BB84: Quantum Coins

We can demonstrate the basic ideas of the BB84 protocol in the following game. We need three groups (Alice, Bob and Eve), and a moderator/courier to act as a quantum channel and enforce the laws of quantum mechanics. The aim will be to establish a shared key between Alice and Bob, and show that they can detect the presence of an eavesdropper, Eve.

Instructions

Alice:

- Toss a coin. Result tells you what basis to encode in – heads: H/V, tails: D/A.
- Toss another coin. Result tells you what bit to transmit – heads: 0, tails: 1.
- So, based on the two coin tosses encode as follows:

	H/V box	D/A box	Basis	Bit
HH	Place coin heads up	Place coin inside and shake to randomize	H/V	0
HT	Place coin tails up	Place coin inside and shake to randomise	H/V	1
TH	Place coin inside and shake to randomize	Place coin heads up	D/A	0
TT	Place coin inside and shake to randomize	Place coin tails up	D/A	1

Both boxes together represent a single quantum system – each box represents a different possible measurement that could be made by Bob / Eve. Shaking the box representing the basis NOT used by Alice ensures that both outcomes are equally likely if a measurement is made in this basis.

Moderator:

Take both boxes to Bob, stopping at Eve on the way.

Eve:

For the purposes of this demonstration, Eve's strategy will be to make a measurement on only one in five of the signals she receives, to try to gain some information about the key without being detected. Eve therefore proceeds as follows:

- Make a measurement on one in five systems, chosen at random. In all other cases return both boxes to the moderator undisturbed.
- Making a measurement:
    - Toss a coin. The coin toss decides in which basis Eve chooses to measure. Heads – H/V; tails – D/A.
    - The moderator allows Eve to look in the corresponding box and write down the bit value found there (heads: "0", tails: "1").
    - The moderator shakes the other box to randomise. **Randomizing the other box is crucial!!! This simulates the disturbance caused to the system by Eve's measurement.**

Bob:

- For each system received, Bob chooses at random a basis in which to measure. He does this by tossing a coin. Heads: H/V, tails: D/A.
- The moderator allows Bob to look in the corresponding box only. Bob writes down the bit value found there (heads: "0", tails: "1").

Post processing 1 (basis reconciliation)

- Once all the quantum systems have been exchanged, Alice publicly announces each basis she used (but be careful she doesn't announce the bit).
- For each basis announced, Bob will say "yes" if he measured in the same basis, and "no" otherwise.
- Both Alice and Bob will keep the corresponding bit if they used the same basis, and discard the bit otherwise.

Post processing 2 (Error rate estimation)

- Alice and Bob publically compare the first third of their bits.
- If all the bits are the same, they can conclude that no Eavesdropper is present and use the rest of the key as their secret key.
- If there is some discrepancy, they detected Eve so throw away the key and go after Eve!

Worksheet (Alice)

Communication			Post-processing
	Raw key		Keep bit?
	Basis (H/V, D/A)	Bit (0, 1)	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			

Final key?

Worksheet (Bob)

Communication			Post-processing
	Raw key		
	Basis (H/V, D/A)	Bit (0, 1)	Keep bit?
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

Communication			Post-processing
	Raw key		
	Basis (H/V, D/A)	Bit (0, 1)	Keep bit?
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			

Final key?

QCSYS
Quantum Cryptography
School for Young Students

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing