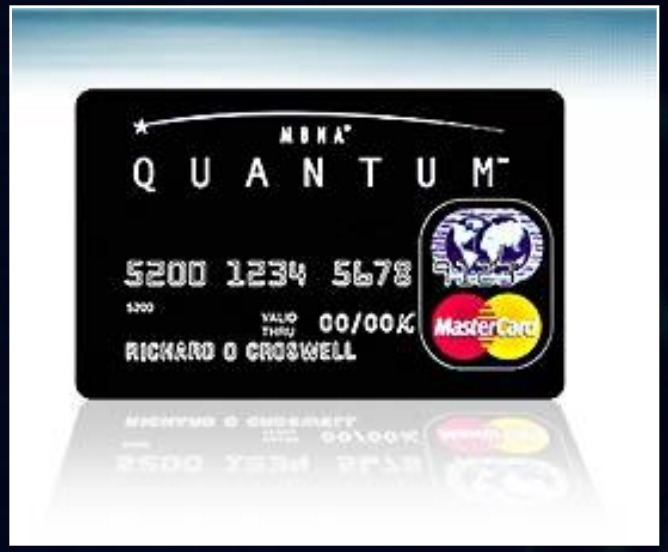
Kwantowe przelewy bankowe - foton na usługach biznesu



Rafał Demkowicz-Dobrzański
Centrum Fizyki Teoretycznej PAN

Zakupy w Internecie

Secure Socket Layer
Bazuje na w wymianie klucza metodą RSA

Jak mogę przesłać ci zaszyfrowaną informację skoro nigdy wcześniej się nie spotkaliśmy i nie mogliśmy ustalić w sekrecie sposobu szyfrowania?

RSA - Bezpieczeństwo dzięki matematyce

Klucz prywatny
Dwie duże liczby pierwsze:
113, 239

Klucz publiczny
113 · 239 = 27007

Sklep

01110101110010101010100

zaszyfrowany numer karty

Użytkownik

odszyfrowanie za pomocą
klucza prywatnego

Do

szyfrowanie numeru karty
za pomocą klucza publicznego

Odszyfrowanie możliwe jest tylko za pomocą klucza prywatnego. Do zaszyfrowania wystarcza klucz publiczny

Czy na pewno bezpieczne?

Bezpieczeństwo bazuje na przekonaniu, że trudno jest rozłożyć liczbę na czynniki pierwsze

Obecnie, czas potrzebny na złamanie szyfru RSA używającego 1024 bitowe klucze - około 5 lat

Zagrożenia:

- Wzrastająca moc komputerów - trzeba systematycznie wydłużać klucz. W roku 1995 wystarczał 768 bitowy. Dzisiaj zaleca się 1280 bitowy.
- Ktoś może jutro wymyślić efektywniejszy algorytm rozkładu liczby na czynniki pierwsze
- Algorytm Shora - algorytm dokonujący błyskawicznie rozkładu na czynniki pierwsze, ale potrzebujący komputera kwantowego, którego jeszcze nie udało się zbudować

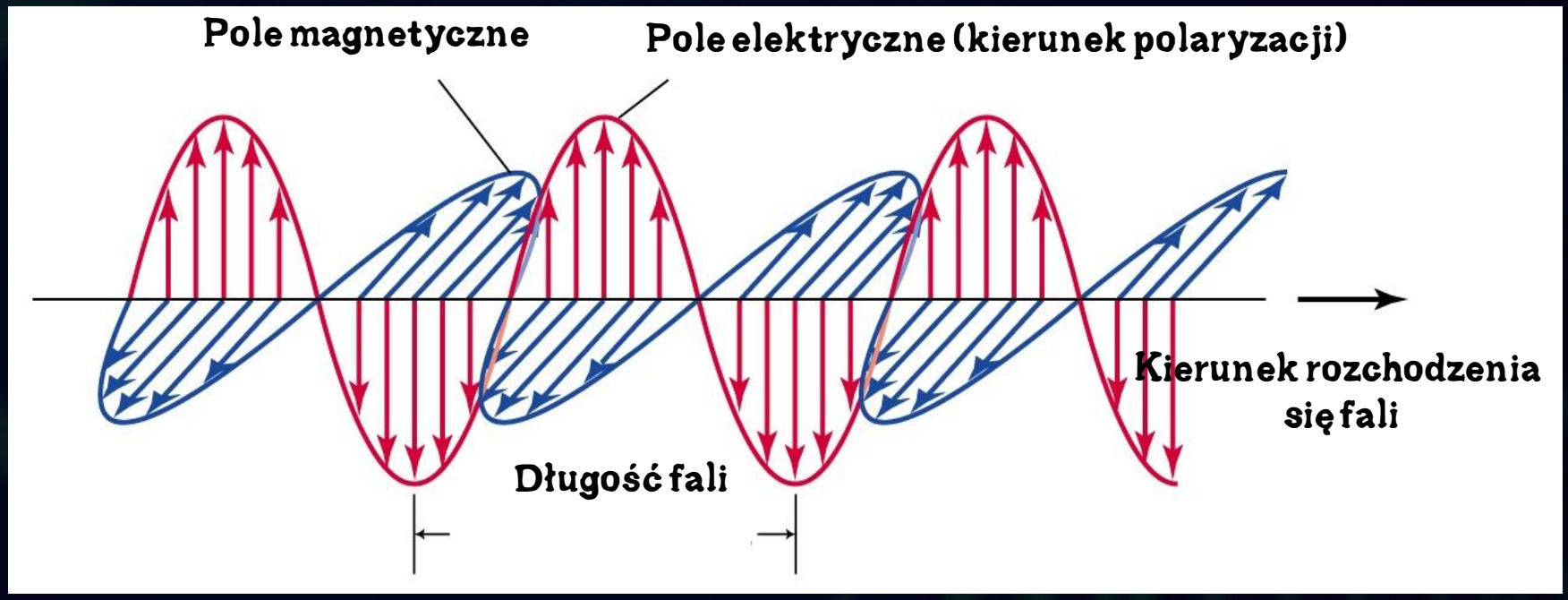
Kwantowa kryptografia - bezpieczeństwo dzięki fizyce

Pomiar stanu układu kwantowego nieuchronnie prowadzi do jego zaburzenia!

Możemy zawsze wykryć podsłuchiwacza

XIX wiek: Światło jest falą

Fala elektromagnetyczna o określonej długości fali:



Czy da się bezkarnie podejrzeć stan polaryzacyjny fotonu?

Sklep

Użytkownik

Światło jest falą elektromagnetyczną

$|0^o\rangle$ $|90^o\rangle$ $|90^o$ $|90^o\rangle$ $|0^o\rangle$ $|0^o\rangle$ $|0^o\rangle$

światłowód

- **Sklep wysyła do użytkownika fotony, każdorazowo wybierając jedną z polaryzacji $|0^o\rangle$ lub $|90^o\rangle$**
- **Podsłuchiwacz umieszcza polaryzator pionowy i sprawdza , czy foton przeszedł czy nie.**

Jeśli przeszedł to znaczy, że był: $|90^o\rangle$

Podsłuchiwacz odsyła użytkownikowi $|90^o\rangle$

Jeśli nie przeszedł to znaczy, że był: $|0^o\rangle$

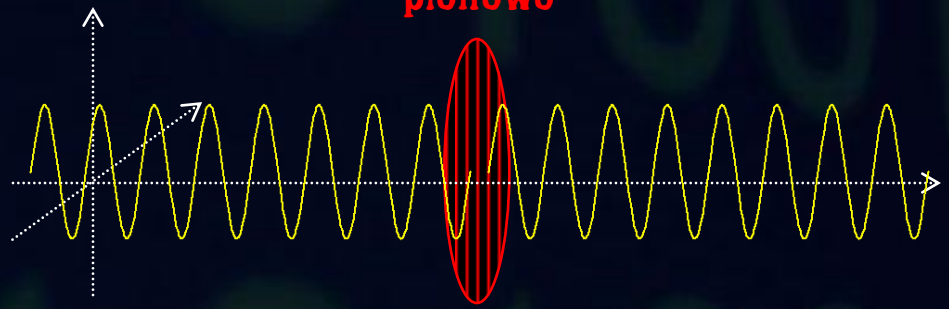
Podsłuchiwacz odsyła użytkownikowi $|0^o\rangle$

Podsłuchiwacz bezkarnie poznał informację

Przechodzenie światła przez polaryzator

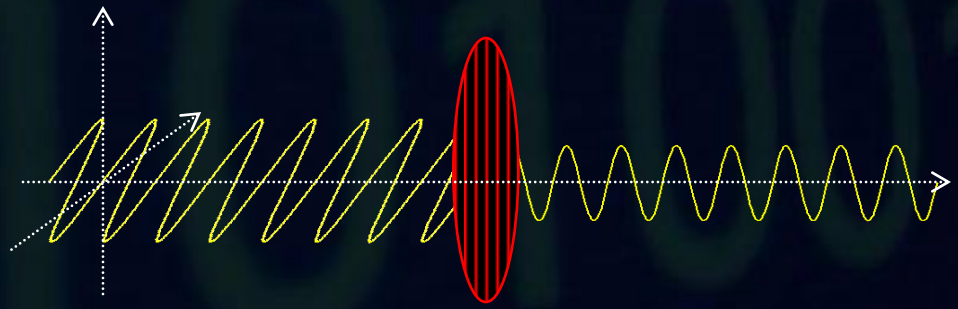
Polaryzator ustawiony pionowo

Światło o polaryzacji pionowej



Przechodzi bez osłabienia

Światło o polaryzacji pod kątem 45 stopni do poziomu

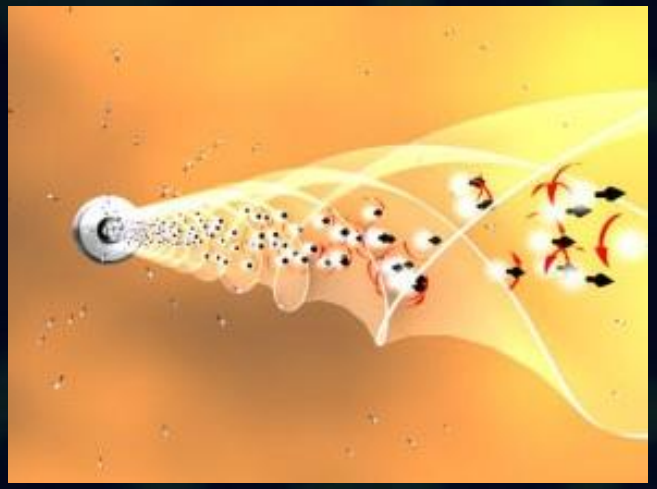


Natężenie światła spada do połowy

Światło o polaryzacji poziomej

Światło całkowicie pochłonięte przez polaryzator

XX wiek: Światło składa się z fotonów

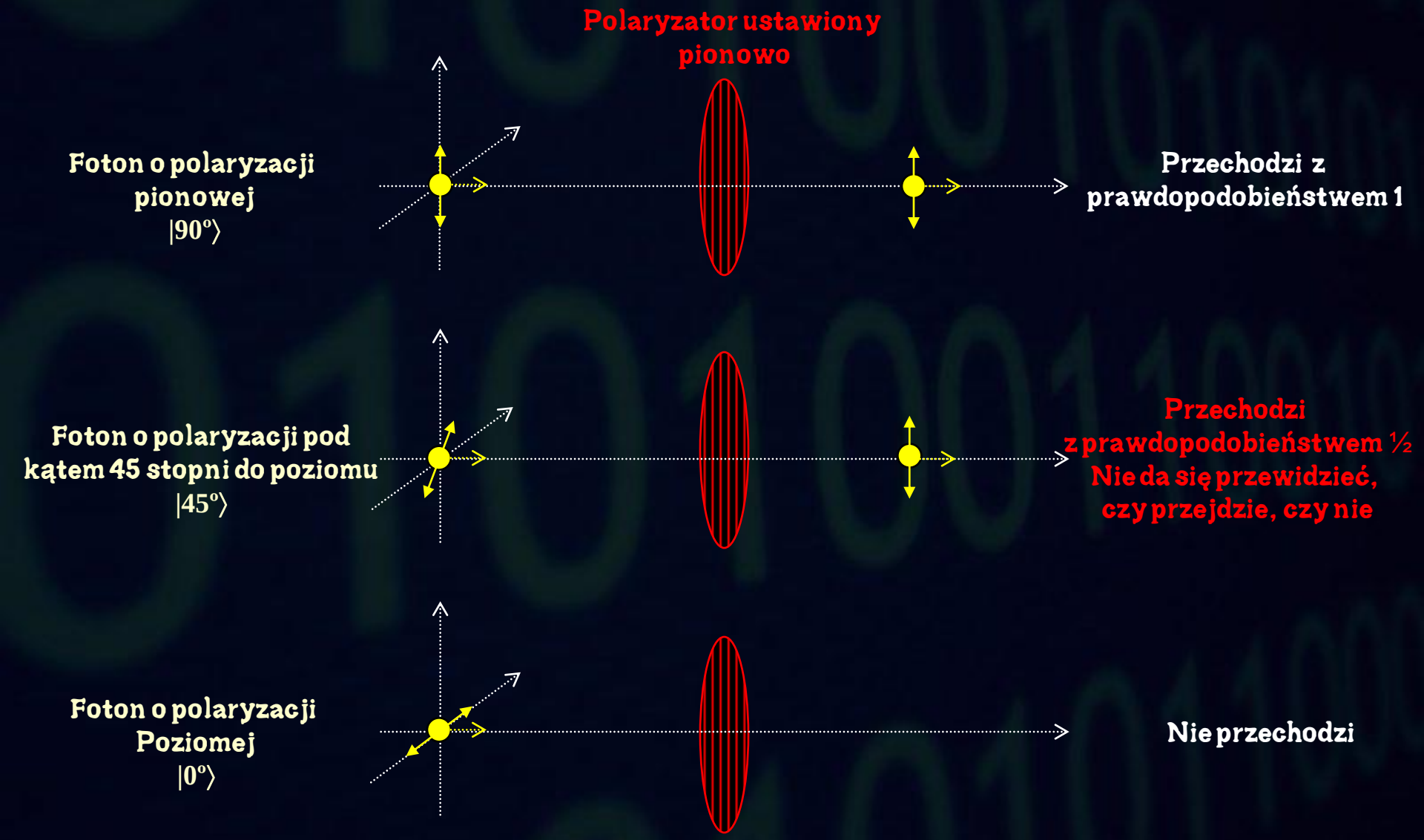


Światło = strumień cząstek zwanych fotonami

Foton może mieć różne polaryzacje

- Światło o polaryzacji pionowej składa się z fotonów o polaryzacji pionowej
- Światło o polaryzacji poziomej składa się z fotonów o polaryzacji poziomej
- ...

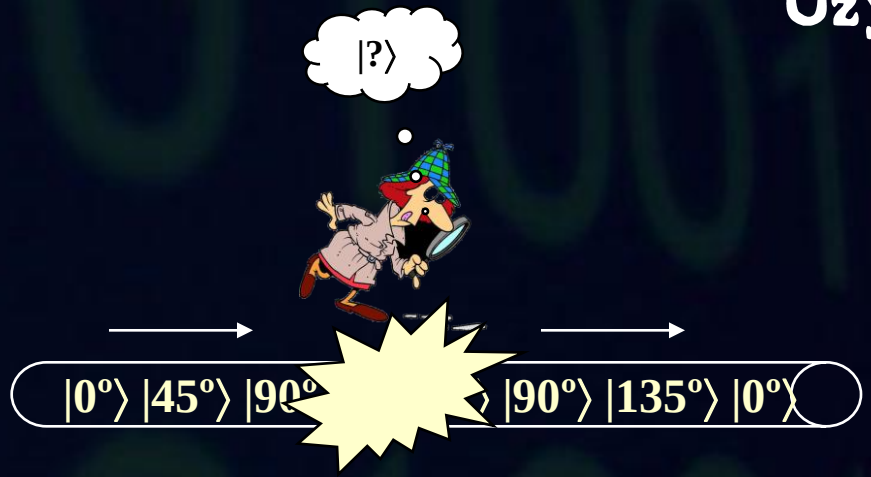
Przechodzenie fotonu przez polaryzator



Użyjmy więcej stanów...

Sklep

Użytkownik



- Sklep wysyła do użytkownika fotony, każdorazowo wybierając jedną z polaryzacji $|0°\rangle$, $|90°\rangle$, $|45°\rangle$, $|135°\rangle$

Do

- Podsłuchiwacz umieszcza polaryzator np. pionowo i sprawdza czy foton przeszedł czy nie.

jeśli przeszedł to mógł być:
$|90°\rangle$, $|45°\rangle$, $|135°\rangle$

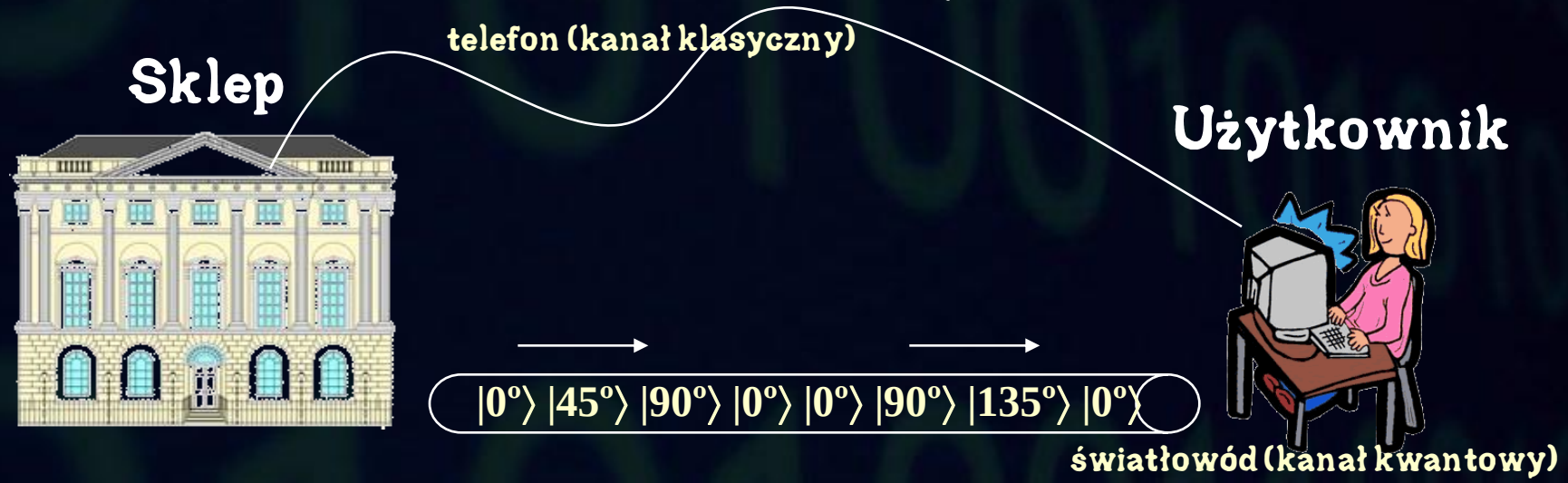
podsłuchiwacz odsyła użytkownikowi $|90°\rangle$

jeśli nie przeszedł to mógł być:
$|0°\rangle$, $|45°\rangle$, $|135°\rangle$

podsłuchiwacz odsyła użytkownikowi $|0°\rangle$

Podsłuchiwacz nie ma pewności jaki foton leciał i ponadto wprowadza zaburzenie

Kryptografia kwantowa - czyli jak rozesłać sekretny klucz?

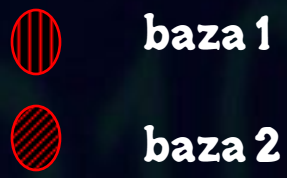


Protokół BB84 (Charles Bennett, Gilles Brassard, 1984)

- Sklep wysyła do użytkownika przypadkowo wybrany jeden z czterech stanów

baza 1:	$\|0°\rangle$	$\|90°\rangle$
baza 2:	$\|45°\rangle$	$\|135°\rangle$
bit	0	1

- Użytkownik mierzy polaryzatorem ustawionym przypadkowo albo pionowo, albo pod kątem 45°



Protokół BB84

- Sklep wysyła do użytkownika przypadkowo wybrany jeden z czterech stanów

baza 1:	$\|0°\rangle$	$\|90°\rangle$
baza 2:	$\|45°\rangle$	$\|135°\rangle$
bit	0	1

- Użytkownik mierzy polaryzatorem ustawionym przypadkowo albo pionowo, albo pod kątem 45°

baza 1

baza 2

- Użytkownik zapisuje sobie jakie stany fotonów zmierzył

sklep	foton	$\|90°\rangle$	$\|90°\rangle$	$\|45°\rangle$	$\|135°\rangle$	$\|0°\rangle$	$\|45°\rangle$	$\|90°\rangle$	$\|0°\rangle$	$\|135°\rangle$
	bit	1	1	0	1	0	0	1	0	1
użytkownik	polaryzator									
	foton	$\|90°\rangle$	$\|45°\rangle$,$\|135°\rangle$	$\|0°\rangle$,$\|90°\rangle$	$\|135°\rangle$	$\|45°\rangle$,$\|135°\rangle$	$\|0°\rangle$,$\|90°\rangle$	$\|90°\rangle$	$\|0°\rangle$	$\|135°\rangle$
	bit	1	0 lub 1	0 lub 1	1	0 lub 1	0 lub 1	1	0	1

- Sklep i użytkownik komunikują się za pomocą kanału klasycznego (mogącego być na podsłuchu) i ujawniają jakich baz używali

Protokół BB84

- Sklep wysyła do użytkownika przypadkowo wybrany jeden z czterech stanów

baza 1:	$\|0°\rangle$	$\|90°\rangle$
baza 2:	$\|45°\rangle$	$\|135°\rangle$
bit	0	1

- Użytkownik mierzy polaryzatorem ustawionym przypadkowo albo pionowo, albo pod kątem 45°

baza 1

baza 2

- Użytkownik zapisuje sobie jakie stany fotonów zmierzył

sklep	foton	$\|90°\rangle$	$\|90°\rangle$	$\|45°\rangle$	$\|135°\rangle$	$\|0°\rangle$	$\|45°\rangle$	$\|90°\rangle$	$\|0°\rangle$	$\|135°\rangle$
	bit	1	1	0	1	0	0	1	0	1
użytkownik	polaryzator									
	foton	$\|90°\rangle$	$\|45°\rangle$,$\|135°\rangle$	$\|0°\rangle$,$\|90°\rangle$	$\|135°\rangle$	$\|45°\rangle$,$\|135°\rangle$	$\|0°\rangle$,$\|90°\rangle$	$\|90°\rangle$	$\|0°\rangle$	$\|135°\rangle$
	bit	1	0 lub 1	0 lub 1	1	0 lub 1	0 lub 1	1	0	1

- Sklep i użytkownik komunikuj się za pomocą kanału klasycznego (mogącego być na podsłuchu) i ujawniają jakich baz używali

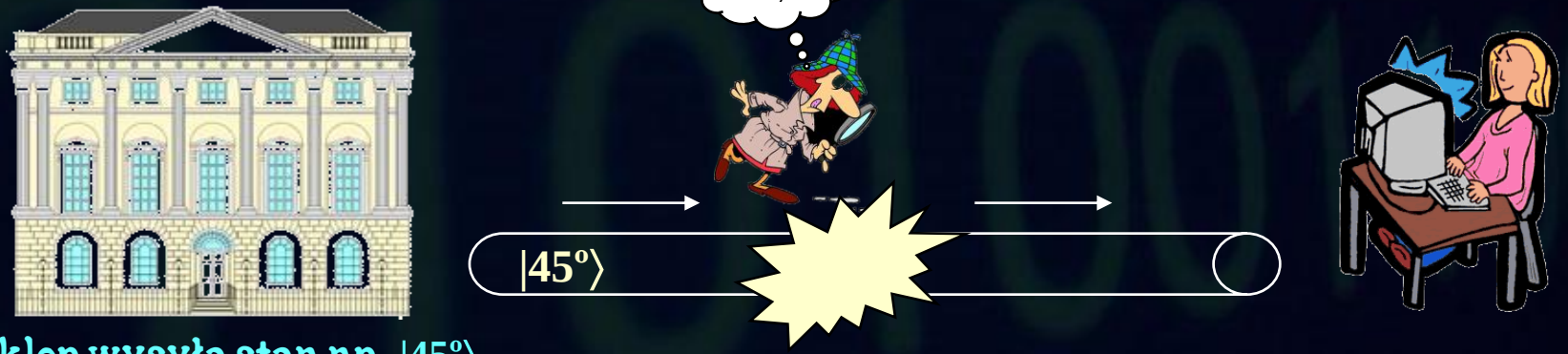
- Jako klucz biorą te bity, kiedy ich bazy były zgodne: 11101

Bezpieczeństwo BB84

- Po uzgodnieniu baz, sklep i użytkownik wybierają przypadkowo część bitów (np. 10%) ze swoich kluczy i ogłaszają je publicznie

Jeśli ujawnione bity się zgadzają, to znaczy, że nikt nie podsłuchiwał i pozostałe bity stanowią sekretny klucz

- Gdyby ktoś podsłuchiwał…



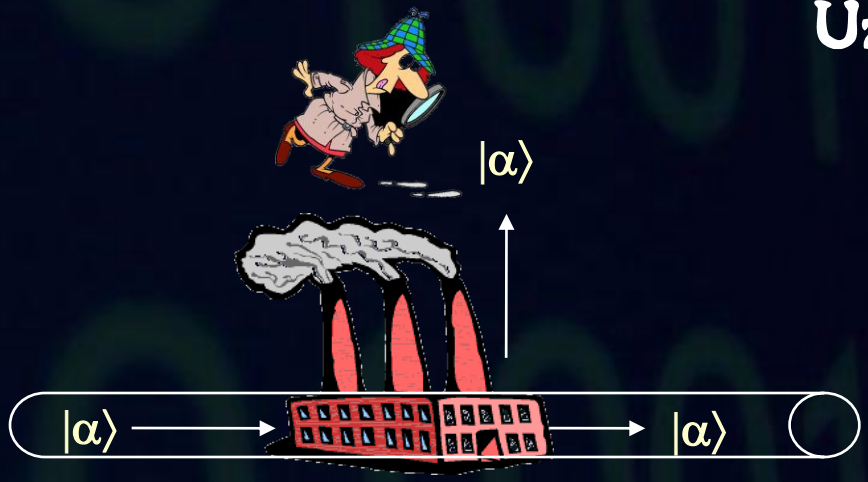
- sklep wysyła stan np. $|45^\circ\rangle$
- podsłuchiwacz z prawdopodobieństwem 1/2 mierzy w niezgodnej bazie i odeśle użytkownikowi stan $|0^\circ\rangle$ lub $|90^\circ\rangle$
- mimo, że użytkownik ma bazę ustawioną zgodnie z bazą sklepu, z prawdopodobieństwem 1/2 uzyska błędny bit

- prawdopodobieństwo, że w wyniku działalności podsłuchiwacza pojawi się błąd w danym bicie = 1/4
- porównując np. 30 bitów, wykryjemy podsłuchiwacza z prawdopodobieństwem 99,98%

O co z klonowaniem?

Sklep

$|\alpha\rangle = |0^o\rangle, |90^o\rangle, |45^o\rangle, |135^o\rangle$



urządzenie klonujące
stan fotonu

Użytkownik

Nieprostopadłych stanów kwantowych nie da się sklonować!

William Wooters, Wojciech Żurek (1982)

Co daje kryptografia kwantowa?

Pozwala dwóm stronom uzyskać przypadkowy ciąg zer i jedynek, o którym wiadomo, że nikt go nie podsłuchał

Co zrobić z przypadkowym ciągiem zer i jedynek?

0+0=0
0+1=1
1+0=1
1+1=0

Informacja: 10101010101010

\+

Klucz: 11101001011001

Zaszyfrowana informacja: 01000011110011

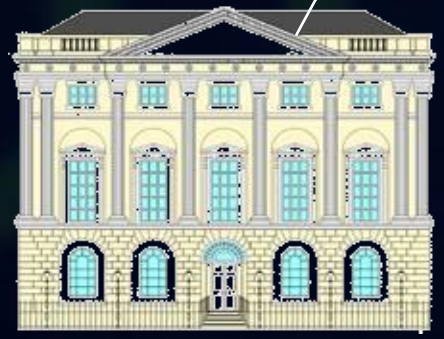
Informacja: 10101010101010

Klucz: 11101001011001

\+

Zaszyfrowana informacja: 01000011110011

Sklep



telefon (kanał klasyczny)

Użytkownik

I mamy 100% bezpieczną komunikację

Trudności kryptografii kwantowej

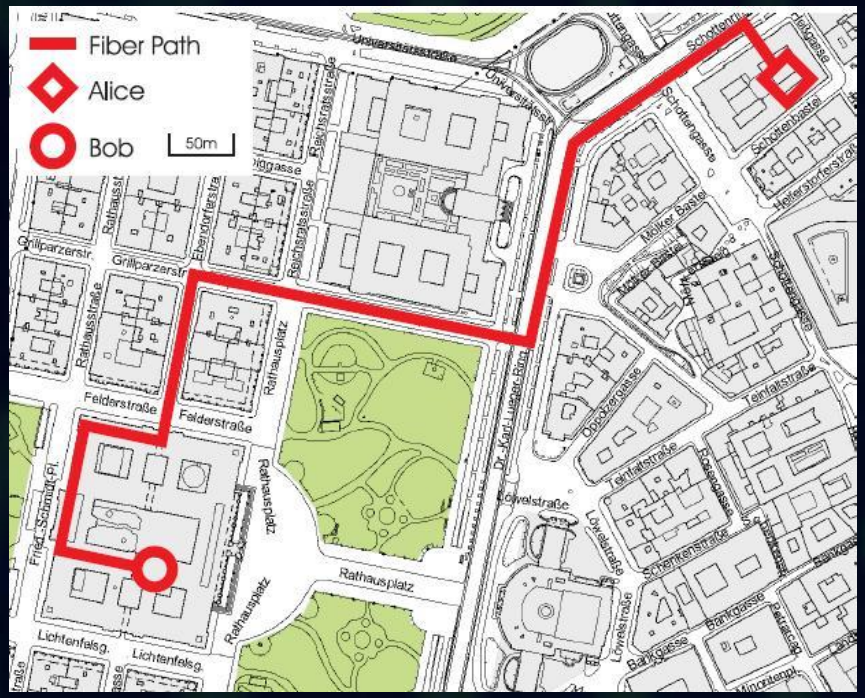
Źródła pojedynczych fotonów

Detektory pojedynczych fotonów (drogie i niewydajne)

Tłumienie w światłowodach
(obecne odległości około 100km)

Zawsze są błędy, nie tylko jak podsłuchiwacz podsłuchuje -
korekcja błędów, wzmocnienie prywatności

Pierwszy kwantowy przelew bankowy



Wiedeń, 21.04.2004

Wymiana klucza pomiędzy Ratuszem i pobliskim Bankiem (odległość 1.5km), zakończony wykonaniem przelewu bankowego

Gdzie to można kupić?

Id Quantique
www.idquantique.com
(Szwajcaria)

MagicQ
www.magicqtech.com
(USA)

Odległość max: 150km
Transfer: 25 kbps
Cena: 100000 $

Już za parę lat....

Kryptografię kwantową rozwijają obecnie jedne z największych firm elektronicznych: NEC, Fujitsu, Toshiba

NEC planuje sprzedawać urządzenia do kryptografii kwantowej od 2008 roku

Urządzenia były już testowane przez armię i największe amerykańskie firmy telekomunikacyjne

W USA, roczne nakłady na badania nad kryptografią kwantową wynoszą 100 mln $.

Kryptografia kwantowa

bezpieczeństwo gwarantowane prawami fizyki kwantowej, a nie wiarą w złożoność pewnych operacji matematycznych