Quantum Cryptography

CMPUT 396

Future of Cryptanalysis

- In theory, cryptographers are now stronger than cryptanalysts.
- In practice, messages are routinely intercepted.
- Peripheral attacks include keystroke recording, viruses, Trojan horses, and intentional backdoors.
- RSA depends on sufficiently large keys (2000 bits).
- Breaking RSA would requires a theoretical or technological breakthrough.

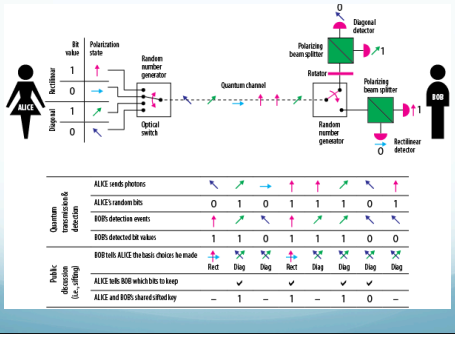
Quantum Mechanics

- Wave/particle duality of light
- Thomas Young's double slit experiment (1799)
- Quantum theory is counter-intuitive, but solid
- Quantum superposition principle
- Can we create quantum-based computers?
- Qubits = quantum bits
- Computations performed in multiple universes
- Operational quantum computers could destroy RSA

Quantum Money

- Stephen Wiesner's idea
- Measure photon polarization with Polaroid filters
- Heisenberg's uncertainty principle
- Assume there are only four polarizations: | — \ /
- The bank embeds photon traps in each bill.
- The forger cannot accurately measure the polarizations.
- But the bank can, because it knows the polarizations for each serial number.

Quantum Cryptography



Quantum Protocol

- Alice selects random filter and bit sequences
  - `filters: ++x+x++x+xxx+x`
  - `message: 11001101010111`
  - `photons: ||\-/|-/-/\/|/`
- Bob selects a random filter sequence
  - `filters: +xx+xx++++xxx+`
  - `photons: ||\-/|-/-/\/|/`
  - `outcome: 1?001?0?0?01??`
- Alice and Bob exchange and match filter sequences
  - `matched: + x+x + + xx`
  - `key:  1 001 0 0 01`
- message on matching filters is the key: **10010001**

Quantum Security

- Eve intercepts the transmissions between Alice and Bob
  - Eve measures the photon polarizations
  - Eve can correctly guess about 50% of the filters
  - Eve eavesdrops the phone calls between Alice and Bob
- Eve guesses a random filter sequence
  - `filters: xx++xx++x+x+x`
  - `photons: ||\-/|-/-/\/|/`
  - `detects: \/|--//--/|/|/`
  - `matched: + x+x + + xx`
  - `key:     1 001 0 0 01`
  - `guessed: 0 100 1 0 11`
- So, Eve correctly guessed about 50% of the key bits

Interception Detection

- Eve's measurements alter about 50% of the photons
- This results in about 25% of Bob's bits being wrong
- Alice and Bob can verify a sample of the key bits
  - `photons: ||\-/|-/-/\/|/`
  - `matched: + x+x + + xx`
  - `key:     1 001 0 0 01`
  - `sample:  .   .     .`
  - `Alice:   1   1     0`
  - `Bob:     1   0     1`
- Errors indicate that the photons have been intercepted