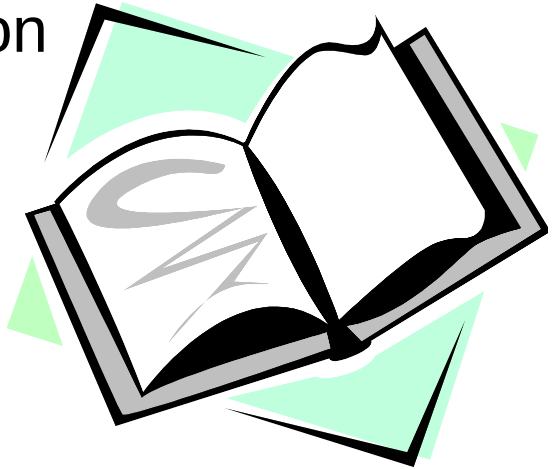
Cryptography
CS 555

Topic 25: Quantum Crpytography

Outline and Readings

- Outline:
  - What is Identity Based Encryption
  - Quantum cryptography
- Readings:



Identity Based Encryption

- Idea: Allow an arbitrary string (e.g., an email address) to be used as a public key
- Benefit: Easy to obtain authentic public key.
- Catch: Needs a Trusted Third Party (TTP).

- TTP publishes public parameters, and has master secret.
- A user can register with the TTP to obtain private key corresponding to an identity string.
- A sender can encrypt a message with public parameter and receiver's identity string.
- Exist constructions using parings (elliptic curves).
- TTP generates everyone's private key, and can decrypt anything.

- Quantum Cryptography
  - based on a survey by Hoi-Kwong Lo. http://www.hpl.hp.com/techreports/97/HPL-97-151.html
  - And on http://en.wikipedia.org/wiki/Quantum_key_distribution

Quantum Mechanics & Cryptography

- Quantum communication
  - Protect communication using principles of physics
- Quantum computing
  - Can efficiently solve some problems that are computationally infeasible for traditional computers to solve
    - e.g., Shor's efficient algorithm for factoring
  - Exploits quantum superposition and entanglement
    - N bits in classical computers can only be in one of 2^N states
    - N qubits can be in an arbitrary superposition of up to 2^N different states simultaneously
      - When measured, it collapse into one state with some probability
    - Quantum computers can compute with all states simultaneously

Properties of Quantum Information

- *Wave function collapse*
  - A superposition when measured by an observer, collapse to a specific state
  - Measurement of a signal changes it
- A quantum state is described as a vector
  - e.g., a photon has a quantum state,
  - quantum cryptography often uses photons in 1 of 4 polarizations (in degrees): 0, 45, 90, 135

Encoding 0 and 1 under two basis

Basis	0	1
+ (rectilinear)	↑	→
× (diagonal)	↗	↘

Properties of Quantum Information

- No way to distinguish which of ↗↑→↘ a photon is
- Quantum “no-cloning” theorem: an unknown quantum state cannot be cloned.
- Measurement generally disturbs a quantum state
  - one can set up a rectilinear measurement or a diagonal measurement
    - a rectilinear measurement disturbs the states of those diagonal photons having 45/135
- Effect of measuring

Basis	↑	→	↗	↘
+	↑	→	↑ or →	↑ or →
×	↗ or ↘	↗ or ↘	↗	↘

Quantum Key Agreement

- Requires two channels
  - one quantum channel (subject to adversary and/or noises)
  - one public channel (authentic, unjammable, subject to eavesdropping)
    - Protocol does not work without such a channel

The Protocol [Bennet & Brassard'84]

1. Alice sends to Bob a sequence of photons, each of which is chosen randomly and independently to be in one of the four polarizations
   - Alice knows their states

2. For each photon, Bob randomly chooses either the rectilinear based or the diagonal base to measure
   - Bob record the bases he used as well as the measurement

The Protocol [Bennet & Brassard'84]

3. Bob publicly announces his basis of measurements
4. Alice publicly tells Bob which measurement basis are correct and which ones are not
   - For the photons that Bob uses the correct measurement, Alice and Bob share the same results

See the following page for an example:

http://en.wikipedia.org/wiki/Quantum_key_distribution

The Protocol [Bennet & Brassard'84]

5. Alice and Bob reveal certain measurement results to see whether they agree
   - to detect whether an adversary is involved or the channel is too noisy

- Why attackers fail
  - Any measurement & resending will disturb the results with 50% probability

Additional Steps

- Information reconciliation
  – Figure out which bits are different between Alice and Bob
  – Conducted over a public channel
- Privacy amplification
  – Reducing/eliminating Eve's partial knowledge of a key

Coming Attractions …

- Review of some HW/Quiz questions