# CS406 Research Directions in Computing

## 21st May 2004 — REVIEW OF QUANTUM CRYPTOGRAPHY

- Using quantum effects we can solve the problem of key distribution

- If a secret key $k$ is exchanged in perfect secrecy, messages can be encrypted and decrypted using perfect cryptosystems $(E_k, D_k)$:

$$D_k\{E_k\{m\}\} = m$$

### THE BASIC IDEA OF QUANTUM KEY DISTRIBUTION:

1. Take a sequence of bits $\{b_i\}$.
2. Map each bit to a state $|\psi_i\rangle$ using basis ⊞ or ⊗.
3. The only way to recover each $b_i$ is by using the same basis for decoding:
   - if the correct basis is used, correct result
   - if the wrong basis is used, result is random!

### PHOTONS:

Map a 0 to $|\rightarrow\rangle$ and a 1 to $|\uparrow\rangle$ } Rectilinear basis (⊞)

Map a 0 to $|\nearrow\rangle$ and a 1 to $|\searrow\rangle$ } Diagonal basis (⊗)

EAVESDROPPER :

- Receives a photon e.g. $|\rightarrow\rangle$
- She doesn't know the basis used, so she chooses:
  - if she uses ⊞ she obtains $|\rightarrow\rangle$ and knows it is a 0,
  - if she uses ⊗ she obtains:

    $|\nearrow\rangle$ with 50% probability, and interprets it as a 0 ;

    $|\searrow\rangle$ with 50% probability, and interprets it as a 1.

The same applies for the legitimate receiver.

To correct ERRORS or differences btw. Alice and Bob's sequences, they perform

"RECONCILIATION"

by discussing the bases they used over a public channel.

- Whatever the eavesdropper learns at this point is of no use, because it's too late to make measurements again.

# Using Entanglement for QKD

## What is an EPR-pair?

→ A pair of correlated qubits $(|\psi_1\rangle, |\psi_2\rangle)$ such that measuring one of the two collapses the state of the other.

To do key distribution, an EPR source generates N pairs $(|\psi_1\rangle, |\psi_2\rangle)$ and sends $|\psi_1\rangle$ to Alice (the sender) and $|\psi_2\rangle$ to Bob (the receiver).

*When the polarisation of $|\psi_1\rangle$ is measured, measuring $|\psi_2\rangle$ will give a known result (and vice versa).*

An eavesdropper's only hope is to attack the EPR source and try to get $|\psi_1\rangle$ or $|\psi_2\rangle$. In this case, the pair will be disturbed and Alice and Bob's qubits will not match!

So Alice and Bob make measurements and compare their results. If their results are different when the same measurement basis was used, they know they have detected an eavesdropper. So they start again, some other day!

GOOD LUCK WITH YOUR EXAMINATIONS!

☺