QEC recovery-see book
IQI Wiki: Signup: Dec 6 or Dec 11
No more PS. Best 5/6 : $\frac{\text{total points}}{\text{total possible}}$
EC: 5%

$\boxed{\text{Ph 452}}$ Lecture 27

Classical Cryptography: Security conditional on computation assumption.

Taking Given

Quantum Cryptography: Digital fingerprints (cryptographic Hash fn)
Digital signatures (sign/verify), Secret Sharing, Data Hiding, Coin Tossing

One-time pad / Vernam cipher:

| | Alice | | Bob | |
|---|---|---|---|---|
| Solution's bits | | Shared random bits ($\longleftrightarrow$ ("key")) | | |
| key | 011101 | | 011101 | |
| solution | message $\oplus$ 101101 | public channel $\longrightarrow$ | | |
| ciphertext | 110010 | | 110010 | ciphertext |
| | | | $\oplus$ 011101 | key |
| | | | 101101 | message |

Idea: random + message = random

Very easy to decide if revised. → Caveats: 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)

Not just "Eve disturbs by measuring" b/c Bayesian collapse is a thing.

- Idea: Key sent using nonorthogonal states
(States decoded by POVM with (some) non-commuting operations)

Ph450 Lecture 27

## BB84 protocol: (Bennett, Brassard 1984)

use colored chalk.

Idealization: ① Eavesdropper cannot change signals on public classical channels.
② Noiseless communication.

| QUANTUM PHASE | Alice | | Bob |
|---|---|---|---|
| random | 0 1 1 0 1 | | |
| basis | $\lvert 0/1\rangle, \lvert\pm\rangle, \lvert\pm\rangle, \lvert 0/1\rangle, \lvert\pm\rangle$ | | |
| Message | 0 1 0 1 1 | | |
| encode ciphertext | $\lvert 0\rangle \lvert -\rangle \lvert +\rangle \lvert 1\rangle \lvert -\rangle$ | $\xrightarrow[\text{channel (PQC)}]{\text{public quantum}}$ | $\lvert 0\rangle \lvert -\rangle \lvert +\rangle \lvert 1\rangle \lvert -\rangle$ ciphertext |
| | | | $\lvert 0/1\rangle \lvert 0/1\rangle \lvert\pm\rangle \lvert 0/1\rangle \lvert\pm\rangle$ basis (Don't solicit, fix 3) |
| | | | $\lvert 0\rangle \lvert ?\rangle \lvert +\rangle \lvert 1\rangle \lvert -\rangle$ measure |
| CLASSICAL PHASE | | $\xleftarrow[\text{(PCC)}]{\text{Public Classical Channel}}$ | "n bits received & measured" Ack |
| basis revealed | "0/1, ±, ±, 0/1, ±" | $\xrightarrow{\text{PCC}}$ | "0/1, ±, ±, 0/1, ±" |
| | "0/1, 0/1, ±, 0/1, ±" | $\xleftarrow{\text{PCC}}$ | "0/1, 0/1, ±, 0/1, ±" basis revealed (could just send locations of agreement) |
| sifting (Eve could do this) (lose 50%) | 0 X 0 1 1 | | 0 X 0 1 1 |
| eavesdropper testing | "0 (random fraction p of sifted bits sent)" | $\xrightarrow{\text{PCC}}$ | "0" |
| | | $\xleftarrow{\text{PCC}}$ | "All ok / something didn't match, we're being eavesdropped" |
| Key: | $\boxed{0\ 1\ 1}$ | | $\boxed{0\ 1\ 1}$ |

N.B: Bob's measurement is POVM $\{\frac{1}{4}|0\rangle\langle 0|, \frac{1}{4}|1\rangle\langle 1|, \frac{1}{4}|+\rangle\langle +|, \frac{1}{4}|-\rangle\langle -|\}$.

Ph452 Lecture 27

Why idealization (1): "Man-in-the-middle attack": Key btw AE & EB instead.

Alice — Eve — Bob

$\boxed{011} \longleftrightarrow \boxed{011} \longleftrightarrow \boxed{011}$

Solution: <u>Authentication</u>: AB share $\log\log|M|$ bits,

where $|M|$ = size of message space to be authenticated

Don't have enough info to theory of quantum info

→ makes prob (faking authentication) $\sim e^{-|\text{message}|}$

<u>Composability</u>: Distributed key can authenticate future QKD rounds

Q: How to establish Authentication key securely?

A: James Bond.

QKD is really <u>Q.K Expansion.</u>

---

Other protocols: [2,0] code

Ekert91: AB share many copies of $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle-|--\rangle)$

mention first

∴ Verified by sacrificing fraction & measuring stabilizer (XX, ZZ)

→ Key cannot be cloned – no need to guard!

Too fast!

∴ If A measured both parts first & sent B parts to Bob ⇒ same as BB84!

B92: Like BB84 but A sends $|0\rangle$ or $|+\rangle$ for 0 or 1

6-state: Like BB84 but 6 states used.

time-reversed EPR: ① A, B prepare $|011\rangle$ or $|1\pm\rangle$ and send to C.

② C measures ZZ, XX, & announces outcome

③ A, B announce bases, test for eavesdroppers

→ Allows 3rd (untrusted) party to hold the qubits.

Ph 452 Lecture 27

How to remove idealization 2: Noisy channels

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

Solution: Use QECCs: $|\bar{0}\rangle, |\bar{1}\rangle, |\bar{+}\rangle, |\bar{-}\rangle$.

Could formalize w/ mutual info

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

Problem: QEC hard to implement technologically

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

$\boxed{0\ 1\ 1}$ ——— $\boxed{0\ 1\ 1}$

Classical error correction (EC) "information reconciliation"

$\boxed{1\ 1\ 1} = \bar{1}$ $\qquad$ $\boxed{1\ 1\ 1} = \bar{1}$

General string, e.g.

$\bar{1}\bar{0}\bar{0}\bar{1}\bar{0}\bar{1}$ $\qquad$ $\bar{1}\bar{0}\bar{0}\bar{1}\bar{0}\bar{1}$

privacy amplification (PA)

$\bar{\bar{1}} = \text{parity}(100101)$ $\qquad$ $\bar{\bar{1}} = \text{parity}(100101)$

(parity of random subsets of size $m$ – a security parameter)

Analysis: Key rate $r = \frac{\#\text{ shared key bits}}{\#\text{ sifted key bits}} = 1 - 2H_2(p_{err})$

$$H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$$

$$\boxed{r > 0 \text{ for } p_{err} \lesssim 11\%!}$$

$p_{err} = \max\{p_x, p_z\}$

Can be boosted to $p_{err} \lesssim 20\%$ [Gottesman-Lo, 2003]

Ph 452 Lecture 27

Security: How do AB know that $p < 1/8$?

Statistical sampling → tricky part of security proof

Security statement: QKD 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/detection 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. ("Tho obviously ① + ② are conditions")

Got this far

Attack types:

"Coherent": Most general
"Individual": Eve attaches 1 probe/signal & measures probe
"Collective": " " " " " " " all probes collectively.

BB84 attack conjecture: collective attacks are optimal.

Ph452 Lecture 27

## Realistic optical QKD: (BB84)

Single-photon polarization:

$|0,1\rangle$ : $\updownarrow, \leftrightarrow$ polarization } spin-1 particle,

$|+,-\rangle$ : $\swarrow, \searrow$ polarization }

$$U(\hat{n},\theta) = e^{-i\theta\hat{n}\cdot\vec{\sigma}}$$

Problem: No single-photon sources (yet).

Attenuated laser pulse:

$$\rho = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|$$

$|n\rangle$ = n-photon state

$\mu$ = average photon #/signal ($\mu=0.1 \Rightarrow$ 0.58 signals have $\geq 2$ photons)

Problems:

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

A sends $|1\rangle$ : works like BB84 $[p = \mu e^{-\mu}]$

A sends $|n\rangle, n\geq 2$ : E can do photon number splitting (PNS) attack! $[p = 1-(1-\mu)e^{-\mu}]$

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

If $n\geq 2$, send n-1 to B, keep 1

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

If $n=1$, block some fraction 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.