Quantum Cryptography: Public key distribution and coin tossing

Charles H. Bennett, Gilles Brassard 1984

- uncertainty principle - makes it impossible to eavesdrop $\Delta x \Delta p \geq \hbar/2$ without high probability of detection.
- coin tossing protocol - secure against traditional cheating, even with an unlimited computing power.
  - not secure against the Einstein-Podolsky-Rosen paradox
    ↳ entangle two particles, can predict particle A by measuring particle B without disturbing particle A
- information theory - key is only totally secure if it is as long as the plaintext
- works on a passive eavesdropping channel - can't be so active as to suppress communication completely
- disadvantages - quantum transmissions can not be amplified
  - no digital signatures
- polarized light - send light through Polaroid filter or calcite crystal
  - uncertainty principle - can't measure more than 1 bit into about polarization
  - polarization axis α → filter at orientation β → probability transmitted: $\cos^2(\alpha-\beta)$
    ↑ probability absorbed: $\sin^2(\alpha-\beta)$
  - deterministic when axis are perpendicular
  - when not perpendicular: $\alpha°$ axis α → pass through filter axis β → axis β loses info about axis α

The filter changes axis polarization of the light

- Bases: for polarized photon is 2D

  ex: $r_1 = (1, 0)$ horizontal polarization
  $r_2 = (0, 1)$ vertical polarization

  angle α polarized horizontal: state vector $(\cos\alpha, \sin\alpha)$

  measurement: $P(\text{horizontal}) = \cos^2\alpha$
  $P(\text{vertical}) = \sin^2\alpha$

  r_1, r_2 are rectilinear basis
  d_1, d_2 are diagonal basis

  $d_1 = (0.707, 0.707)$ represents 45° photon
  $d_2 = (0.707, -0.707)$ represent 135° photon

  - conjugate: if 2 bases (rectilinear and diagonal), each has equal length projections on all vectors of that basis.
    - Photon in one basis loses all stored info when measured in other basis.
- 3rd basis - circular polarization
  $c_1 = (0.707, 0.707i)$
  $c_2 = (0.707i, 0.707)$ - not used by this by this paper
- classical public key cryptography - trapdoor functions
- one-time pad - key used once per msg
- Alice - random polarization bases to encrypt key
- Bob - random polarization bases to decrypt key
  - half the data is lost (if Bob measures in wrong base)
- Alice and Bob compare over classical channel - assume channel susceptible to eavesdropping but NOT injection or alteration of msg.
- example; compare 1/3 of shared key to test for interception
  - don't use these bits in key
- Wegman-Carter authentication tags - small secret key that Alice and Bob agree on beforehand (similar to check sum) can use key bits from quantum channel to replace used bits.

Quantum Coin Tossing

- apply similar technique to the coin problem -
  problem: Alice and Bob are on the phone. They don't trust eachother. How can they agree on wins on fair coin toss.
- method is secure against opponent of unlimited computing power
- Einstein-Podolsky-Rosen effect - threatens this system however, it requires perfect detection of photons
  - EPR paper rises skepticism in entanglement, our understanding of physics and universe. non-locality.
  - QKD relies on our current understanding of quantum mechanics

1. Alice chooses random basis and random bits and sends encoded bits to Bob
2. Bob chooses random basis for each photon. He records decrypted bits in two tables, one for rectilinear and one for diagonal basis. He guesses which bases Alice used. Bob wins if he chose correct basis
3. Alice certifies the win/loss by sending her bits over a quantum channel
4. Bob compares Alice bits match the corresponding table.

- Any attempts to cheat by Alice will be detected