Lecture 21

Quantum cryptography

E91 (Ekert) protocol

- pairs of entangled photons in polarisation state

$$\begin{aligned}\psi(1,2) &= \frac{1}{\sqrt{2}}\Big(V(1)\,V(2)+H(1)\,H(2)\Big)\\ &= \frac{1}{\sqrt{2}}\Big(D(1)\,D(2)+A(1)\,A(2)\Big)\end{aligned}$$

- one sent to Alice, one to Bob
- Alice and Bob each set their analysers at random:
  either $+$: measure V or H; or $\times$: D or A
- entangled states → results agree if both choose same setting
- Alice and Bob measure stream of photons
  then exchange information on settings of analysers
  but not results of measurements
- each time both chose the same setting → one shared secret bit

Eavesdropper Eve measures Bob’s photons before they reach him

- must set her analyser at random
- when Eve’s setting is the same as Alice’s and Bob’s
  → she gets one of their “secret” bits
- but measurement collapses state → destroys entanglement
- when Eve’s setting is different from theirs
  Alice and Bob get unentangled photons → random results
- Alice and Bob can compare results of some of their measurements where they used the same settings
  (should all agree)
- if 25% disagree → sign that Eve is listening in