Quantum Cryptography

Julie Butler

Quantum Coin Flipper

Coin Flipping

- Specifically in cryptography: two people who distrust each other and are in separate locations need to agree on a piece of information without relying on a third party

Quantum Coin Flipper vs. Quantum Key Distribution

- Quantum Key Distribution: Assumes that both people involved in the transactions trust each other
  - Protocols in place to prevent an outside untrustful person
  - No protocols to prevent the two people in the transaction from being distrustful, assume that they will co-operate fully
- Quantum Coin Flipper: Assumes the two people in the transaction do not trust each other
  - Both members of the transaction need to provide private information, but neither is trusted to not cheat
  - Protocols are put into place to prevent each member of the transaction from cheating.

Quantum Coin Flipper Protocol

- Person 1 generates a random string of bits. All bits are then encoded with the same filter (Filter 1 or Filter 2).
- Person 1 sends Person 2 the string of qubits
- Person 2 measures each qubit using both Filter 1 and/or Filter 2, recording the results for each.
- Person 2 determines which filter was used to encode the bits.
- Person 2 shares with Person 1 the filter used and a random bit he decoded.
- Person 1 shares the filter and the same random bit.
- If they match then the people can trust each other.

Assumptions and Cheating

- Assumptions: Person 1 and Person 2 are independent, Person 2 is able to measure all states with an equal probability, The string and Person 2's choice of measuring are completely random
- Cheating: Person 2 could cheat if he had a greater than 50% probability of knowing Person 1's basis ahead of time. Person 1 can deny Person 2's claim or send Person 2 a different string of qubits.
- Detecting third parties is similar to quantum key distribution but harder due to the mistrust

To the Board!

- Assume Person 1 used Filter 1 and the binary string: “011001”
- Now assume Person 1 used Filter 2.