Wyklad5

13 marca 2011
16:18

Implementacje kwantowej dystrybucji klucza

Potrzebujemy trzech elementów

1. Źródła pojedynczych fotonów
2. Kanały do przesyłania fotonów
3. Detektory pojedynczych fotonów.

Idealnie chcielibyśmy mieć źródła wysyłające pojedyncze fotony na żądanie o wysokiej częstości repetycji ~ GHz, kanały w których stan fotonu nie ulega zakłóceniu a sam foton nie ginie, oraz detektory które klikają $\Leftrightarrow$ gdy wpadnie foton .....

To są marzenia, żaden z tych trzech idealnych elementów nie istnieje.

W praktyce

1. Źródła fotonów:

stabe impulsy laserowe, takie że średnia liczba fotonów w impulsie $\bar{n} \lesssim 1$

Impuls laserowy ma statystykę Poissonowską

$$p_n = \frac{\bar{n}^n}{n!} e^{-\bar{n}}$$

Więc może wystąpić również dwa lub więcej fotonów. Niebezpieczne ☠

Przyjmijmy, że $\bar{n}$ może $\bar{n} \ll 1$ wtedy:

$p_0 = e^{-\bar{n}}$ $p_1 = \bar{n} e^{-\bar{n}}$ $p_{n\geq 2} = 1 - p_0 - p_1 = 1 - e^{-\bar{n}} - \bar{n} e^{-\bar{n}}$

Jeśli $\bar{n} \ll 1$

$$p_1 \approx \bar{n} \qquad p_{n\geq 2} \approx -\frac{\bar{n}^2}{2} + \bar{n}^2 \approx \frac{\bar{n}^2}{2}$$

widzimy że $\frac{p_{n\geq 2}}{p_1} = \frac{\bar{n}}{2}$, czyli udział

zdarzeń wielofotonowych jest tym mniejszy im słabsze

impulsy. Ale impulsy nie mogą być za słabe

bo wtedy mamy prawie ciągle pomiarnie...

Trzeba uwzględnić stany wielofotonowe w analizie

bezpieczeństwa

2. Kanały

Podstawowy problem tłumienie. Nat. światła
(a tym samym prawdop. przeżycia fotonu) spada
wykładniczo:

$$I(L) = I(0)\, 10^{-\alpha \cdot L}$$

gdzie α - wsp tłumienia. Podawany zazwyczaj
w dB/km. (α = 10 dB/km oznacza że
natężenie spada 10 razy na 1 km)

a) free space (Tadna pogoda)

- dla fal w zakresie 780-850nm, 1520-1600nm
  $\alpha \leq 0{,}1$ dB/km
  więc super. straty 10 krotne dopiero przy
  100km.
- problemy: trzeba trafić do celu,
  pogoda, powodowanie wiązki...

pomysły: komunikacja przez satelite

patrz np. http://arxiv.org/abs/0806.0945

b) Światłowody

- zalety: można skierować tam gdzie się
  chce. Gotowa infrastruktura telekomunikacyjna
- wady
  - tłumienie większe niż w powietrzu
  ...

tylko dwa praktyczne okienka:

$\alpha = 0{,}34$ dB/km (1330 nm)

$\alpha = 0{,}2$ dB/km (1550 nm)

- fluktuująca dwójłomność – niekontrolowane zmiany polaryzacji w wyniku zmian temperatury, naprężenia.

Jeśli używać się przy qubicie polaryzacyjnym trzeba sporo zachodu żeby mieć aktywną kompensację fluktuującej dwójłomności (potencjalna furtka dla podsłuchiwacza ...)

Pomysł: zakodujmy qubit inaczej ---- kodowanie fazowe (patrz dalej)

c) detektory pojedynczych fotonów

(avalanche photo diodes – jeden foton może wybija elektron, ten przyspieszony może i wybija więcej elektronów itd. aż mamy mierzalny sygnał.

- Si APD, sprawność $\eta = 60\%$ $\lambda = 400-1000$ nm
  ciemne zliczenia $\delta = 100$ Hz, ($T = -30°C$)
  count rate $\simeq$ 15 MHz

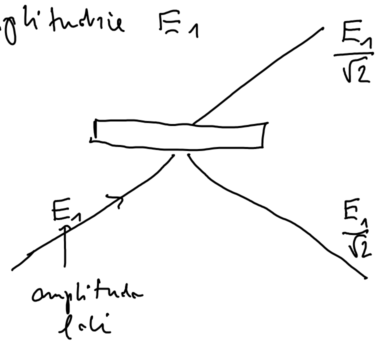
- InGaAs, $\eta = 10\%$ $\lambda = 1000-1650$ nm
  trzeba bramkować, przy count-rate = 0,1 MHz mamy $\delta = 100$ Hz. ($T = -100°C$)
  Jeśli pracujemy w światłowodach to niestety musimy używać takich detektorów, bo Si nie czułe na podczerwień

Te detektory nie rozróżniają liczby padających fotonów.

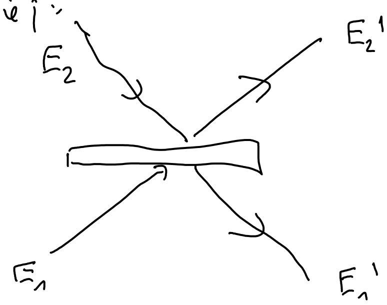
Kodowanie fazowe

- Interferometr Macha-Zehndera

• Płytka światłodzieląca 50%. Myślimy o fali płaskiej o amplitudzie E_1



Ogólniej:



~~$E_1' = \frac{1}{\sqrt{2}}(E_1 + E_2)$~~

~~$E_2' = \frac{1}{\sqrt{2}}(E_1 + E_2)$~~ Tak jest źle!

Dlaczego? Całkowite natężenie przed płytką:

$I \sim E_1^2 + E_2^2$

A energia za płytką

$I' \sim E_1'^2 + E_2'^2 = E_1^2 + E_2^2 + 2E_1E_2 > I$!

Musi dodatkowo być przesunięcie fazowe. Np:

$E_1' = \frac{1}{\sqrt{2}}(E_1 + E_2)$

$E_2' = \frac{1}{\sqrt{2}}(E_1 - E_2)$

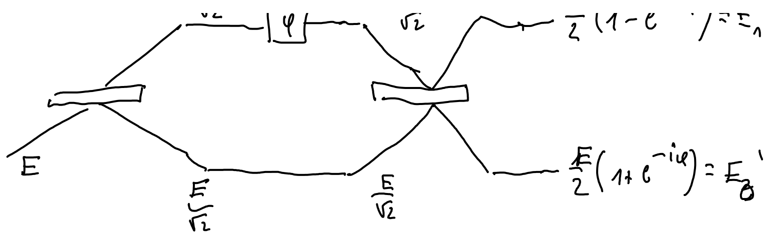
fala E_2 dostaje fazę π przy odbiciu

Można np myśleć tak

wiemy, że przy odbiciu od ośrodka o wyższym n mamy zmianę fazy o π.

• Interferometr   opóźnienie fazowe $\varphi = \frac{\Delta L}{\lambda} 2\pi$ (różnica dróg optycznych)

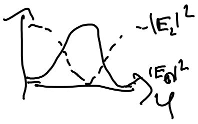
E → $Ee^{i\varphi}$ $E(\ldots e^{i\varphi})\ldots$



Natężenia: $\sim |E_0'|^2$, $\sim |E_1'|^2$

$$|E_1'|^2 = \frac{E^2}{4}\left((1-\cos\varphi)^2 + \sin^2\varphi\right) = \frac{E^2}{4}(2 - 2\cos\varphi) = \frac{1}{2}E^2(1-\cos\varphi)$$

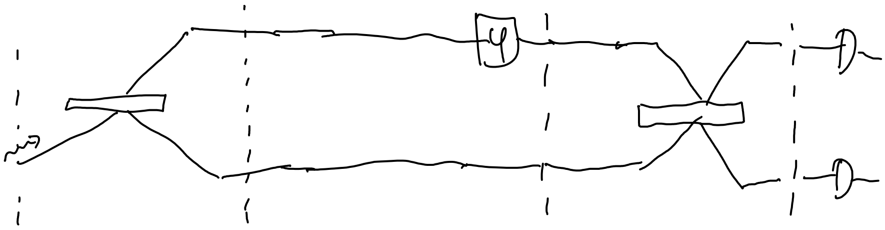
$$|E_0'|^2 = \frac{1}{2}E^2(1+\cos\varphi)$$



W zależności od φ zmienia się natężenie na portach wyjściowych.

Pojedynczy foton w interferometrze

Analogicznie jak dla polaryzacji potraktujemy amplitudy fal jako amplitudy prawdopodobieństwa, a względne natężenia mówią nam o prawdopodobieństwach.



$|0\rangle$ — foton w dolnym ramieniu

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ — foton w superpozycji jednocześnie i w górnym i w dolnym ramieniu.

$\frac{1}{\sqrt{2}}(|0\rangle + e^{-i\varphi}|1\rangle)$

$\frac{1}{2}(1+e^{-i\varphi})|0\rangle + \frac{1}{2}(1-e^{-i\varphi})|1\rangle$

Na koniec mierzymy gdzie jest foton.

Prawdopodobieństwa:

$$p_0 = \frac{1}{2}(1+\cos\varphi) \qquad p_1 = \frac{1}{2}(1-\cos\varphi)$$

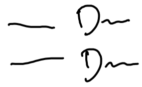
Mamy inną fizyczną realizację qubitu (dual rail qubit). Możemy przygotować stan qubitu używając płytki światłodzielącej i opóźnienia fazowego. Możemy mierzyć po prostu, albo po przepuszczeniu przez kolejną

po prostu, albo po przepuszczeniu przez kolejną płytkę światłodzielącą, jak w interferometrze.

Wszystko co robiliśmy z polaryzacją możemy zrobić też tutaj.

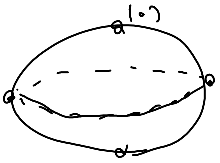
np  = półfalówka pod kątem 22,5°
a gdy same współczynniki odbicia i transmisji to łamy kąt półfalówki

= kostka z opóźnieniem φ

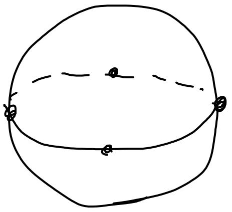
 = polaryzator ustawiony pionowo i poziomo

Protokół BB84 z kodowaniem fazowym

zamiast używać 4 stanów:



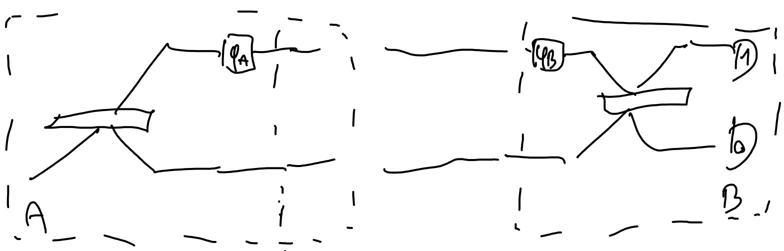
Użyjemy równomiernie stanów na równiku!



$\frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$

dla $\varphi = 0, \pi$ baza 1

$\varphi = \frac{\pi}{2}, \frac{3}{2}\pi$ baza 2



$\frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi_A}|1\rangle)$

Przygotowane stany

$\varphi_A = 0, \pi$

$\varphi_A = \frac{\pi}{2}, \frac{3}{2}\pi$

jeśli $\varphi_B = 0$:

pomiar w bazie $\{0, \pi\}$

0 – klika 0

π – klika 1

$\frac{\pi}{2}, \frac{3}{2}\pi$ – klika 0 v 1 z $p = \frac{1}{2}$

jeśli $\varphi_B = \frac{\pi}{2}$:

pomiar w bazie $\{\frac{\pi}{2}, \frac{3}{2}\pi\}$

$\frac{\pi}{2}$ – klika 0

$\frac{3}{2}\pi$ – klika 1

$\frac{3}{2}\pi$ - wynika 1

$0\ \pi$ - wynika 0 v 1 z $p = \frac{1}{2}$

Mamy BB84