# The Bennett-Brassard Protocol
# Protecting Information, Chapter 3.1

Timo Lindfors

20.2.2008

# Motivation

- Alice and Bob want to generate a shared secret.
- Eve has a quantum computer.
- Alice has read "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" [Shor94] and knows that a quantum computer can solve the discrete logarithm problem (DLP) efficiently.
- Traditional Diffie-Hellman key exchange depends on the difficulty of DLP so Alice and Bob need to use something else.

# Idea: Use quantum effects to detect Eve

- "Quantum cryptography: Public key distribution and coin tossing" [Bennett & Brassard 1984]
- Alice can send photons to Bob and encode the key in the polarization of the photons.
- Recall that measurement of a quantum variable is not passive.
- If Eve uses wrong basis for her measurement she will get random measurements. However, the same is also true for Bob.
- To solve this, Alice and Bob use a classical channel to figure out which measurements were done using right basis. Measurements done with wrong basis can be ignored.

# Step 1/6: Generate key

- Alice generates two random $n$-bit strings
  $A = (a_1, \ldots, a_n)$
  $S = (s_1, \ldots, s_n)$
- where $a_i \in \{0, 1\}$ is used to represent secret bits and
- $s_i \in \{+, x\}$ denotes the basis used for photons polarization.

## Step 2/6: Send photons

- Alice sends n photons to Bob.
- Alice uses $s_i$ to select between two possible bases
  $M_+ = (|\updownarrow\rangle, |\leftrightarrow\rangle)$
  $M_\times = ((|\updownarrow\rangle + |\leftrightarrow\rangle)/\sqrt{2}, (|\updownarrow\rangle - |\leftrightarrow\rangle)/\sqrt{2})$
- and $a_i$ to select if he uses the first or the second element of the basis.

# Step 3/6: Receive photons

- Bob generates random $n$-bit string
  $R = (r_1, \ldots, r_n)$
- where $r_i \in \{+, \times\}$.
- When Bob receives $i$th photon he measures its polarity in base $r_i$ and finally gets bit string
  $B = (b_1, \ldots, b_n)$
- If Alice and Bob happened to chose the same basis and no tampering occured $a_i = b_i$.

# Step 4/6: Exchange S and R

- Alice and Bob exchange S and R over a classical channel and compare them.
- If $s_i \neq r_i$ Alice removes $a_i$ from A and Bob removes $b_i$ from B. Let's denote the modified versions with A' and B'.
- If there has been no interference A' and B' should be identical since they were sent and measured in the same basis.
- Since there is a 50% chance that Alice and Bob used the same basis the length of A' should be approximately $n/2$.

## Step 5/6: Estimate errors

- Even without Eve there will be errors in the transmission.
- Alice sends a random subset of A' to Bob over a classical channel.
- Bob can estimate the total number of errors using this sample.
- After the estimation bits sent over classical channel are removed from A' and B' since Eve knows them. We'll denote the end result A" and B".

# Step 6/6: Estimate information Eve could have gained

- Estimated number of error bits in the previous step is used to estimate the amount of information Eve might have got.
- This information is used to derive even smaller strings A''' and B''' that Eve should not be able to know anything about.
- Details covered in Chapter 5 (presentations on 9.4. and 23.4.) involve error correction and privacy amplification.

# Probabilistic analysis

- Suppose Eve measures a photon with probability p and then resends it to Bob.
- Eve learns the bit with probability p/2.
- Eve causes an error with probability p/4 (Eve uses wrong basis and Bob measures wrong bit).

# Estimating amount of information

- If Eve knows that a bit is 0 with probability $p_0$ and 1 with probability $p_1$ the Rényi entropy of the distribution is defined as
$$H_R(p_0, p_1) = -log_2(p_0^2 + p_1^2)$$
- With $H_R(0, 1) = 0$ Eve knows exactly what the bit is.
- With $H_R(1/2, 1/2) = 1$ Eve does not know anything about the bit.
- With $H_R(1/8, 7/8) = 0.36$ Eve has reasonably strong belief that the bit is 1.
- We also define the term Rényi information to mean $1 - H_R$.

# Limitations

- Naturally man-in-the-middle is still possible if Eve can modify traffic on both quantum and classical channels.
- Errors in the quantum channel limit the practical distance over which messages can be sent.
- Imprefect hardware might send more than one photon per bit. Eve could measure these with different bases and learn the right basis. However, "Unconditional security of practical quantum key distribution" [Inamori et al. 2006] claims that the protocol can be made secure in even in such a real-world setting.

# Summary

- The Bennett-Brassard protocol provides a secure way to share a secret.
- The protocol needs both a quantum channel and an authenticated classical channel.
- Security is mainly based on the fact that there is no passive way to measure a quantum variable.
- (Quantum) error correcting codes and privacy amplification are needed to use the protocol in the real world. These will be covered later in other representations.