Ph 452 Lecture 27

Classical Cryptography: Security conditional on computational assumption.

Quantum Cryptography: Digital fingerprints (cryptographic hash fn).

Digital signatures (sign/verify), Secret Sharing, Data Hiding, Coin Tossing.

One-time pad (Vernam cipher).

Alice

Key

Bob

Shared random bits

Message

101101

Public key

100110

Ciphertext

110010

Plain text

101101

Channel

\[ \oplus \]

Key

101101

Message

Idea: random + message = random.

Causes:

1. Need to distribute key securely.
2. Need to guard key once distributed.
3. Can only use key once.

Solution to 1? (and 2)

Quantum Key Distribution (QKD)

Idea: Key sent using nonorthogonal states.

(States decoded by POVM with (some) non-commuting operations."

\[ \text{EC recovery see book} \]

\[ \text{1A1 Wiki: Sign-up: Dec 6 or Dec 11} \]

\[ \text{No more PS, Best 5/6: total points} \]

\[ \text{EC: 53 total possible} \]
Lecture 27

**BB84 Protocol** (Bennett, Brassard 1984)

Idealization: Eavesdropper cannot choose signals on public classical channels.

**Quantum Phase**

- **Random Basis**: \( |0\rangle, |1\rangle, |+\rangle, |\tilde{+}\rangle, |-\rangle, |\tilde{-}\rangle \)

**Message**: 0 1 0 1 1

**Ciphertext**: 0 2 1 \(\rightarrow\) 1 \(\rightarrow\) 1 \(\rightarrow\) 1 \(\rightarrow\) (Public Quantum Channel)

**Ciphertext**: 1 0 1 \(\rightarrow\) 1 \(\rightarrow\) 1 \(\rightarrow\) 1 \(\rightarrow\) (Public Classical Channel)

**Basis (Distillation)**

**Basis Revealed**: 0/1, +/\(\tilde{+}\), 0/1, +/\(\tilde{+}\)

**Sifting**

**Classical Basis**

**Eavesdropper Testing**

**Fraction p of sifted bits sent**

**Key**: 0 1 1

**NB**: Bob's measurement is PoVM \( E_{0} |0\rangle x |0\rangle, E_{1} |1\rangle x |1\rangle, E_{i} |i\rangle x + |i\rangle, E_{\tilde{i}} |i\rangle x + |\tilde{i}\rangle \)
Why idealization? “Man-in-the-middle attack” — key lost AE ≠ EB indeed.

Alice  Eve  Bob

\[
\begin{array}{c}
011 \\
\rightarrow \\
011 \\
\rightarrow \\
011
\end{array}
\]

Solution: Authentication: AB share \(\log \log |M|\) bits,

where \(|M|\) = size of message space to be authenticated

\[\rightarrow \text{makes prob (faking authentication)} \sim e^{-\text{message}}\]

Composability: Distributed key can authenticate future QKD rounds.

Q: How to establish Authentication key securely?

A: James Bond.

QKD is really QK Expansion.

Other protocols:

Ekert91: AB share many copies of \[\frac{1}{\sqrt{2}}(101+111) = \frac{1}{\sqrt{2}}(111-100)\]

Verify by sacrificing function + measuring stabilizer \((XX, ZZ)\)

\[\text{Key cannot be cloned - no need to guard!} \]

\[\text{If A measured bit puts first \# and B sends to Bob \# Sameras BB84!}\]

BB92: Like BB84 but A sends 0 or 1+ for 0 or 1

6-state: Like BB84 but \(\# 6\) states used.

EPR: @ A, B prepare \((011)\) or \((1+)\) and send to C.

\[\text{C measures } \overline{XX} \text{, announces outcome}\]

\[\text{A, B announce bases, test for eavesdroppers}\]

\[\rightarrow \text{Allows 3rd (untrusted) party to hold the ebits.}\]
How to remove idealization 2: Noisy channels

"Seems impossible — any noise has to be chalked up to meddling"

Solution: Use QECCs: {\(0\), \(1\), \(\cdot\), \(\cdot\), \(\cdot\), \(\cdot\)}.

QEC restores errors, expels correlations Eve may have (no-cloning bound).

Problem: QEC hard to implement technologically.

Solution: Shor-Preskill [2000]: Equivalent to extracting classical phase of BB84:

\[
\begin{array}{ll}
\text{Classical error-corrected} & \\
\text{Information reconciliation} & \\
\end{array}
\]

\[
\begin{bmatrix}
0 & 1 & 1 \\
\end{bmatrix} = \bar{1}
\]

\[
\begin{bmatrix}
1 & 1 & 1 \\
\end{bmatrix} = \bar{1}
\]

General string, e.g.,

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 1 \\
\end{bmatrix}
\]

Private amplification: \(\bar{1} = \text{parity}(00101)\)

\(\bar{1} = \text{parity}(10010)\)

Analysis: key rate \(r = \frac{\text{#shared key bits}}{\text{#sifted key bits}} = 1 - 2 \cdot H_2(\text{error})\)

\[H_2(p) = -p \log_2 p - (1-p) \log_2 (1-p)\]

\(r > 0 \text{ for } P_{\text{err}} \leq 1/2\)

\(P_{\text{err}} = \max \{P_x, P_z\}^3\)

Can be boosted to \(P_{\text{err}} \leq 2/3\) [Gottesman-Lo, 2003]
Security: How do AB know that p(c|x)?

Statistical sampling - tricky part of security proof

Security statement: QKD strict secure to all attacks by Eve subject to the following restrictions:

1. Eve obeys QM
2. Eve only has access to all signals btw AB
   (e.g., not sending/detecting devices)
   ("Subtle in Q. optical implementations as optical channel provides path right to the devices")

Called "Unconditionally Secure" b/c no conditions on computational power of Eve made. ("The obviously
   (w/ no conditions"

Got this far

Attack types:

"Coherent": Most general
"Individual": Eve attaches a probe/signal & measures probe
"Collective": "' ' ' ' ' ' ' ' ' ' ' all probes collectively.

BB84 attack conjecture: collective attacks are optimal."
Realistic optical QKD: (BB84)

Single-photon polarization:

\[ |0, 1\rangle : \uparrow \leftrightarrow \text{polarization} \quad \text{spin-1 particle}, \]

\[ |+,-\rangle : \uparrow, \downarrow \text{polarization} \quad \text{spin-1 particle}, \]

\[ \mathcal{U}(\vec{n}, \vec{0}) = e^{-i \vec{n} \cdot \vec{0}} \]

Problem: No single-photon sources (yet).

Attenuated laser pulse:

\[ P = e^{-M} \sum_{n=0}^{\infty} \frac{M^n}{n!}, \quad |n\rangle < |m| \]

\[ |n\rangle = n\text{-photon state} \]

\[ M = \text{average photon #}/\text{signal} \quad (M=0.1 \Rightarrow 0.5\% \text{ signals have } >1 \text{ photons}) \]

Problems:

A sends \( |0\rangle \): B sees nothing (reduces key rate) \[ P = e^{-M} \]

A sends \( |1\rangle \): Works like BB84 \[ P = Me^{-M} \]

A sends \( |n\rangle \): E can do photon number splitting (PNS) attack \[ P = 1 - (1-n)e^{-M} \]

PNS attack: E asks: "What is n?" (not "What is polarization?")

IF \( n \neq 2 \), send n to B, keep 1

When A reveals basis, E gets a copy of B's bit.

If \( n = 2 \), block same function so B sees expected Poisson distribution

AB solution: Can increase EC, PA to account for this

QKD exist commercially!

Current work: increasing key rates w/better protocols

Improving sources, detectors,