

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%

**Ph 452 Lecture 27**

Classical Cryptography: Security conditional on computation assumption.

Taketai Given

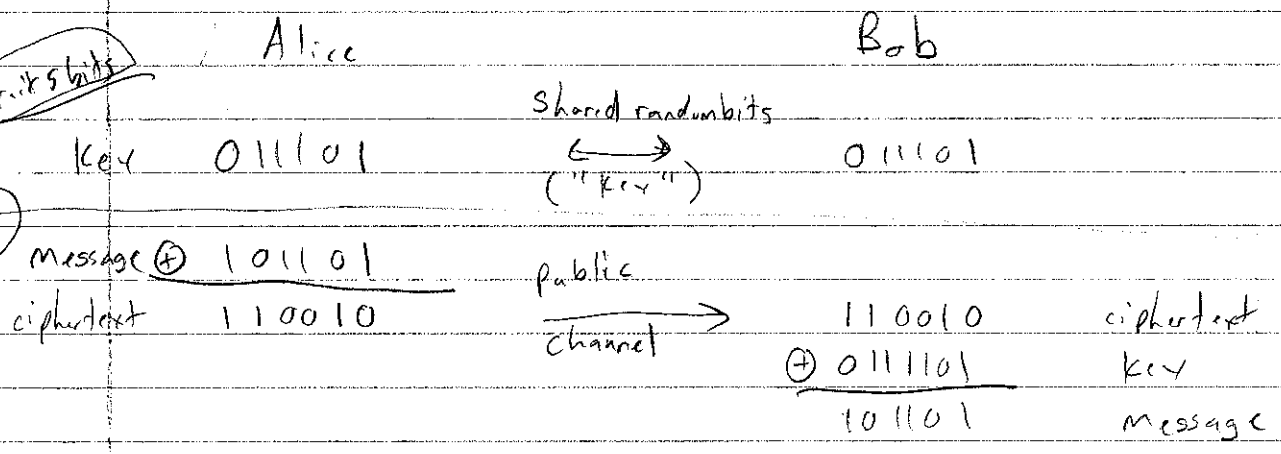
Quantum Cryptography: Digital fingerprints (Cryptographic Hash fn)

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

One-time pad / Vernam cipher:

Subtract 5 bits

90 bits



Idea: random + message = random

Very easy to decode if revealed.

- 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 doesn't

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

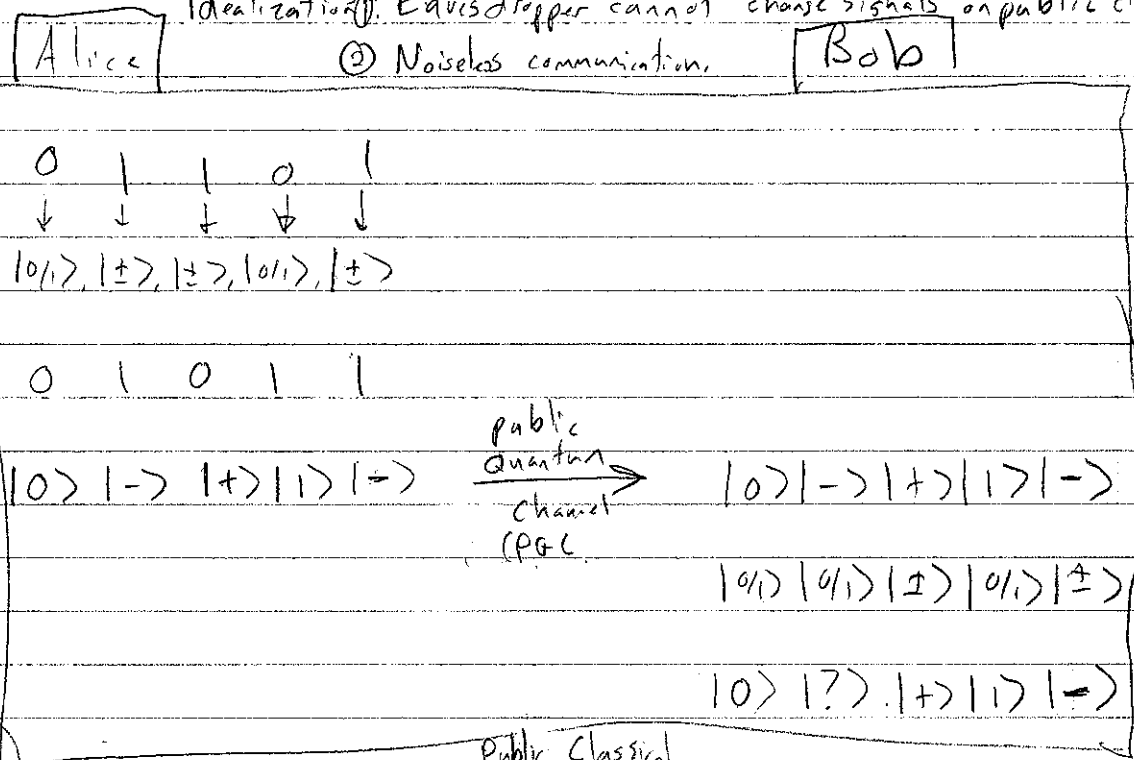
Phys 27 Lecture 27

BB84 protocol: (Bennett, Brassard 1984)

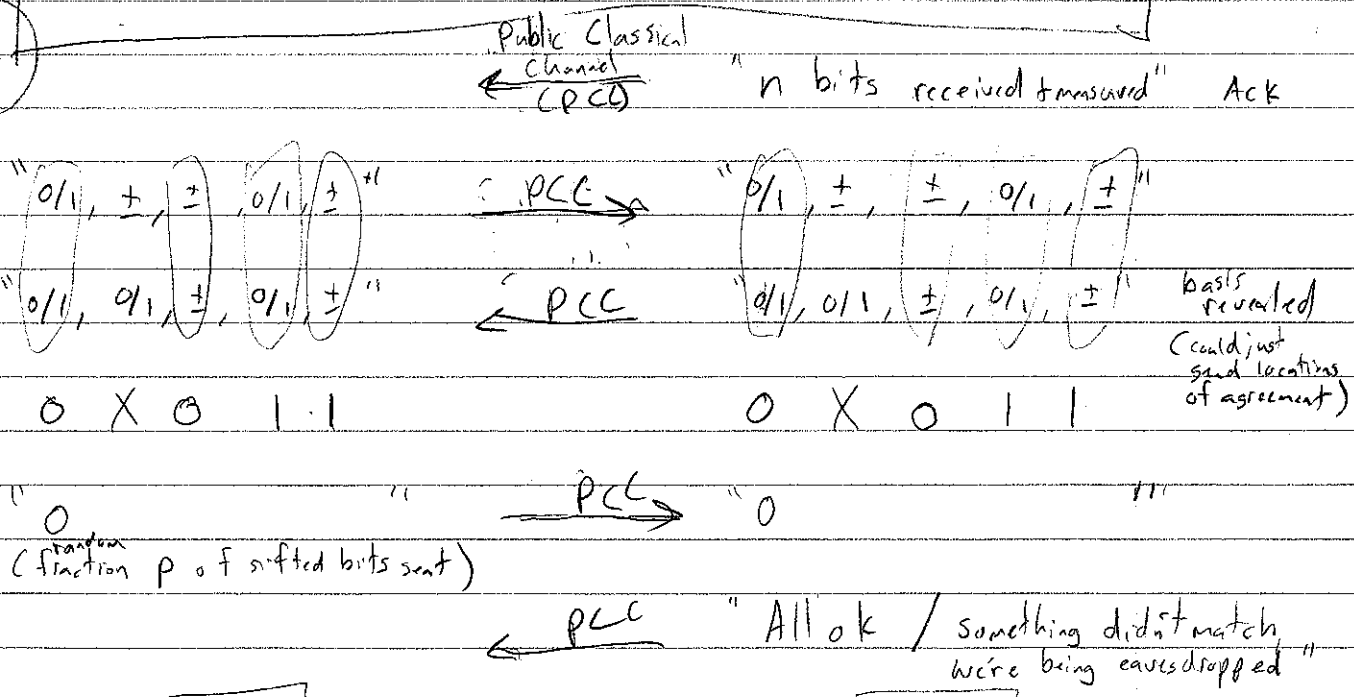
Idealization: Eavesdropper cannot change signals on public classical channels.

Noiseless communication.

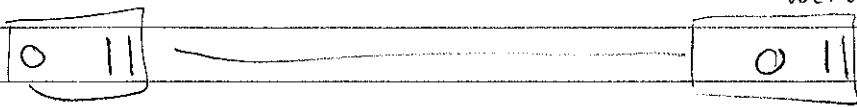
use colored chalk  
**QUANTUM PHASE**



**CLASSICAL PHASE**



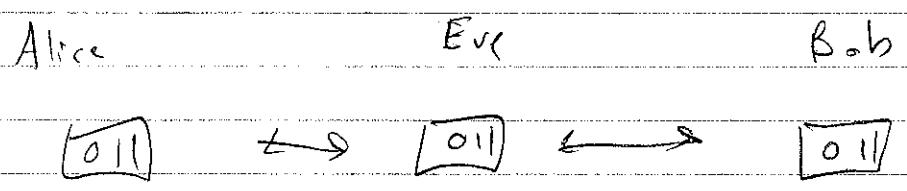
Key:



N.B: Bob's measurement is POVM  $\{\frac{1}{4}|0x0\rangle, \frac{1}{4}|1x1\rangle, \frac{1}{4}|+x+\rangle, \frac{1}{4}|-\times-\rangle\}$ .

# PH452 Lecture 27

Why idealization: "Man-in-the-middle attack": Key btw AE + EB instead.



Solution: Authentication: AB share  $\log \log |M|$  bits,

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

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

Don't have enough info to verify quantity

Composability: Distributed key can authenticate future QKD rounds

Q: How to establish Authentication key security?

A: James Bond.

QKD is really QK Expansion.

Other protocols:

$(2,0)$  code

Ekert 91: AB share many copies of  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

• Verified by sacrificing fraction + measuring stabilizer (XX, ZZ)

→ Key cannot be cloned - no need to guard!

• 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

G-state: Like BB84 but 6 states used.

measuring first

Too fast!

Time-reversed EPR: ① A, B prepare  $|01\rangle$  or  $|1\rangle$  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.

Ph452 Lecture 27

How to remove idealization 2: Noisy channels

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

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

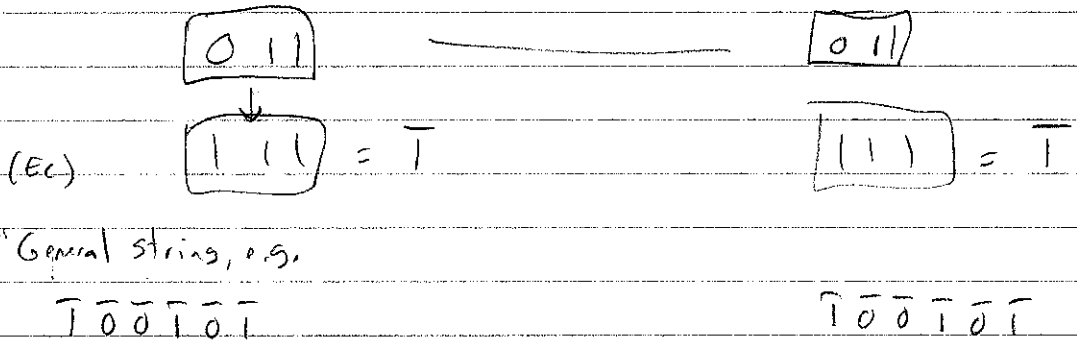
could formalize w/ mutual info

QEC restores errors, expels correlations Eve may have (non-cloning bound)

Problem: QEC hard to implement technologically

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

Classical error correction (EC) "information reconciliation"



privacy amplification (PA)

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

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

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

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

$r > 0$  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  $\rightarrow$  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. ("The obviously  $\text{Q} + \text{Q}$  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:

$$\begin{array}{l}
 |0,1\rangle : \downarrow, \leftrightarrow \text{ polarization} \\
 |+, -\rangle : \nearrow, \searrow \text{ polarization}
 \end{array}
 \left. \vphantom{\begin{array}{l} |0,1\rangle \\ |+, -\rangle \end{array}} \right\} \text{spin-1 particle,}$$

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

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.