Fiber Optic Communications
Lecture 13: Quantum Cryptography

- Classical cryptography
- Quantum key distribution
Cryptography

• Encoding information for a targeted receiver, and obscuring it for all others
• Key distribution is a major challenge
• One approach: Algorithm (such as RSA) exchanges public keys and then uses public + private keys to encrypt information for correspondent
• Bruce force solution is NP-hard:

\[ T(n) = \exp[c(\ln n)^{1/3} (\ln \ln n)^{2/3}] \]
Cryptography

• RSA algorithm now used for most secure internet applications:
  – Public key infrastructure (PKI)
  – SSL/TLS: web certificates
  – Secure e-mail: PGP, GPG, Outlook, etc.
Cryptography Challenges

• Can brute force keys up to 768 bits with sufficient computational power
• With some luck, can cut length of brute force attacks by factors of millions
• As computational power increases, formerly ‘secure’ keys become easier to crack
• RSA algorithm also had a ‘backdoor’ associated with a pseudo-random algorithm (Dual_EC_DRBG) built in as a default
• Therefore, does not satisfy basic security conditions
Simple Attack on Textbook RSA

- Session-key $K$ is 64 bits. View $K \in \{0,\ldots,2^{64}\}$
  Eavesdropper sees: $C = K^e \pmod{N}$.

- Suppose $K = K_1 \cdot K_2$ where $K_1, K_2 < 2^{34}$ (prob. $\approx 20\%$)
  Then: $C/K_1^e = K_2^e \pmod{N}$

- Build table: $C/1^e, C/2^e, C/3^e, \ldots, C/2^{34}e$ . time: $2^{34}$
  For $K_2 = 0,\ldots, 2^{34}$ test if $K_2^e$ is in table. time: $2^{34} \cdot 34$

- Attack time: $\approx 2^{40} \ll 2^{64}$

Courtesy: Dan Boneh (Stanford University)
• Classical cryptography
• Quantum key distribution
Quantum Cryptography

• Here, concept is to use quantum mechanics to solve the key distribution problem
• Unconditionally secure algorithm BB84: proposed by Charles Bennett and Gilles Brassard in 1984.
• Once key is securely received, it can be used to encrypt messages transmitted by conventional channels.
BB84 Setup

- Both Alice and Bob have two polarizers each.
- One has a 0-90 degree basis ( + ), and one has a 45-135 degree basis ( × )

1) Alice uses her polarizers to send randomly photons to Bob in one of the four possible polarizations: 0, 45, 90, or 135 degrees

2) Bob uses his polarizers to measure each polarization of photons he receives. Can use the ( + ) basis or the ( × ) basis, but not both simultaneously.
BB84 Implementation

1. Alice
   - Laser
   - Unpolarized photon

2. Bob
   - Detection filter

3. Eve
   - Detection filter

Polarization filter

Transmitted photon

Alice's bit sequence: 0 0 1 0 1 0 1 1
Alice's filter scheme:  
Bob's detection scheme: + + + + x + + + +
Bob's bit measurements: 1 0 1 0 1 0 0 1 1
Retained bit sequence (key): — 0 — 0 1 — — 1 1
Eavesdropper Eve

• If Eve uses the filter aligned with Alice’s, she can recover the original polarization of the photon.
• If she uses the misaligned filter, she will receive no information about the photon.
• Also, she will influence the original photon and be unable to retransmit it with the original polarization (no-cloning theorem).
• Thus, Bob will be able to deduce Eve’s presence.
Security of quantum key distribution

• Quantum cryptography obtains its fundamental security from the fact that each qubit is carried by a single photon, and each photon will be altered as soon as it is read.

• This makes impossible to intercept message without being detected.
Disadvantages

• Susceptibility to noise: noise looks like an eavesdropping attack, since it degrades quantum coherence
Quantum one-way functions

• Consider a map $f: k \rightarrow |f_k\rangle$.
  – $k$ is the private key
  – $|f_k\rangle$ is the public key

• One-way function: For some maps $f$, it’s impossible (theoretically) to determine $k$, even given many copies of $|f_k\rangle$

• We can give it to many people without revealing the private key $k$
Commercial QC providers

- **id Quantique** (Geneva, Switzerland)
  - Optical fiber-based system
  - Tens of km

- **MagiQ Technologies** (New York City)
  - Optical fibers
  - Up to 100 km

- **NEC** (Tokyo): 150 kilometers

- **QinetiQ** (Farnborough, England)
  - Through the air: 10 kilometers.
  - Supplied system to BBN in Cambridge, MA
References