Quantum Information Spring 2023 Problem Set 6

Solutions are due on Sunday June 04, 23:59.

1. **QKD–1: One-time pad**
   Show how to get the message coded using a random sequence of 0's and 1's. Assume that the message is only a letter 'T'. Its ascii is 84, with the command bin(84) in python you get the corresponding binary sequence. Create some random secret key (8 bits) and make the message that Alice sends to Bob using the one-time pad-method.

   Show how Bob regenerates the original message.

   Solution.
   Not applicable.

2. **QKD–2: Attenuated laser**
   Assume 1 GHz pulse repetition rate for pulses that are used for creating secret keys with a highly attenuated semiconductor laser. Assume that the used protocol can stand 4 % pulses containing more than one photon (semiclassical treatment).

   Calculate how many photons you can at maximum use for key production per second. For a laser telecommunication wavelength of $\lambda = 1.55$ μm, what is the corresponding optical power? (photon energy is $\hbar\omega \equiv \hbar(2\pi c/\lambda)$, where
   $\hbar = 1.064 \cdot 10^{-34}$ J·s is the Planck constant.)

   Solution.
   Laser is a coherent source, so the number of photons ("k") in a pulse follows the Poisson distribution ($\langle N \rangle$ is the mean number of photons):

$$p(k) = \left(\frac{\langle N \rangle^k}{k!} \right) e^{-\langle N \rangle}.$$

   Probability x ($x = 0.04$ in this task) of having 2 or more photons per pulse is:

$$x = 1 - p(0) - p(1) = 1 - (1 + \langle N \rangle)\, e^{-\langle N \rangle}. \tag{1}$$

   Assuming the number of photons is low ($N << 1$), one can use the expansion:

$$e^{-\langle N \rangle} \approx 1 - \langle N \rangle + O\left(\langle N \rangle^2\right) \approx 1 - \langle N \rangle\,.$$

For x one has

$$x \approx 1 - (1 + \langle N \rangle)(1 - \langle N \rangle) = \langle N \rangle^2 .$$

Thus, the probability of having $k > 1$ increases with $\langle N \rangle$, and

$$\langle N \rangle_{\mathrm{MAX}} \approx \sqrt{x} \approx 0.2.$$

Exact numerical solution of (1) gives

$$\langle N \rangle_{\mathrm{MAX}} \approx 0.31.$$

This is the mean number of photons per pulse. For the given repetition rate f_{rep}, the maximum number of photons per 1 second is

$$N_{phot}\,(1\text{ s}) = \langle N \rangle_{\mathrm{MAX}} \cdot f_{rep} \cdot 1\text{ s} \approx 3.1 \cdot 10^8,$$

i.e. about 300 millions of photons per second.

Optical power can be calculated as total energy carried by the photons per unit time. Number of photons per second is N_{phot}, and the energy of an individual photon is ($\lambda_0 = 1.55$ μm)

$$E_1 = \hbar\omega = \hbar\frac{2\pi}{\lambda_0} \approx 1.3 \cdot 10^{-19}\text{ J}.$$

Resulting optical power P is

$$P = \frac{\Delta E}{\Delta t} = \frac{N_{phot} E_1}{1\text{ s}} = \hbar\frac{2\pi}{\lambda_0} \approx 4.0 \cdot 10^{-11}\text{ W}.$$

Main outcome is that the number of photons per pulse is significantly lower than one. ■

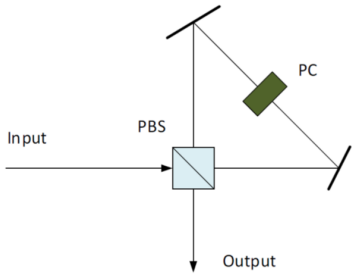
3. **Cavity-based quantum memory**

Cavity-based quantum memory device with a cavity length of 100 cm and a polarization control unit (Pockels cell) with a switching time of 50 ps is used to store light pulses of 200 fs $= 2 \cdot 10^{-13}$ s duration.

- How many distinct pulses N_{stored} can be stored in a single memory unit?
- What is the lowest overall transmittance of the cavity (per one pass) T_{cav}, optical elements included, that allows storing a pulse with 80% efficiency during $K = 200$ passes of the cavity?

Assume non-dispersive medium and negligibly small optical length (= time delay) in both the beam-splitter and Pockels cell.

Reference values of reflectance (power ratio between the reflected and the incident beams) are: $\approx 96\%$ for metal mirrors; $\approx 99.5\%$ for dielectric multilayer mirrors; up to $(1 - 3 \cdot 10^{-7})$ for main mirrors in LIGO gravitational wave interferometer.



Solution
For several pulses to be stored successfully, the pulses need to not intersect with one another in time. Also, the memory should be able to retrieve the desired pulse alone, without extracting additional pulses. Thus, the shortest time interval between adjacent pulses can be estimated as (τ_{PULSE} – pulse duration, τ_{PC} – response time of the Pockels cell):

$$\tau_{PULSE} + \tau_{PC} \approx 50 \text{ ps}.$$

The cavity "capacity" (= cavity round trip time) is (c — speed of light, L -– cavity length):

$$T_{CAVITY} = L/c \approx 3.3 \text{ ns}.$$

That is, one can store up to 3.3 ns/50 ps = 66 pulses in such a memory.
To estimate the efficiency of storing a pulse in a cavity, let us assume that the cavity transmission (overall; for a single pass) is T. For a number $K = 200$ of passes, the storage efficiency η is

$$\eta = T^K.$$

For $\eta = 80\%$:

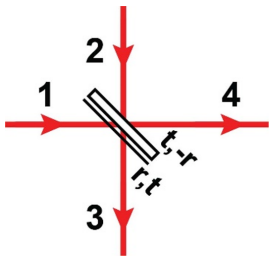
$$T = (\eta)^{1/K} \approx 0.9989.$$

4. **Hong-Ou-Mandel interference – 1**

Let the light at each of the two input ports of a beam-splitter to be in the Fock state $|n\rangle_{\text{F}}$ – that is, the number of photons (n) is fixed. Let the numbers of photons be $n_{1\,F} = M$ and $n_{2\,F} = 0$.
(1) Use the following properties of creation ($\hat{a}$) and annihilation ($\hat{a}^\dagger$) operators

$$\begin{aligned} \hat{a}\,|n\rangle_F &= \sqrt{n}\,|n-1\rangle_F \ , \\ \hat{a}^\dagger\,|n-1\rangle_F &= \sqrt{n}\,|n\rangle_F \ , \\ \hat{a}\,|0\rangle &= 0\cdot|0\rangle = 0 \ , \end{aligned}$$

to express the input state $|M\rangle_{1\,\mathrm{F}}\,|0\rangle_{2\,\mathrm{F}}$ via the operators $\hat{a}_1^\dagger$, $\hat{a}_2^\dagger$.
(2) Using the input-output relations between $\hat{a}_1^\dagger$, $\hat{a}_2^\dagger$ and $\hat{a}_3^\dagger$, $\hat{a}_4^\dagger$ (Figure below and lecture materials), substitute the equations for $\hat{a}_1^\dagger$ and $\hat{a}_2^\dagger$ to the solution of (a). Write down the light state at the output of the beam-splitter. Use the photon-number basis.



$$\begin{pmatrix}\hat{a}_3^\dagger\\ \hat{a}_4^\dagger\end{pmatrix} = \begin{pmatrix} r & t\\ t & -r\end{pmatrix}\begin{pmatrix}\hat{a}_1^\dagger\\ \hat{a}_2^\dagger\end{pmatrix}$$

Solution.
(a) From the properties of operators $\hat{a}$ and $\hat{a}^\dagger$ and for the input state written in the Fock basis as follows:

$$|\Psi_{in}\rangle = |M\rangle_{1\,F}\,|Q\rangle_{2,F}\,, \tag{2}$$

we obtain directly

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{M!\,Q!}}\left(\hat{a}_1^\dagger\right)^M\left(\hat{a}_2^\dagger\right)^Q|0\rangle_1\,|0\rangle_2\,. \tag{3}$$

(b) Following the lecture material, let us use the symmetric form of a transfer matrix for a beam-splitter (r and t are reals):

$$\begin{pmatrix} r & t\\ t & -r\end{pmatrix}. \tag{4}$$

Then the relation between creation operators for input and output modes reads:

$$\begin{pmatrix}\hat{a}_3^\dagger\\ \hat{a}_4^\dagger\end{pmatrix} = \begin{pmatrix} r & t\\ t & -r\end{pmatrix}\begin{pmatrix}\hat{a}_1^\dagger\\ \hat{a}_2^\dagger\end{pmatrix},\ \Rightarrow\quad \begin{pmatrix}\hat{a}_1^\dagger\\ \hat{a}_2^\dagger\end{pmatrix} = \begin{pmatrix} r & t\\ t & -r\end{pmatrix}\begin{pmatrix}\hat{a}_3^\dagger\\ \hat{a}_4^\dagger\end{pmatrix}. \tag{5}$$

Here we will heavily use the following properties of the creation operators:

$$\begin{aligned}\hat{a}\,|n\rangle_F &= \sqrt{n}\,|n-1\rangle_F\ ,\\ \hat{a}^\dagger\,|n-1\rangle_F &= \sqrt{n}\,|n\rangle_F\ ,\\ \hat{a}\,|0\rangle &= 0\cdot|0\rangle = 0\,,\end{aligned}$$

Let the input state be

$$|\Psi_{in}\rangle = |M\rangle_{1\,F}\,|Q\rangle_{2,F}\,, \tag{6}$$

where F denotes the Fock state basis.

Writing it with creation operators for the input radiation modes:

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{M!\,Q!}} \left(\hat{a}_1^\dagger\right)^M \left(\hat{a}_2^\dagger\right)^Q |0\rangle_1 |0\rangle_2 \,. \tag{7}$$

The output state is then

$$|\Psi_{out}\rangle = \frac{1}{\sqrt{M!\,Q!}} \left(r\hat{a}_3^\dagger + t\hat{a}_4^\dagger\right)^M \left(t\hat{a}_3^\dagger - r\hat{a}_4^\dagger\right)^Q |0\rangle_1 |0\rangle_2 \,. \tag{8}$$

From now on, let us use the simplified case when $Q = 0$ – which is what we are asked to calculate:

$$\begin{aligned} |\Psi_{out}\rangle &\to \frac{1}{\sqrt{M!}} \left(r\hat{a}_3^\dagger + t\hat{a}_4^\dagger\right)^M |0\rangle_{3\,F} |0\rangle_{4\,F} = \\ &= \frac{1}{\sqrt{M!}} \sum_{k=0}^{M} \frac{M!}{k!(M-k)!} r^k t^{M-k} \sqrt{k!}\sqrt{(M-k)!}\, |k\rangle_{3\,F} |M-k\rangle_{4\,F} = \\ &= \sum_{k=0}^{M} \sqrt{\frac{M!}{k!(M-k)!}} r^k t^{M-k} |k\rangle_{3\,F} |M-k\rangle_{4\,F} \,. \end{aligned} \tag{9}$$

An example for $M = 2$ and $Q = 0$:

$$|2\rangle_{1\,F} |0\rangle_{2\,F} \to t^2 |0\rangle_{3\,F} |2\rangle_{4\,F} + \sqrt{2}rt\, |1\rangle_{3\,F} |1\rangle_{4\,F} + r^2 |0\rangle_{3\,F} |2\rangle_{4\,F} \ . \tag{10}$$

For $M = 1$ and $Q = 1$ one gets the Hong-Ou-Mandel effect, in which for a symmetric beam-splitter ($r = t = 1/\sqrt{2}$) two indistinguishable input photons can only leave the device at the same port:

$$|1\rangle_{1\,F} |1\rangle_{2\,F} \to rt\sqrt{2}\, |2\rangle_{3\,F} |0\rangle_{4\,F} + (t^2 - r^2)\, |1\rangle_{3\,F} |1\rangle_{4\,F} + rt\sqrt{2}\, |0\rangle_{3\,F} |2\rangle_{4\,F} \ . \tag{11}$$

The probability P to have one photon at each of the outputs is

$$P = |\langle 1|_{3\,F} \langle 1|_{4\,F} |\Psi_{out}\rangle|^2 = \left(t^2 - r^2\right)^2 . \tag{12}$$

This probability vanishes for a balanced beam-splitter ($r = t = 1/\sqrt{2}$), so the indistinguishable photons exit the symmetric beam-splitter from the same port.

5. **Hong-Ou-Mandel interference – 2**

Using the setting and the results of the previous exercise, evaluate the output state if the input one is

$$|1\rangle_{1\,\mathrm{F}}\,|0\rangle_{2\,\mathrm{F}}\ .$$

If the photons at ports 1 and 2 are used as a path-entangled qubit ($|1\rangle_{1\,\mathrm{F}}\,|0\rangle_{2\,\mathrm{F}} \equiv |0\rangle_{logical}$, $|0\rangle_{1\,\mathrm{F}}\,|1\rangle_{2\,\mathrm{F}} \equiv |1\rangle_{logical}$), what is the equivalent quantum circuit that performs the same transformation on the input state?

Solution.

For $m_0 = m_1 = 1$, we obtain from (9):

$$|\Psi_{out}\rangle = r\,|1\rangle_{3\,F}\,|0\rangle_{4\,F} + t\,|0\rangle_{0\,F}\,|1\rangle_{4\,F}\ . \tag{13}$$

For a symmetric beam-splitter, this transformation is given by the Hadamard gate:

$$|\Psi\rangle_{out} = \begin{pmatrix} r & t \\ t & -r \end{pmatrix} |\Psi\rangle_{in} \to \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |\Psi\rangle_{in} = \mathbf{H}\,|\Psi\rangle_{in}\ . \tag{14}$$