

# Cryptography CS 555

## Lecture 23



## Quantum Cryptography

# Review

- Perfect secrecy (definition, limitations)
- One-time pad
- Stream ciphers
  - fundamental weaknesses
  - RC4, WEP weaknesses
  - LFSR, CSS weaknesses
- PRNG (property)

# Review

- Block ciphers
  - ideal block ciphers
  - Feistel network, DES construction
  - DES cryptanalysis
  - encryption modes: ECB, CBC, CFB, OFB, CTR
  - multiple encryption (2DES, 3DES)
  - PRFs, PRPs
  - AES, IDEA (parameters)

# Review

- Notions of security
  - adversarial objectives: key recovery, plaintext recovery, distinguishing
  - adversarial modes: ciphertext only, known plaintext, (adaptive) chosen plaintext, (adaptive) chosen ciphertext
- Cryptographic hash functions
  - three security properties (their relationships)
  - Iterated construction, Merkle-Damgard
  - MD5, SHA-1, SHA
  - Birthday attacks

# Review

- Message Authentication Code
  - security objectives (non-existence of  $(x,y)$  forger)
  - constructions from hash functions, HMAC
  - constructions from block ciphers, CBC-MAC
  - strongly universal hash families
- Number theory
  - Extended Euclidian algorithm, Chinese remainder theorem, Euler Phi, Fermat's theorem, primality testing, etc.
  - See Dan Boneh's notes

# Review

- Security notions of public key encryption
  - KR-, PR-, IND-, NM-, CPA, CCA, CCA2
- RSA encryption
  - algorithm, attacks, factoring, equivalence of factoring  $n$ , computing  $\Phi(n)$ , and computing  $d$  and  $e$
- Rabin encryption
  - proof of security, attacks
- Goldwasser-Micali
- Padding Scheme, OAEP
- Discrete Log, CDH, DDH, El Gamal

# Review

- Digital signatures
  - security properties, RSA, El Gamal, DSA, Schnorr, Lamport, Merkle, blind signatures,
  - undeniable signatures
- Public key certificates
  - X.509, certification revocation
- Entity authentication
  - passwords, salting, one-time passwords, challenge-response
  - Zero knowledge: properties, Fiat-Shamir, Schnorr, convert to non-interactive and signatures

# Review

- Key establishment protocols
  - properties:
  - AKEP2, using MAC, encryption, Needham-Schroeder secret-key based, public-key based
  - Diffie-Hellman, authenticated Diffie-Hellman
- Secure multiparty computation
  - Oblivious transfer, Scrambled circuit
  - Secret sharing,

- # Quantum Cryptography

- lecture prepared based on a survey by Hoi-Kwong Lo.  
<http://www.hpl.hp.com/techreports/97/HPL-97-151.html>

# Quantum Mechanics & Cryptography

- Quantum communication
  - protecting communication using principles of physics
- Quantum computing
  - building quantum computers
  - developing quantum algorithms
    - e.g., Shor's efficient algorithm for factoring

# Properties of Quantum Information

- *Heisenberg Uncertainty Principle (HUP)*
  - If there is a particle, such as an electron, moving through space, it is impossible to measure both its position and momentum precisely.
- 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

# Properties of Quantum Information

- 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

# Quantum Key Agreement

- Requires two channels
  - one quantum channel (subject to adversary and/or noises)
  - one public channel (authentic, unjammable, subject to eavesdropping)

# 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
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 measurements are correct and which ones are not correct
  - For the photons that Bob uses the correct measurement, Alice and Bob share the same results

# The Protocol [Bennet & Brassard'84]

5. Alice and Bob reveals certain information about the shared bits to see whether they agree
  - to detect whether an adversary is involved or the channel is too noisy

# Summary

- Quantum key agreement



# Next Lecture...

- Biometrics

