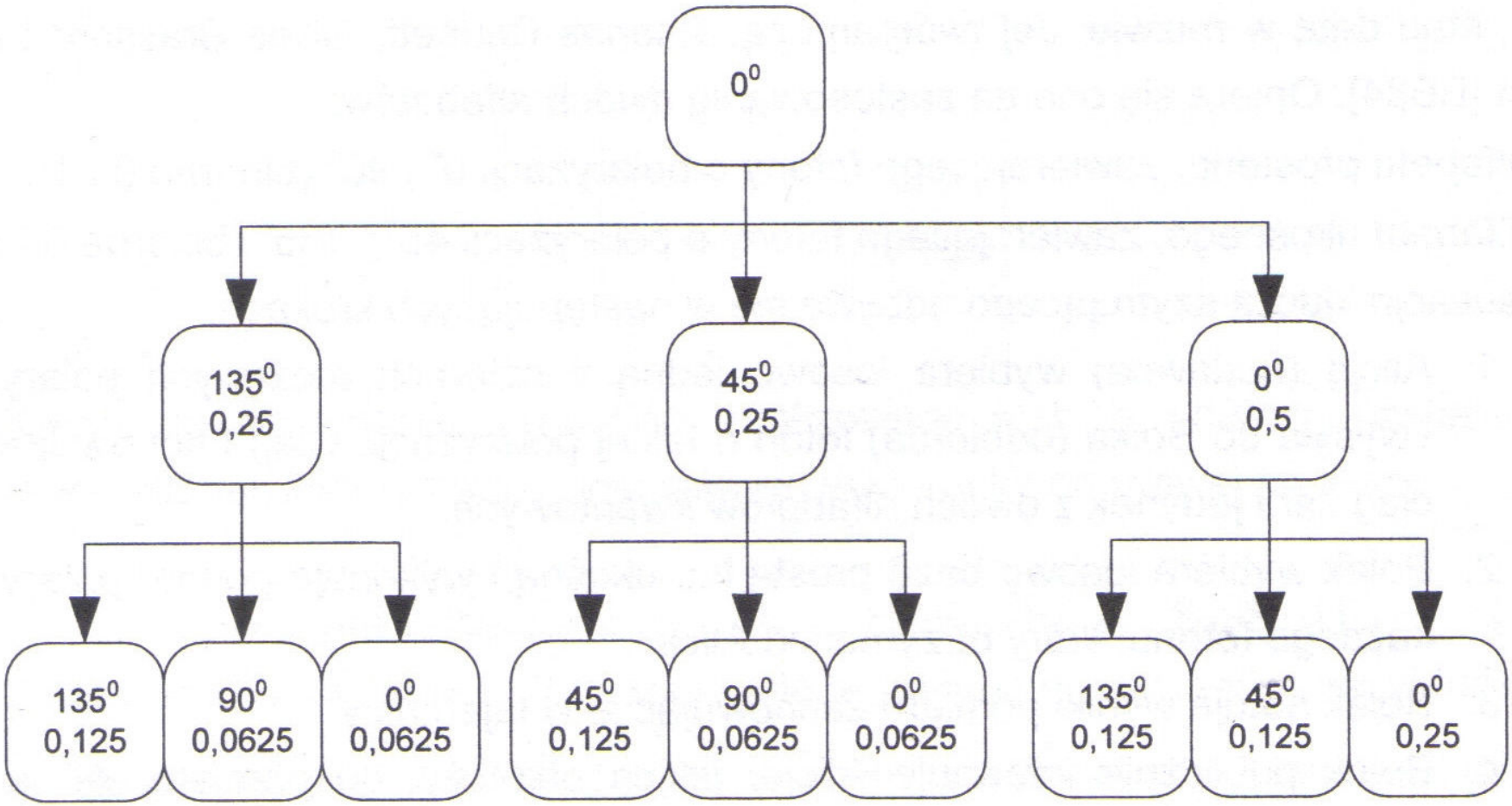
Ewa podsłuchuje

Protokół BB84

- Alicja i Bob mogą wykryć obecność Ewy porównując losowo wybraną część bitów z uzgodnionego już klucza (bity te następnie usuwają).
- Jeżeli okaże się, że bity zostały zmienione, to Ewa podsłuchiwała.
- Wtedy uzgadnianie klucza zaczyna się od nowa.

Ewa podsłuchuje

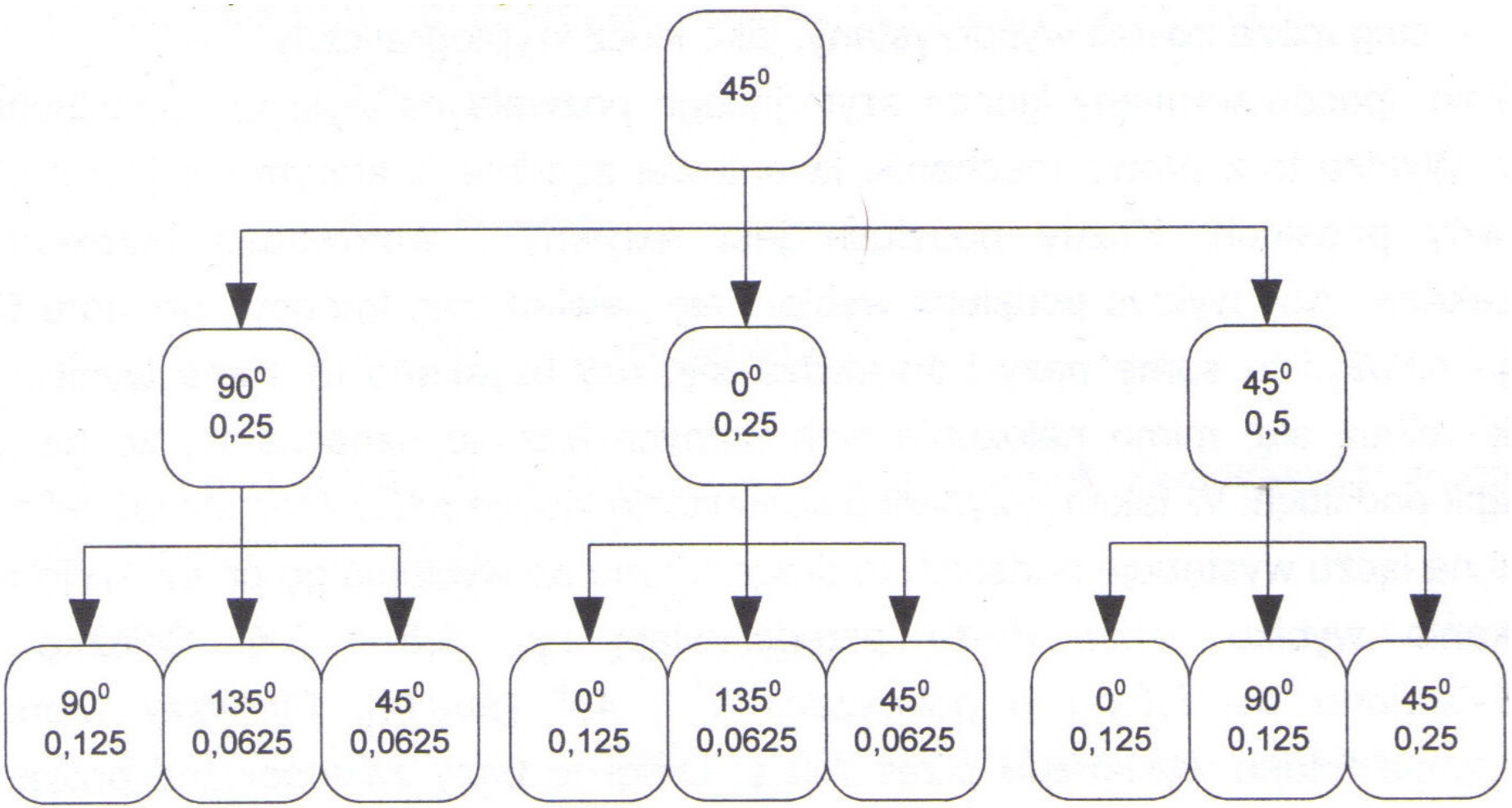
Protokół BB84



Możliwe ścieżki fotonu o polaryzacji prostej od nadawcy do adresata przy założeniu, że występuje podsłuch.

Ewa podsłuchuje

Protokół BB84



Możliwe ścieżki fotonu o polaryzacji ukośnej od nadawcy do adresata przy założeniu, że występuje podsłuch.

Ewa podsłuchuje

Protokół BB84

- Na poziomie kwantowym nie ma możliwości pasywnego podsłuchu – każdy podsłuch zaburza przekaz.
- Prawa mechaniki kwantowej gwarantują bezpieczeństwo przy uzgadnianiu klucza kryptograficznego.

Protokół B92

- Opiera się na dwóch nieortogonalnych stanach kwantowych.
- Można przyjąć, że dwa takie stany to fotony o polaryzacji 0° (0) i 45° (1).
- Fotony o takich polaryzacjach generuje Alicja. Bob odczytuje ich polaryzację w stanach ortogonalnych do 0° i 45°, czyli 90° i 135°.

Protokół B92

Etapy:

- Alicja wybiera losowo jedną z dwóch polaryzacji 0° lub 45° i foton o takiej polaryzacji wysyła do Boba.

- Bob wybiera losowo bazę prostą lub ukośną i dokonuje odczytu polaryzacji fotonów. Jeżeli wybrana baza jest prawidłowa (ukośna dla fotonu 0° - może uzyskać bit 0 lub prosta dla fotonu 45° - może uzyskać bit 1), to otrzyma wynik z prawdopodobieństwem ½. Jeżeli wybrana baza jest nieprawidłowa nie uzyska wyniku.

Protokół B92

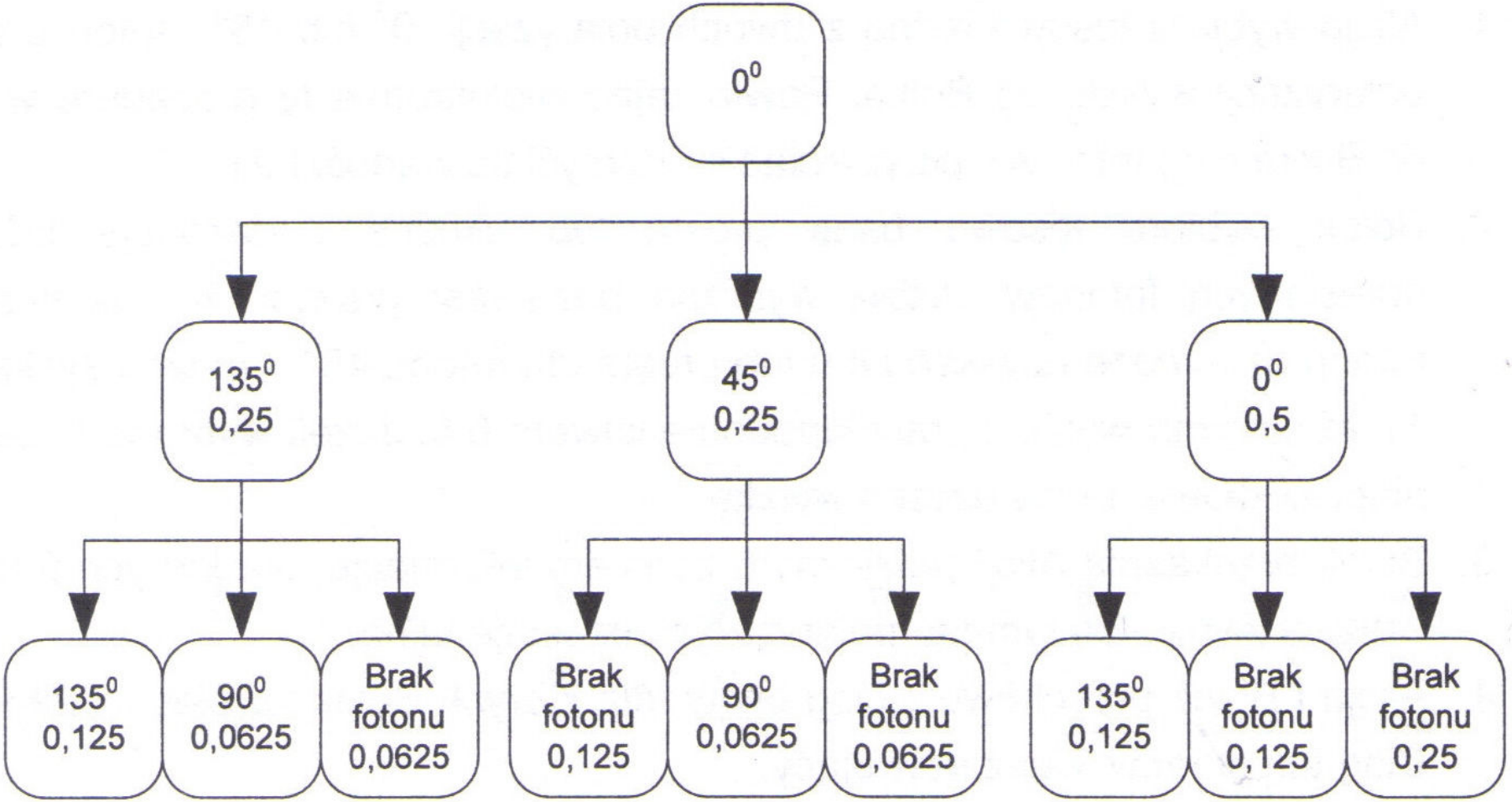
Etapy c.d.:

- Bob przekazuje Alicji kanałem publicznym informację, dla których fotonów uzyskał wynik. Otrzymana polaryzacja pozostaje tajna.
- Alicja i Bob przechowują ciąg bitów, dla których Bob zarejestrował foton. Ciąg ten stanowi klucz szyfrujący.

Protokół B92

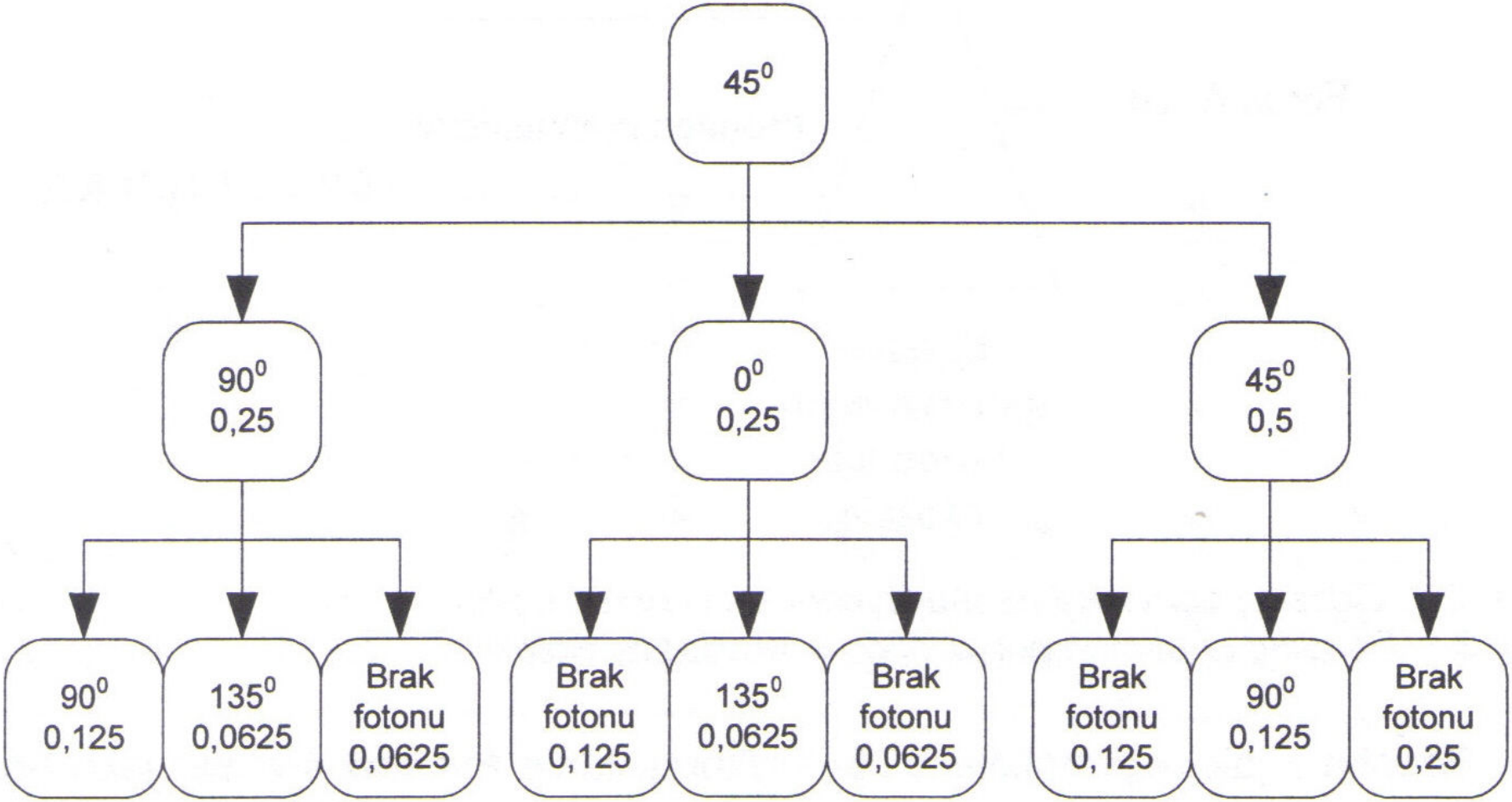
Odczyt polaryzacji fotonów wykonywany przez Boba.

Protokół B92



Możliwe ścieżki fotonu o polaryzacji 0° od nadawcy do adresata przy założeniu, że występuje podsłuch.

Protokół B92



Możliwe ścieżki fotonu o polaryzacji 45° od nadawcy do adresata przy założeniu, że występuje podsłuch.

Protokół B92

- Wykorzystanie fotonów światła jako nośników informacji pozwala na wykrycie podsłuchu na łączu.
- Proces sprawdzania czystości łącza polega na porównaniu ciągu bitów o odpowiedniej długości i stwierdzeniu, czy ciągi te są takie same.
- Jeżeli oba ciągi różnią się od siebie oznacza to, że na łączu wystąpiło przekłamanie spowodowane najprawdopodobniej podsłuchem.
- W takiej sytuacji proces konsultacji klucza rozpoczyna się od początku.

Literatura

- A. Kopczyński, M. Sobota, *Kryptografia kwantowa i biometria jako rozwinięcie klasycznych metod ochrony informacji*, Gliwice 2008.
- Ch. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, 1984.
- http://zon8.physd.amu.edu.pl/~tanas/kwantkrypt.pdf