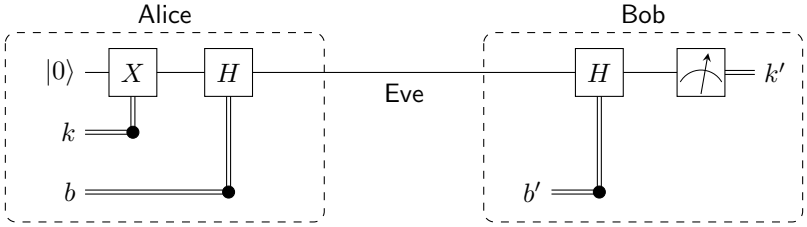
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 27 Jan 2021

Tutorial 10 (Quantum key distribution and the BB84 protocol[1])
Quantum key distribution (QKD) is a provably secure protocol by which two people (who want to communicate privately) create a private key over a *public* quantum channel. The security of this protocol relies on the fact that obtaining information from a qubit (in general) disturbs the qubit. As usual, we call the two parties Alice and Bob.

(a) Consider a third party, Eve, who is trying to distinguish between two non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$. Prove that she will necessarily disturb the states.

Knowing this, Alice and Bob can look for anomalies and restart the protocol if they suspect any eavesdropping.

One specific QKD protocol is the so-called *BB84* protocol, which works (slightly simplified) as follows: Alice first generates a string of random classical bits, a subset of which will eventually become the key. In the diagram below, k denotes one of these bits. She then encodes each bit as $\{|0\rangle, |1\rangle\}$ (Z eigenbasis) or $\{|+\rangle, |-\rangle\}$ (X eigenbasis). Which basis to use is also decided at random, by generating another string of random classical bits of the same length; b in the diagram denotes one of these bits. She sends the states through a public quantum channel to Bob, who measures them in the X or Z eigenbasis. Bob likewise decides which basis to use by generating his own random bit string. The diagram summarizes the protocol for sending one qubit.



(b) Describe what Bob will obtain compared to what Alice sent, assuming no noise and no eavesdropping.

Once Bob has received and measured all qubits sent by Alice, he and Alice compare the basis in which they encoded/measured each qubit, by communicating the string of bs and b's over a classic (possibly public) channel. (Note that neither b nor b' reveal anything about k or k'.) They discard all bits for which they used a different basis.

(c) Let's assume an eavesdropper Eve had access to the public quantum channel. She intercepted Alice's qubits and – due to lack of knowledge which basis to use – randomly guessed whether to measure each intercepted qubit with respect to the Z or X eigenbasis, before passing it on to Bob. In this case, how will Alice's and Bob's bit strings compare?

(d) How can Alice and Bob finally agree on a key while ensuring there were no eavesdroppers?

(e) Why is it essential that Alice publishes her string of bs *after* Bob has completed his measurements?

Exercise 10.1 (Reduction of factoring to order-finding)

(a) We apply the algorithm from the lecture to factor $N = 221$: First confirm that steps 1 and 2 are passed. For step 3, suppose we choose $x = 55$, which is co-prime to 221. Compute the order r of x modulo N (for which you should obtain an even number), and verify that $x^{r/2} \neq -1 \mod N$. So the algorithm succeeds! As last step, compute $\gcd((x^{r/2} \bmod N) \pm 1, N)$, both of which should yield a factor of N.

Hint: Regarding step 2, you can numerically compute $\sqrt[b]{N}$ for integers $2 \leq b \leq \log_2(N) = 7.78\ldots$, and confirm that this never results in an integer.

(b) Show that $N = 15$ is the smallest number for which the order-finding subroutine is required, that is, it is the smallest composite number that is not even or a power of some smaller integer.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Section 12.6.3

Exercise 10.2 (Quantum operations and amplitude damping[2])
For this exercise we will use the formalism of quantum operations, which describes in general terms how a quantum system evolves, typically when applying quantum gates or performing measurements.[3] Abstractly,

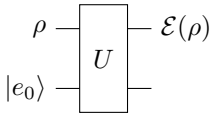
$$\rho' = \mathcal{E}(\rho),$$

where $\mathcal{E}$ is the quantum operation and ρ the density matrix of the initial quantum system. For example, a unitary transformation is written as $\mathcal{E}(\rho) = U\rho U^\dagger$, and a measurement with outcome m as $\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$ (possibly up to a normalization factor). It turns out that the following *operator-sum representation*

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \tag{1}$$

with E_k complex matrices satisfying[4] $\sum_k E_k^\dagger E_k \leq I$, captures in greatest generality any quantum operation compatible with the laws of quantum mechanics.

Another (equivalent) representation is obtained by embedding the principal system ρ into an environment, which we can assume (without loss of generality) to start in some state $|e_0\rangle$, and then applying a unitary transformation to the combined system, as illustrated in the following diagram:



From that, one obtains $\mathcal{E}(\rho)$ by "tracing out" the environment; for this purpose we first extend $|e_0\rangle$ to a basis $\{|e_k\rangle\}$ of the environment:

$$\mathcal{E}(\rho) = \mathrm{tr}_{\mathsf{env}}\left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right] = \sum_k \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle = \sum_k E_k \rho E_k^\dagger$$

with the matrix entries of E_k given by $(E_k)_{\ell,m} = \langle \ell, e_k|U|m, e_0\rangle$. Thus we have derived the operator-sum representation in Eq. (1)!

Amplitude damping models effects due to the loss of energy from a quantum system, for example by loosing a photon (elementary particle of light) from a cavity. In this case one can think of $|0\rangle$ and $|1\rangle$ as the physical system with zero or one photon, respectively. Specifically, the operator-sum representation of amplitude damping is given by

$$\mathcal{E}_{\mathsf{AD}}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$$

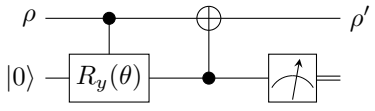
with

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \tag{2}$$

and a real parameter $\gamma > 0$, which one can interpret as the probability of losing a photon. Note that E_1 maps $|1\rangle \mapsto \sqrt{\gamma}\,|0\rangle$.

(a) Show that the operation elements $\{E_k\}$ in Eq. (2) satisfy $\sum_{k\in\{0,1\}} E_k^\dagger E_k = I$.

We now want to verify that the following circuit describes the amplitude damping operation, with $\gamma = \sin(\theta/2)^2$:



Recall that R_y is the rotation operator

$$R_y(\theta) = \mathrm{e}^{-i\theta Y/2} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}.$$

(b) Find the 4×4 matrix representation U_{AD} of the controlled-$R_y(\theta)$ gate followed by the flipped CNOT gate in the above circuit.

(c) Finally, read off the corresponding operation elements with entries $(E_0)_{\ell,m} = \langle \ell, 0|U_{\mathsf{AD}}|m, 0\rangle$ and $(E_1)_{\ell,m} = \langle \ell, 1|U_{\mathsf{AD}}|m, 0\rangle$, and confirm that they agree with Eq. (2).

[2] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Exercise 8.20
[3] It might be helpful to revisit section "4. The density operator" for this exercise.
[4] We write $A \leq B$ for matrices A and B if $B - A$ is positive semidefinite.