QNT 402 Quantum Information
Homework 4

1. [30] *RSA lite*. The RSA protocol can be written as:
   1. The receiver picks two (large) prime numbers m and n
   2. The receiver computes their product $p = mn$.
   3. The receiver picks a random small odd integer j that has no common factors with the quantity $b = (m-1)(n-1)$.
   4. The receiver then computes k from $k\ j$ mod b = 1.
   5. The receiver then publishes their public key as the pair of numbers (j, p)
   6. The receiver does not share their secret key k
   7. The transmitter encrypts their message M (a bit stream) according to:
      $$E(M) = M^j \text{mod } p.$$
   8. The transmitter sends $E(M)$ over a public channel.
   9. The receiver then decrypts the message according to:
      $$M = \big(E(M)\big)^k \text{mod } p$$

   To see RSA, in action let's work through an example.
   a.) [5] Given $m = 11$ and $n = 19$, find k assuming we have chosen $j = 13$.
   b.) [5] What is the public key that Alice publishes?
   c.) [5] Suppose Alice wants to send the phrase "CA" to Bob and uses the alphabet we discussed in class, i.e. C = 00011 and A = 00001 to Bob. To send this as one message we can put them together as the binary number 0001100001_2. Calculate the encrypted message $E(M)$ that Alice will send.
   d.) [5] Show that Bob can decode this with his secret k.
   e.) [10] The chosen m and n can only be used to send messages up to a certain length. Find the maximum value of M that can be successfully sent with this m and n.

2. [40] *Quantum communication preliminaries.* In order to use quantum communication protocols like BB84 it is necessary to produce single photons in a desired polarization state. Suppose, you have a single photon source that always produces vertical polarization.
   a.) [20] Design the system that Alice would need in order to use these vertically polarized photons in the BB84 protocol. Your system will need the ability to produce both polarizations in the H/V basis and the Diagonal basis. Show using Jones calculus that your design can accomplish the production of the necessary four polarization states.
   b.) [20] Design the system that Bob would need to measure these photons in the BB84 protocol. Show using Jones calculus that your design is correct.

   For both (a) and (b), please don't worry about how you would control the necessary optical elements, but rather just draw what they are and use the Jones calculus to show they create what is required.

3. [80] *B92 is not an airplane.* In this problem we'll write a B92 simulator using QuTip quantum objects. In the B92 protocol Alice sends 0 as $|\leftrightarrow\rangle$ and 1 as $|\nearrow\rangle$, while Bob measures with either a vertical polarizer in front of his detector (i.e. $|\updownarrow\rangle$) or with the polarizer rotated to the opposite diagonal polarization that Alice uses (i.e. $|\nwarrow\rangle$). Thus, if Bob is using a vertical polarizer and sees a click on his photon detector he knows that Alice must have sent a 1, while if he's using his diagonal polarizer and sees a click on his photon detector he knows she sent a 0.
    a.) [15] Write a python function that models Alice. That is, "Alice" is a function that accepts an integer N_p which is the number of bits (photons) that Alice sends to Bob via the quantum channel. "Alice" outputs a list that has N_p rows and two columns. The first column is just the index number of the event (i.e. it runs from 1 to N_p). The second column is a qutip quantum object (qubit) that is the polarization of the photon that was sent. Write the photon state in the H/V (i.e. 0/1) basis. For each photon, have "Alice" choose randomly which bit to send – overall she should send bit 0 with probability ½ and bit 1 with probability ½.
    b.) [15] Write a function that models Bob. The function "Bob" accepts the output of "Alice" and returns only the events where he gets a click and therefore knows what bit Alice meant to send. Specifically, have Bob return a list that has two columns. The first column is the index (event number) and the second column is the bit that Bob thinks Alice sent.
    c.) [10] Using your functions to generate a private key based on sending 100 photons from Alice to Bob. Suppose Alice and Bob use ½ of their accepted events – here accepted events are simply the events where Bob gets a click -- to verify their channel.
    d.) [20] Now write a function for a spy "Eve" who takes the output that "Alice" produces, performs the same measurement that Bob uses, and then outputs an a list that is in the same form as the output of Alice. "Eve" must respect the quantum no cloning theorem and therefore can only make her best guess about what quantum state Alice sent based on the result of her measurement. Use any strategy you want to make this guess.
    e.) [10] Now pass the output of Alice to Eve and the output of Eve to Bob to attempt to generate a key from 100 photons. Suppose Alice and Bob use ½ of their accepted events to verify their channel. What is the error rate they find?
    f.) [10] Try to design an Eve which achieves an error rate of about 25%. (When find the error rate you'll find it helpful to increase N_p so that you are comparing more bits at the end and therefore have better statistics.)