University of Exeter, **Exeter Scholars** online residential - July 2020

Quantum Cryptography - Quiz

1. **Binary code:** There are many ways of encoding English language letters into a binary alphabet of 0's and 1's. For electronic communication, a standard code is *ASCII*. Find out what *ASCII* stands for, for example on Wikipedia, and then answer the following question.
   What does the binary code "110000111010111100001" stand for in English letters?

   A. "buy"
   B. "not"
   C. "lol"
   D. "aka"

   If you are intrigued by encoding systems, look up *UTF-8* which has superseded *ASCII* and today is the most commonly used encoding for the World Wide Web. You may also find this (external) post interesting.

2. **One-time-pad (OTP) -1- :** Let's assume Alice wants to send the ordered binary message 010 to Bob, where here the symbol 0 shall simply code for "don't buy" and symbol 1 codes for "buy". The position in the code refers to three publicly known stocks, Stock 1, 2 and 3, i.e. the only stock that Alice wants Bob to buy is Stock 2.

   Consider the set of random one-time-pads abc with $a, b, c \in \{0, 1\}$. List the possible (ordered) one-time-pads that could be used to encrypt Alice's message above. How many different one-time-pads are there?

   A. 10
   B. 8
   C. 6
   D. 4

3. **One-time-pad (OTP) -2- :** Following on from the previous question, now list the set of possible encrypted messages that Alice could send, i.e. work out $010 \oplus abc$ for each one-time-pad abc where $\oplus$ stands for binary addition for each position, i.e. binary-add 0 and a and write the encrypted bit for Stock 1, and so on.

   What is the percentage of the set of possible encrypted messages $010 \oplus abc$ to have a "1" in the second position? I.e. if the encrypted message is intercepted by Eve and she takes it as Alice's original message, how likely is Eve to guess the correct bit value ("1") for the second position?

   A. 0%
   B. ≈ 33%
   C. 50%
   D. 100%

4. **Quantum encodings:** As described in the talk, in quantum key distribution Alice chooses a photon's polarisation axis randomly as either z or x, and also encodes randomly either 0 or 1. How likely is Alice to send the state $+$?

   A. 0%
   B. 25%
   C. ≈ 33%
   D. 50%

5. **Quantum probabilities:** The notation $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ describes the set of possible polarisation states of a single photon in the so-called "$z-x$ plane", where θ is an angle. For example, for $\theta = 0°$ the state is $|\psi\rangle = |0\rangle$ which we called "0" in the talk, for $\theta = 180°$ the state is $|\psi\rangle = |1\rangle$ which we called "1" in the talk, for $\theta = 90°$ the state is $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which we called "+" in the talk, and for $\theta = -90°$ the state is $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ which we called "−" in the talk.

   As discussed in the talk, when a "1"-polarised photon is measured with a z-polarising filter, the outcome is "1" with probability 1 while when a "+"-polarised photon is measured with a z-polarising filter, the outcome is "1" with probability 1/2 (and "0" with probability 1/2).

   For a photon polarised at angle $\theta = 60°$, when measured with a z-polarising filter, what do you think is the probability to obtain the outcome "1"?

   A. 1/4
   B. 1/3
   C. 1/2
   D. -1/2

6. **Key rate generation -1- :** In the key-distribution protocol discussed in the talk, Alice encodes a random symbol 0 or 1 in a photon's polarisation in either z or x axis, randomly chosen. Then Bob measures with either a z-polarising filter or an x-polarising filter, also chosen randomly.

   If there are no eavesdroppers and no noise on the transmission line from Alice to Bob, what is the chance that they prepare and measure in the same axis?

   A. 1/2
   B. 1/4
   C. 1/3
   D. 3/4

   In cryptography, the number above is the "key rate", i.e. the number of bits Alice and Bob share per bit sent.

7. **Key rate generation -2- :** Alice sends a random symbol as in the previous question, but now the eavesdropper Eve measures using either the z or x-polarising filter (randomly chosen), and then sends a photon prepared in the state of her measurement outcome on to Bob.

   Considering only those situations where Alice and Bob prepared and measured in the same axis, what is the chance that their bit values disagree (because of Eve's intervention)?

   A. 1/2
   B. 1/3
   C. 1/4
   D. 1/8

8. **Three dimensions - 1 - :** One can extend the key-distribution protocol discussed in the talk to include a third axis of encoding, the y-axis, see Fig. 1. So, in addition to using the z and the x axis, Alice can now also use the two states of the y axis, ↻ and ↺, which physically correspond to a right-circular-polarised photon and a left-circular-polarised photon.

   Indeed the set of all (so-called "pure") polarisation states of a single photon is actually $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\mathrm{i}\phi}\sin\frac{\theta}{2}|1\rangle$ where e is the exponential function, i is the imaginary number, $\mathrm{i} = \sqrt{-1}$, and ϕ is an angle between $[0°, 360°]$, which previously we hadn't considered, i.e. we had assumed it was $0°$. All states $|\psi\rangle$ lie on a sphere called "Bloch sphere". Fixing $\theta = 90°$, we now have for $\phi = +45°$ the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle)$ which we give the symbol "↻", while for $\phi = -45°$ the state is $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle)$ which we denote "↺".

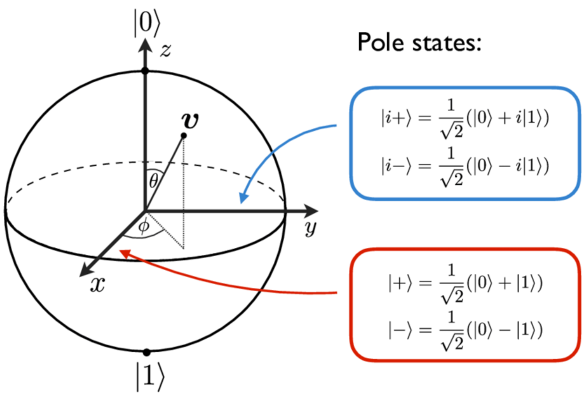

Figure 1: Illustration of Bloch sphere, reproduced from the thesis of A. Ketterer, available on Researchgate 19 July 2020. The pole states along the z-axis are $|0\rangle$ and $|1\rangle$. The pole states along the y-axis, here denoted $|i+\rangle$ and $|i-\rangle$, are our ↻ and ↺. The symbol $\boldsymbol{v}$ in the figure representing any polarisation state on the Bloch sphere is $|\psi\rangle$ in our notation. For further information on the Bloch sphere see, e.g., this post on Wikipedia.

   Similar to Question 4 above, if Alice's encoding is done at random, but now in three possible axes rather than two, how likely is Alice to send the state ↺?

   A. 50%
   B. 25%
   C. ≈ 33%
   D. ≈ 16%

9. **Three dimensions - 2 - :** Similar to Question 6 above, if there are no eavesdroppers and no noise on the transmission line from Alice to Bob, what is the chance that they prepare and measure in the same axis?

   A. 1/2
   B. 1/4
   C. 1/3
   D. 3/4

10. **Three dimensions - 3 - :** Similar to Question 7 above, considering only those situations where Alice and Bob prepared and measured in the same axis, and Eve measured Alice's photon in one of the three axes at random and sent on to Bob a photon encoding her measurement result, what is the chance that Alice and Bob's bit values disagree (because of Eve's intervention)?

    A. 1/2
    B. 1/3
    C. 1/4
    D. 1/8