16 - Implementations

10 stycznia 2011
12:30

We need three elements:

1) source of qubits ('photons')
2) channels (free space or optical fibers)
3) detectors (we need single photon detectors)

Ideally we would like to prepare a single photon in a definite polarization state, send it through channel where it experience no (or controllable) polarization transformation, and have an ideal detector which clicks iff a photon enters it. In reality we do not have any of these elements:

[16.1 Source of qubits]

Single photon sources are impractical so much more common is the use of weak coherent laser pulses

Repetition rate $\approx$ GHz

$|\alpha\rangle$ - coherent state photon statistics $p_n = \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} = \frac{\mu^n}{n!} e^{-\mu}$

So apart from single photons we have multiphoton contribution.

Photon number splitting attack (PNS)

- E performs photon number non-demolition measurement
- If $n=1$ she performs a "single photon" attack (she may also block this photon and send vacuum to B)

If $n>1$ she takes away one photon and sends the remaining ones to B. After A & B announce their basis E measures her stored photon in the correct basis

We need to use weak pulses so that that the multiphoton component is not to big ...

[16.2 Channels]

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

- free space $\alpha < 0{,}1$ dB/km (780-850 nm, 1520-1600 nm)

(10 dB - ten times attenuation $\geq$ 100 km) nice

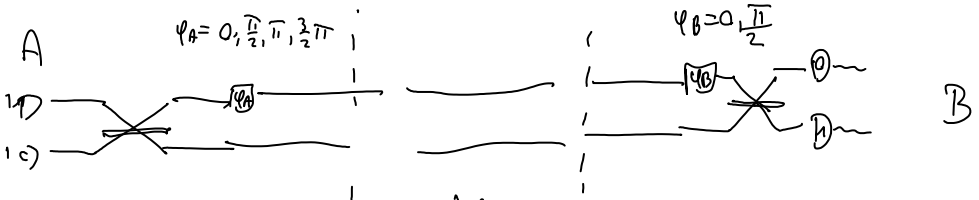
problems - weather, line of sight, beam broadening
ideas maybe via a satelite,

- fibers — $\alpha = 0{,}34$ dB/km (1330 nm)
  $\alpha = 0{,}2$ dB/km (1550 nm

in optical regime not practical, losses to big ~ 10 dB/km.
So we need infrared single photon detectors more challenging than in visible range

— fiber is birefringent, sensitive to stress and temperature variations. Polarization is subject to "random" transformation

Solution: Use a different physical qubit than
- than polarization qubit

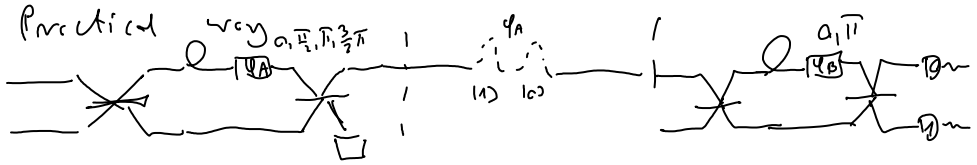


$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + e^{i\varphi_A}|1\rangle|0\rangle\right)$$
$|0\rangle$ $|1\rangle$

if $\varphi_B = 0$ then $\varphi_A = 0 \to |0\rangle$ perfect interference
$\varphi_A = \pi \to |1\rangle$
$\varphi_A = \frac{\pi}{2} \to p = \frac{1}{2}$ |0⟩ $p = \frac{1}{2}$ |1⟩
$\varphi_A = \frac{3}{2}\pi$ — " —

Exactly the same probabilities as in polarization measurement. But this requires stable interferometer over 100s km ~ not practical

- Practical way $0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi_A}|1\rangle\right)$$
↑ ↑
time bins
(50% efficiency)

At B side:
$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi_A}|1\rangle\right) \not\to \frac{1}{2}\left(|0,e\rangle + |0,l\rangle + e^{i\varphi_A}|1,e\rangle + e^{i\varphi_A}|1,l\rangle\right)$$

$\xrightarrow{\varphi}$ $\frac{1}{2}(|1,1\rangle + |0,0\rangle + e^{i\varphi_A}|2,1\rangle + e^{i\varphi_A}|1,0\rangle) \rightarrow$

$\xrightarrow{\text{BS}}$ $\frac{1}{2}\cdot(e^{i\varphi_B}|1,1\rangle + |0,0\rangle + e^{i(\varphi_A+\varphi_B)}|2,1\rangle + e^{i\varphi_A}|1,0\rangle)$

Provided we observe clicks in $|1\rangle$ time bin we have interference and we recover probabilities from ideal setup (overall only $25\% = 50\% \cdot 50\%$ efficiency)

[16.3 Detectors]

We need to register single photon counts

- Si APD $\eta = 50\%$ $\lambda \approx 400\text{–}1000\,nm$ $\delta \approx 100\,Hz$
  (most suitable for infrared) count rate $\simeq 15\,MHz$
  $(T \simeq -30°C)$
- InGaAs $\eta = 10\%$ $\lambda = 1000\text{–}1650\,nm$
  count rate $0{,}1\,MHz$ $\delta \simeq 100\,Hz$ $(T \simeq -100°C)$

[16.4 Practical security analysis]

We use coherent pulses with mean intensity μ, at a repetition rate R_0, over a fiber of length L, with attenuation coefficient α, detectors with efficiency η and dark count rate δ.

At what rate K we can generate secure key ?
(secure bits per second)

We attribute all errors to E and assume her technology is unlimited (lossless fibers, ideal devices etc.). We treat that errors from dark count due to E intervention..

A & B measure QBER (error per bit) and the rate R (number of clicks per second on B side)

B receives a coherent state with average number of photons

$$\mu = \mu_0 \cdot 10^{-\alpha \cdot L}$$

Detector efficiency can be regarded as additional loss

$$\mu = \mu_0 \cdot 10^{-\alpha \cdot L}\,\eta \qquad = \mu \cdot \tilde{\eta}$$

Probability that B registers a click from state sent

$p_{transmition} = 1 - e^{-\mu}$ by A

↑ prob. of vacuum

But additionally B may get a click due to dark counts $p_{dark} = \frac{\delta}{R_0}$

So total click probability:

$$p_{click} = p_{trans} + p_{dark} - \underbrace{p_{trans} \cdot p_{dark}}_{\text{usually negligeble}}$$

Detection rate by B:

$$R = R_0 \cdot p_{click} \approx R_0(1 - e^{-\mu}) + \delta \approx R_0\mu + \delta$$

While $QBER = \frac{1}{2}\frac{\delta}{R} + \varepsilon$

↑ other sources of error (visibility of interferometer) noise in the fiber, (usually negligeble for large distances)

Information gained by E via optimal PNS attack

Let $p_{m\geq 2} = 1 - e^{-\mu_a} - \mu e^{-\mu_a}$ be the probability of more than 1 photon send by A

$$p_{m\geq 2} \approx 1 - 1 + \mu_a - \frac{\mu_a^2}{2} - \mu_a\mu_a \approx \frac{\mu_a^2}{2}$$

If $p_{click} \leq p_{m\geq 2}$ it means E can block single photon signals at only pass multiphoton signals to B on which she has full knowledge so key generation not possible (E uses ideal lossless fiber)

If $p_{click} > p_{m\geq 2}$ then E has to allow some single photon pulses to go to B.

Let f_1 be fraction of $m=1$ pulses that E transmits to B, but of course before that she performs the optimal attack (collective - be careful what collective means here ...)

Then $p_{click} = p_{m\geq 2} + f_1 \cdot p_{m=1} = \frac{R}{R_0}$

This way we can derive f_1:

$$f_1 \simeq \frac{1}{p_{n=1}}\left(\frac{R}{R_0} - p_{n\geq 2}\right) \approx \frac{\mu}{\mu_0} + \frac{\delta}{R_0\mu_0} - \frac{\mu_0}{2}$$

E information per bit...

$$I(A:E) = 1 \cdot \frac{p_{n\geq 2}}{p_{click}} + \frac{Y_1}{\frac{p_{n=1}}{p_{click}}} \cdot h(\varepsilon_1)$$

p_{multi}

error rate introduced in single photon states

$$Y_1 = \left(1 - \frac{R_0}{R} p_{n\geq 2}\right) \simeq 1 - \frac{\mu_0^2}{2\left(\mu + \frac{\delta}{R_0}\right)}$$ - fraction of signals registered by B originating from single photon states

$$QBER = \varepsilon_1 \cdot Y_1$$

$$\varepsilon_1 = \frac{QBER}{Y_1}$$

$$I(A:E) = (1 - Y_1) + Y_1 h\left(\frac{QBER}{Y_1}\right)$$

$$I(A:B) \simeq 1 - h(QBER) = 1 - h\left(\frac{\delta}{2R}\right)$$

Key rate:

$$K \simeq \frac{1}{2} R\left(I(A:B) - I(A:E)\right) =$$

↑ because only in half of the cases basis will agree (can be avoided by using one basis almost all of the time)

$$= \frac{1}{2} R \left(1 - h(QBER) - (1 - Y_1) - Y_1 h\left(\frac{QBER}{Y_1}\right)\right) =$$

$$= \frac{1}{2} R \left[Y_1 \left(1 - h\left(\frac{QBER}{Y_1}\right)\right) - h(QBER) \right]$$

We can optimize over the choice of μ_c

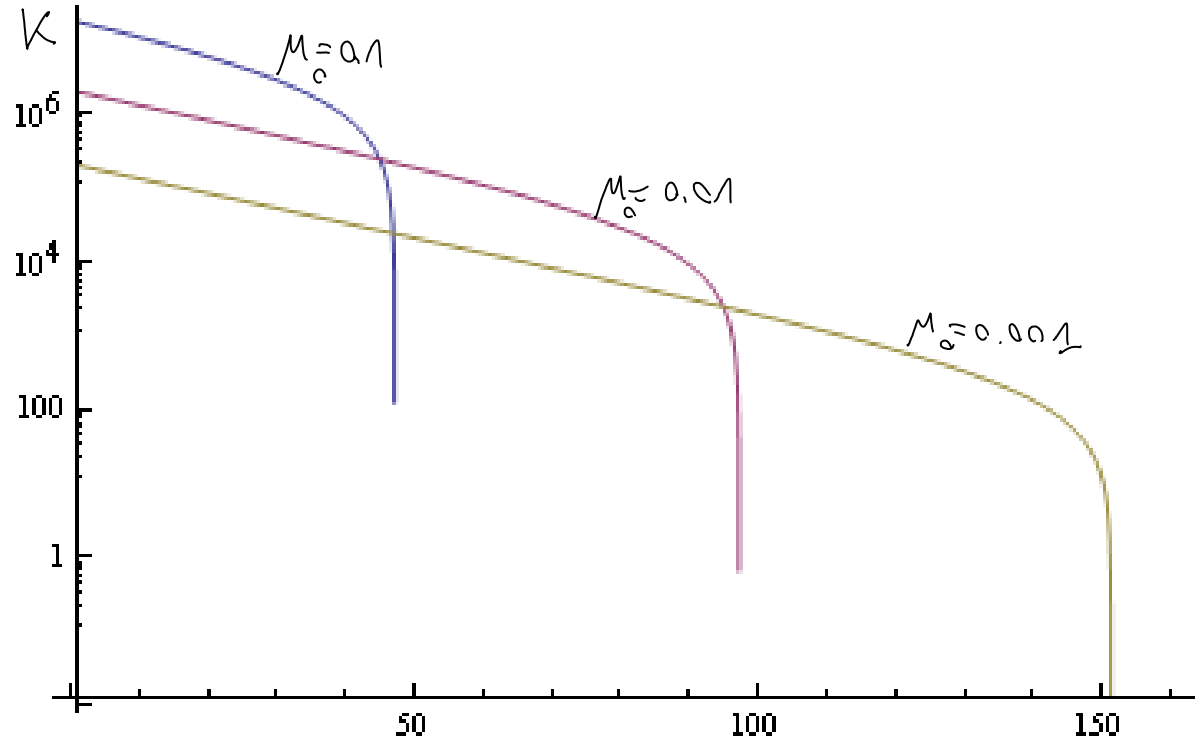
Optimal $\mu_0 \propto \tilde{\eta}$ (we need to lower intensity to lower the danger of multi photon events)

So we need to lower the intensity proportionally to losses $\tilde{\eta}$. Hence $K \propto \tilde{\eta}^2$

Key rate drops very quickly

key rate drops very quickly

A Plot: for ($\alpha = 0{,}2$ dB/km $\eta = 10\%$ $S = 10$ cc Hz $\bar{R} = 1$ GHz



[16.5 Practical ideas]

- Decoy states, to limit the power of PNS attacks A sends a few different types of pulses $\mu_1, \mu_2, \mu_3 \ldots$ (three is enough)

this allows A & B to find exactly $Y_0, Y_1, Y_2, \ldots$ and not only the rate R. Since PNS modifies ratios between Y_i, once this ratios are ok then excludes PNS attack. We get back to

$$K \propto \eta$$

- DPSK
- Continuous variable Cryptography
- MagiQ, Id Quantique

[16.6 Quantum Hacking]

[16.6 Quantum Hacking]

- Imperfect devices
  e.g. different gating times of detectors
- Side channels – other physical channels reveal information about basis settings...