Announcement:

- THIS THURSDAY (24^{th} Oct): 1) BRING LAPTOPS
  2) HANDOUT TAKE-HOME ASSIGNMENTS 1. (THA-1)

- NEXT MONDAY (28^{th}): OFF

- NEXT THURSDAY (31^{ST}): CONSULTATIONS RE. (THA-1) & OTHER.

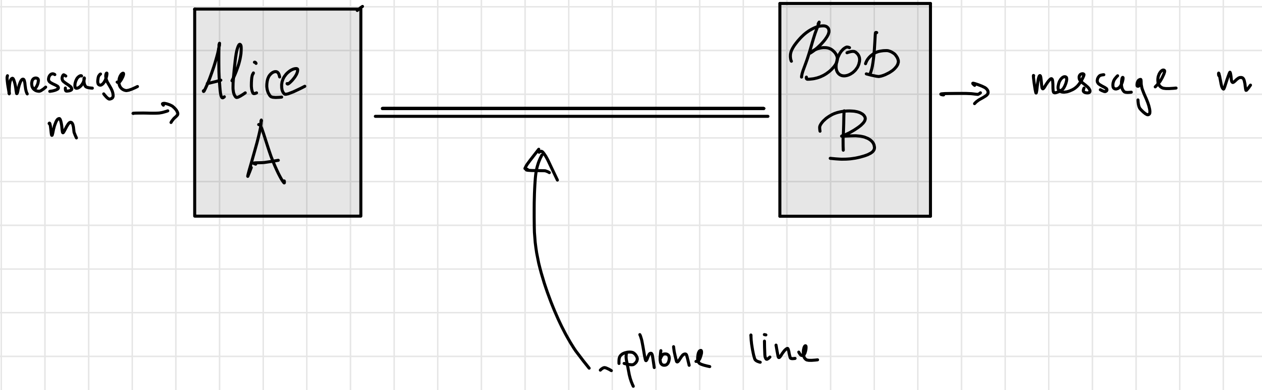
TODAY: - BASICS OF Q-CRYPTO, ESP. QUANTUM KEY DISTRIBUTION OF Bennet, Brassard '84.

- Mathematical formalism of quantum information theory (applied)

LITERATURE:

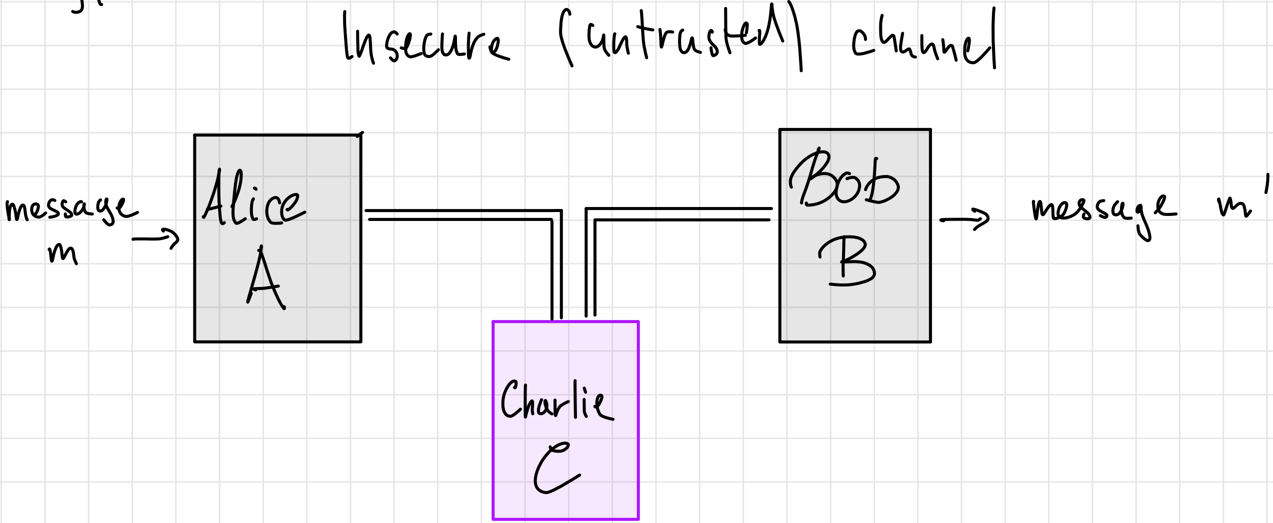
- N & C
- "GUIDE TO MATHEMATICAL CONCEPTS OF QUANTUM THEORY"
  Heinosaari, Ziman; arXiv: 0810.3536
- "CRYPTOGRAPHIC SECURITY OF QUANTUM KEY DISTRIBUTION"
  PORTMANN, RENNER; arXiv: 1409.3525
- "A LARGELY SELF-CONTAINED AND COMPLETE SECURITY PROOF OF QUANTUM KEY DISTRIBUTION"
  TOMAMICHEL, LEVERRIER; arXiv: 1506.08458

Crypto 101.



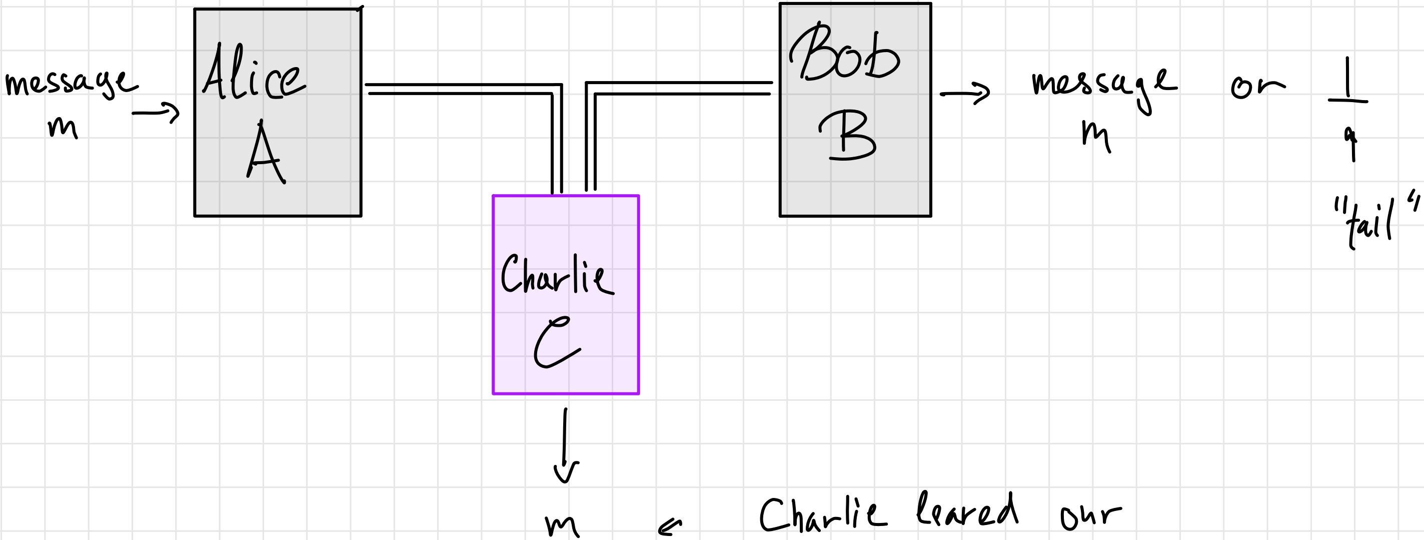
- phone line
- letter
- internet (email)

Crypto 101.


Insecure (untrusted) channel
message m
Alice
A
Bob
B
message m'
Charlie
C

Crypto 101.

Types of "security" : <u>authentication</u>



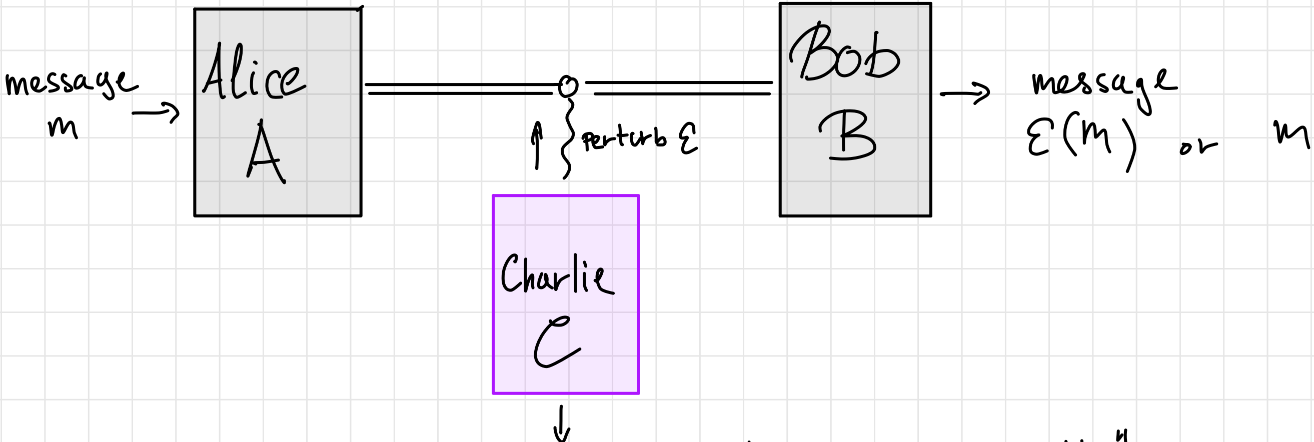
$\Leftarrow$ Charlie leared our secrets... but didn't perturb.

→ message authentication (MA code, MAC)

→ digital signatures

Crypto 101.

Types of "security" : <u>confidentiality</u>



m'

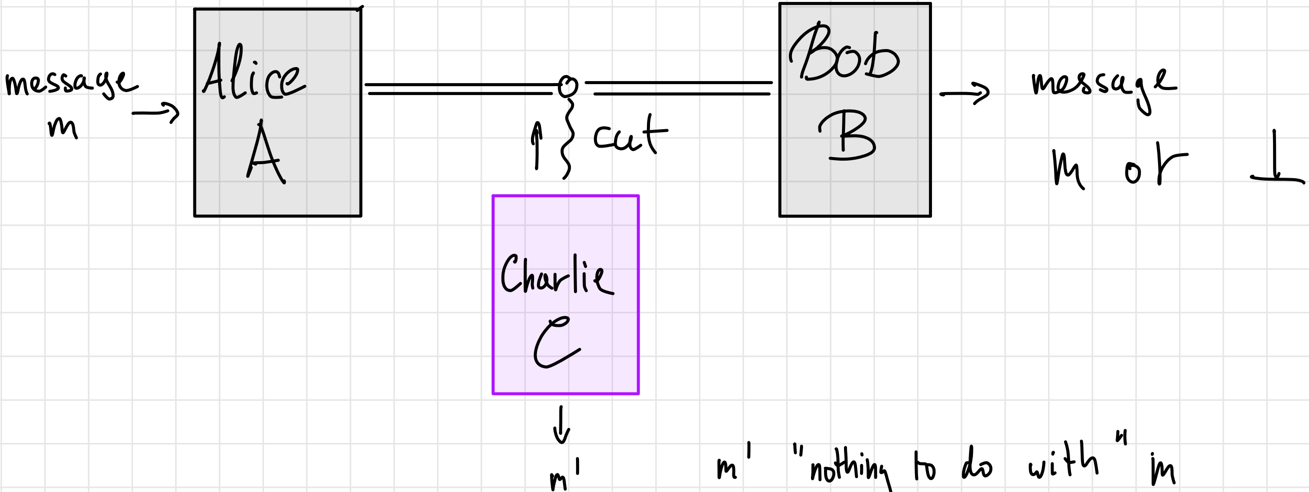
m' "nothing to do with" m

learns nothing, but can perturb

- RSA
- Vernum cypher, one-time pad

Crypto 101.

Types of "security": <u>secure channel</u>



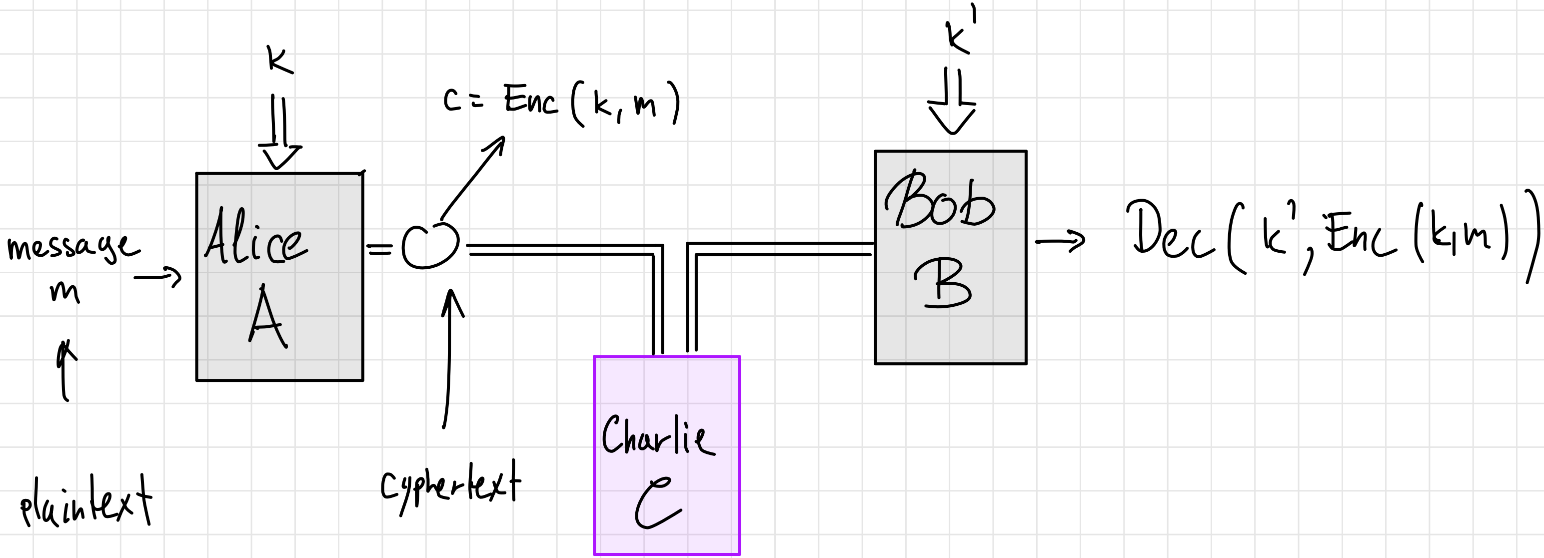
m' "nothing to do with" m

learns nothing, but can perturb

"encrypt and sign"

Crypto 101.

How ? ENCRYPTION



How secure; • Computational security, (public, private) key

Hard to compute private from public (Factoring)

• information-theoretic security! shared keys.

"One - time pad"

INFORMATION THEORETIC SECURITY

$m =$ one bit $\nearrow m=0$, $\searrow m=1$

key : random bit k, shared by A & B

$$c = Enc(k,m) = k \oplus m$$

$$Dec(k',c) = k' \oplus c$$

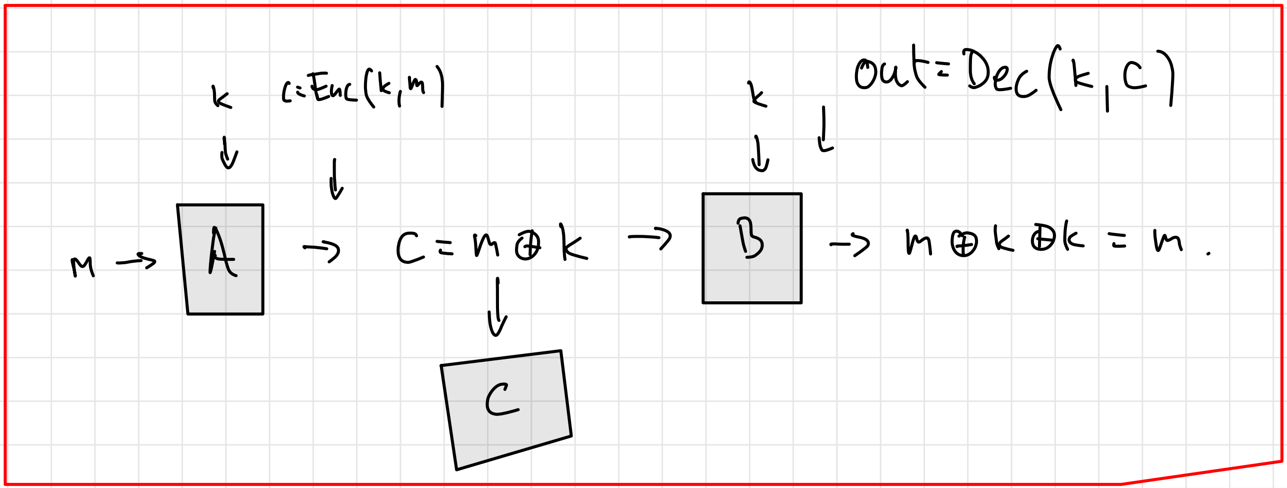
$$Dec(k', Enc(k,m)) = k' \oplus k \oplus m$$

IF $k = k' \Rightarrow Dec(k', Enc(k,m)) = m$.

"correct."

$$\begin{tikzcd}
 & k \arrow[d] & & k \arrow[d] & \\
m \arrow[r] & \boxed{A} \arrow[r] & c = m \oplus k \arrow[r] \arrow[d] & \boxed{B} \arrow[r] & m \oplus k \oplus k = m. \\
 & & \boxed{C} & &
\end{tikzcd}$$

Intuition; c has "nothing to do" with m anymore



A (cryptographic) protocol

- Players
- Inputs & outputs
- what they use & do

PRECISELY: OTP = (A, B, C; insecure channel, shared key; Enc, Dec)

What does "security" or "confidentiality" mean?

MAKING IT <u>FORMAL</u>

$P_C(m)$ - his prior knowledge

definition of security

$$\boxed{\text{"secure" if } P_C(m \mid C) = P_C(m)}$$

Claim IF $P_C(k)$ = uniform. then

OTP is <u>secure</u>

Next: Security proof (most important part...)

$$P_c(M=m)$$

$$P_c(M=m \mid C=c) = \frac{P_c(M=m, C=c)}{P_c(C=c)} \overset{(1)+(2)}{=} \frac{\frac{1}{2}P(m)}{1/2} = P(m)$$

$$P_c(c) = P(m \oplus K) = \frac{1}{2}P(m \oplus 1) + \frac{1}{2}P(m)$$

$$= \frac{1}{2}(1-P(m)) + \frac{1}{2}P(m) = \frac{1}{2}. \quad (1)$$

$$P(m,c) = \sum_k P(k)\,P(m,c \mid k) = \frac{1}{2}P(m,c \mid k=0) + \frac{1}{2}P(m,c \mid k=1)$$

$$= \frac{1}{2}P(m,m) + \frac{1}{2}P(m, 1 \oplus m) = \frac{1}{2}P(m) + 0 = \frac{1}{2}P(m) \quad (2)$$

Many bit message = many bit key... point-wise xor.

How many? Entropy of message distribution...

For uniformly random messages = # bits

Shannon:

Entropy <=> compressability

In short... Having pre-shared a fully random message in the past allows A & B to share n-bit confidential messages in the future.

But... can we share keys.. now?

"key distribution" problem,

Quantum key distribution = "Quantum" protocol for the distribution of classical keys

not QUANTUM keys...

QKD: Allows A & B to generate secure, private shared keys given:

- untrusted quantum channel
- authenticated classical channel

NOT KEYS FROM NOWHERE... AUTHENTICATED CHANNEL NOT INEXPENSIVE

Wegman - Carter: Auth. channel with failure prob $\frac{1}{2^k}$ given k bits

STILL Auth. much cheaper than confidential channel... indep from $\underline{\underline{n}}$.

Basic idea: ... measuring quantum systems in some state $|\psi\rangle$ perturbs it (unless $M = \{ |\psi_i\rangle \}_i$ & $|\psi\rangle = |\psi_i\rangle$ for some i)

... can detect if Charlie <u>listens</u>

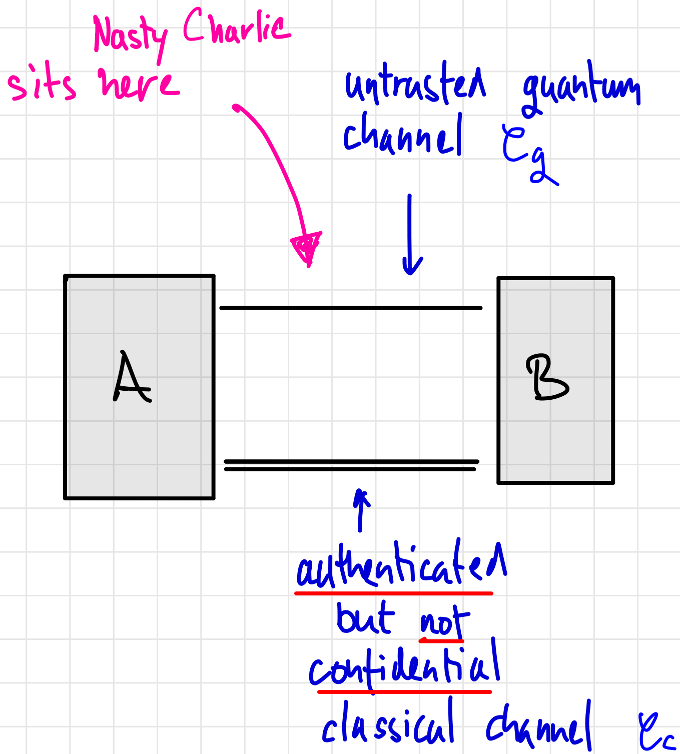
To do this properly need density matrix formalism to talk about <u>ignorance</u> about systems... Later.

For now

$$|0\rangle - \boxed{M = \{ |+\rangle, |-\rangle \}} \begin{cases} \nearrow \text{"}|+\rangle\text{"}, \frac{1}{2} \rightarrow |+\rangle & ✗ \\ \searrow \text{"}|-\rangle\text{"}, \frac{1}{2} \rightarrow |-\rangle & ✗ \end{cases}$$

$$|+\rangle - \boxed{M = \{ |+\rangle, |-\rangle \}} \longrightarrow |+\rangle \longrightarrow |+\rangle \quad ✓$$

Quantum key distribution
- the basics -



<u>Objective</u>:

Using : $\mathcal{E}_q$, $\mathcal{E}_c$, local randomness

Alice & Bob establish a

<u>shared key</u> $k = (k_1 \ldots k_n)$

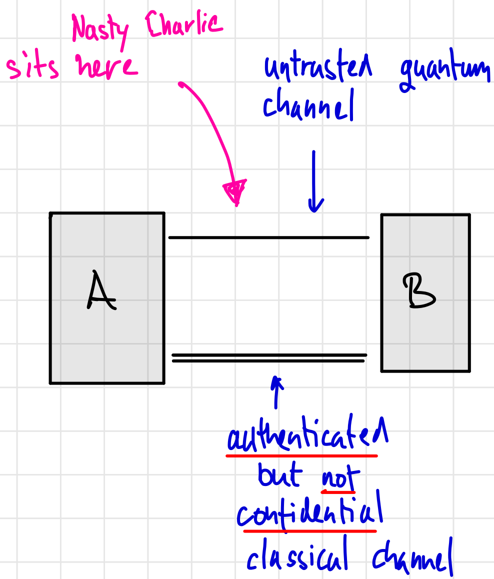
where each bit is uniform at random

& fully unknown to Charlie

$$P_c(k) = P_c(k \mid \text{all information exchanged})$$

or the protocol <u>ABORTS</u> . . .

Quantum key distribution
- the basics -



PROTOCOL QKD:

"QUANTUM PHASE"

A: 1) Chooses $2 \times n'$, $n' = (4+\delta)n$ random bits:

Local randomness easy(er)

$$\left\{ \left(i,\ \underset{\uparrow \text{"data"}}{b_i^1},\ \underset{\uparrow \text{"basis"}}{b_i^2}\right) \right\}_{i=1}^{n'}$$

2) Sends n' qubits to Bob

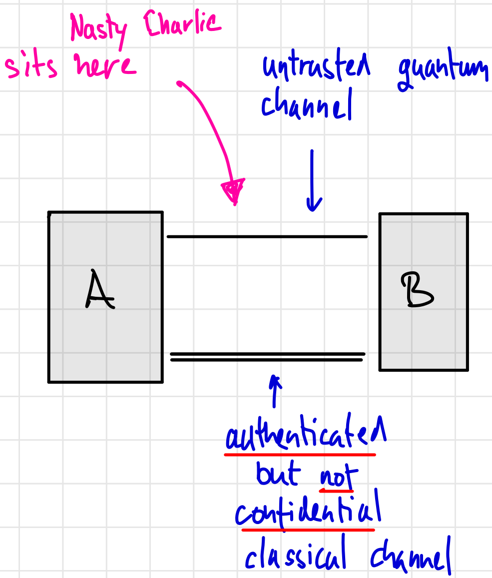
k^{th} qubit is in state

data \ basis	$b_k^2 = 0$	$b_k^2 = 1$
$b_k^1 = 0$	$\|0\rangle$	$\|+\rangle$
$b_k^1 = 1$	$\|1\rangle$	$\|-\rangle$

$$|\psi_k\rangle = H^{b_k^2} X^{b_k^1} |0\rangle .$$

B: Receives qubits, says so, and measures each in the basis $\{|0\rangle, |1\rangle\}$, or $\{|+\rangle, |-\rangle\}$, choosing the basis uniformly at random.

Quantum key distribution
- the basics -



PROTOCOL QKD continued...

"CLASSICAL PHASE"

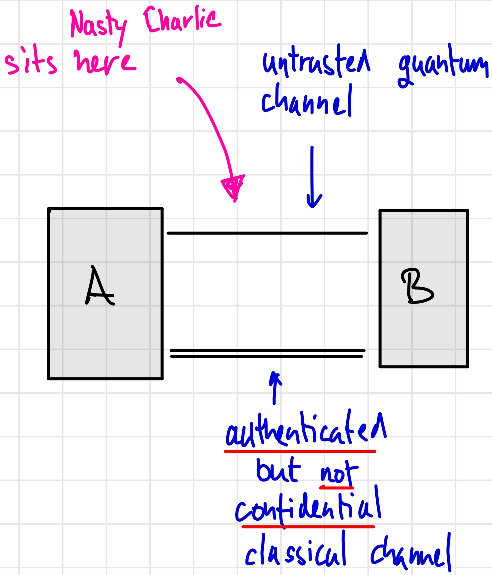
A : Reveals all the "basis" bits
$\{(i, b_i^2)\}_i$

B : Names all positions where he choose the measurement basis correctly.

A&B : discard all bits where they disagreed.

With high probability (in δ) they still share $2n$ bits.

Quantum key distribution
- the basics -



PROTOCOL QKD continued...

A: Selects randomly n bits **(C1)**
and announces to Bob
IF ANY ($\varepsilon \times n$) is wrong
THEY ABORT.

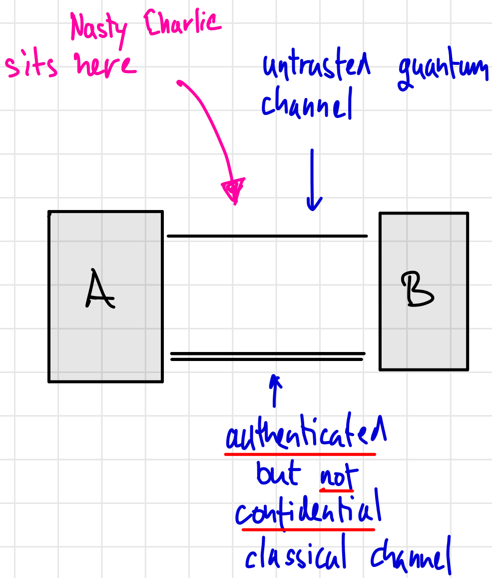
A & B: Run *INFORMATION RECONCILIATION* (IR)

A & B: Run *PRIVACY AMPLIFICATION* (PA)
$n \to m$ bits $(n > m)$

IR = ERROR CORRECTION

PA = HASHING

Quantum key distribution
- the basics -



Now: What is actually going on here?!

Correctness in idealized universe
... all perfect, Charlie doesn't exist.

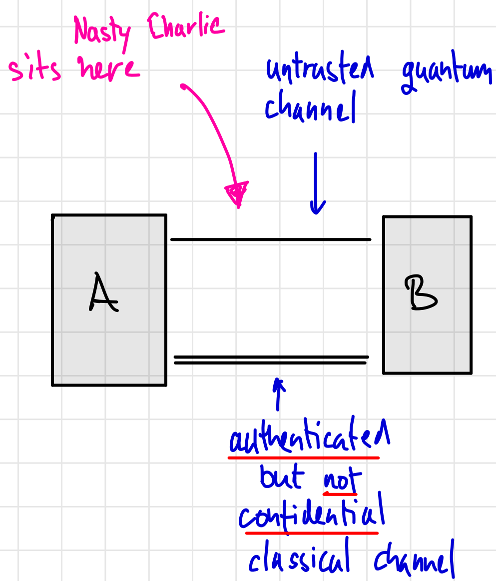
-> with exponentially high probability (in δ)

after revealing bases, share $2n$
bits, correctly measured.

-> no errors are found.

-> IR & PA will output identical keys
when start from identical raw keys.

Quantum key distribution
– the basics –



Now: What is actually going on here?!

Security in presence of Charlie.

For Charlie to learn the key...
he must learn the data bits.

How? Must measure qubits.

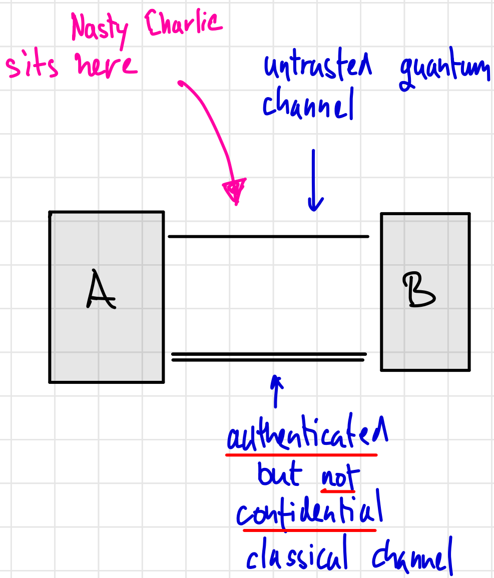
But in which Basis?

$|0\rangle$ or $|1\rangle$ → M

$|+\rangle$ or $|-\rangle$ → M

↓ which Basis

Can he learn the basis?



1 qubits ... 2 bits (data + basis)

→ <u>Holevo bounds</u> (1 bit / qubit)

→ <u>No cloning.</u> (no physical process $|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle$)

→ <u>Information gain implies disturbance</u>

$$|\psi\rangle = H^{b_2} Z^{b_1} |0\rangle \to \boxed{M} \to \begin{cases} \text{info about } b_1 \\ \cancel{\Updownarrow} \\ |\psi_{out}\rangle \neq |\psi_{in}\rangle \end{cases}$$

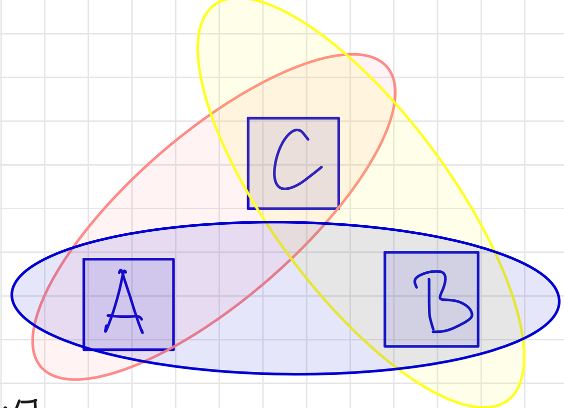
... if Charlie learns <u>something</u> ($S \times n$ bits)

... in the process with high probability he perturbed some states

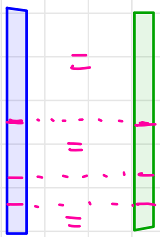
⇒ mismatch in the checking phase <u>C1</u>

⇒ Note .. noise, imperfections also cause errors ...

$\Rightarrow$ not all correlations AC, BC removed with checking (with imperfections $\Rightarrow$ must have tolerance)



INFORMATION RECONCILIATION



Use parity-checks
+ binary search
to pin-point errors..
$\Rightarrow$ LEAKS INFO...

WANT

$$P_{ABC} \approx_\varepsilon P_{AB} \cdot P_C \quad \text{(Charlie uncorrelated)}$$

$$P(k_A, k_B) \approx_\varepsilon \frac{1}{2^n} \times \delta_{k_A, k_B}$$

$$\delta_{x,y} = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$$

(Dirac-delta or Kronecker-delta)

PRIVACY AMPLIFICATION (INFLUENCES ε ...)

Cryptographic Hash functions ... uniformity over outputs...

$$f : \{0,1\}^n \to \{0,1\}^m$$ ... based on subset parities..

Security (INFORMAL): THEOREM $\forall$ Charlie security statement about P_{ABC}
Holds (within ε, except with δ) $P\left(\mathrm{Dist}\left(P_{ABC}^{\text{achieved}}, P_{ABC}^{\text{ideal}}\right) \leq \varepsilon\right) > 1-\delta$

Correctness (informal): For honest Charlie, $k_A = k_B$.

... Proving $\forall$ Charlie is tricky ... Also ... what is the scope?

History of QKD proofs is long ... and rich.

1984. Bennet & Brassard QKD (BB84)
→ intuition for iid Attacks without quantum memory

'90's Ekert ('91) different protocol via Bell
→ iid

mid-90's collective attacks

2000's Shor & Preskill first proofs for general attacks

2003 Toward composable security

2006 Renner one of first broadly applicable proof techiques (exp. Q. de Finetti..)

<u>Security (INFORMAL)</u>: THEOREM $\forall$ Charlie security statement about P_{ABC}
Holds (within ε, except with δ) $\quad P\left(\mathrm{Dist}\left(P^{\text{achieved}}_{ABC}, P^{\text{ideal}}_{ABC}\right) \leq \varepsilon\right) > 1-\delta$

<u>Correctness (informal)</u>: For honest Charlie, $k_A = k_B$.

... Proving <u>$\forall$ Charlie</u> is tricky ... Also ... what is the scope?

Beyond keys & Crypto...
we have learned <u>loads</u>
about math, physics,
information theory by studying
QKD.. it is about
classical & quantum correlations,
local realism, devices & noise...
systems in general...

History of QKD proofs is long ... and rich.

1984. Bennet & Brassard QKD (BB84)
→ intuition for iid Attacks
without quantum memory

'90's Ekert ('91) different protocol via Bell
→ iid

mid-90's collective attacks

2000's Shor & Preskill first proofs for general attacks

2003 Toward composable security

2006 Renner one of first broadly applicable proof techiques (exp. Q. de Finetti..)

Interesting:

- security based on laws of Quantum theory.
- "easy" to implement! only single qubit states & measurements
- Comercial ...

- DENSITY MATRIX FORMALISM
    - QM axioms again
    - reduced state & partial trace (subsystem measurements)
    - Quantum channels & quantum operations
    - Fidelity & trace distance

Back to q. crypto

1) "Ensamble"

In CS we talk about bitstrings & well-defined states of registers ..

state spaces ⟷ distributions over...

Distributions over Quantum states._

In crypto we talk about knowledge, ignorance, correlations...

$X :=$ random variable over message space M

$$P(X=m) = \frac{1}{|M|} ::: \text{"IGNORANCE"}$$

$$P(X=m \mid \text{it is in English}) \neq \frac{1}{|M|}$$

$$P_{AB}(X_A, X_B) \stackrel{?}{=} P_A(X_A) \cdot P_B(X_B)$$

Measures : Entropy - based

Shannon : $H(X) := -\sum_{x \in M} p(x) \log(p(x))$

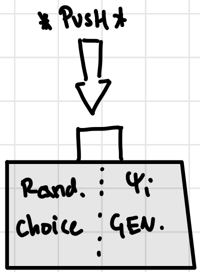
... Relative entropy (Kullback-Leibler divergence) $H(X|y) := -\sum_{x \in M} P(X=x) \log\left(\frac{P(X=x)}{P(Y=x)}\right)$

Mutual Information : $I(X:Y) = H(X) - H(X|Y)$

. - - -

1) "Ensemble"

$|\psi_i\rangle \in \mathcal{H} \quad \forall i$. All states are known ...



$\longrightarrow |\varphi\rangle$

$$|\varphi\rangle = \begin{cases} |\psi_1\rangle & \text{w. prob. } p_1 \\ |\psi_2\rangle & \text{—"—} \quad p_2 \\ \vdots & \\ |\psi_n\rangle & \text{—"—} \quad p_n \end{cases}$$

NOTE... output $\neq \sum_{i=1}^{n} p_i |\psi_i\rangle$ ... not even normalized

$\Rightarrow$ NEED MORE "ROOM" IN REPRESENTATION... ALL $|\psi\rangle \in \mathcal{H}$ are already used up

$$|\varphi\rangle \Rightarrow |\varphi\rangle\langle\varphi| \Longleftrightarrow \Pi^{|\varphi\rangle}$$

pure state $\Longleftrightarrow$ rank-1 projector.

$$\left(\Pi^{|\varphi\rangle}|\psi\rangle = |\varphi\rangle\langle\varphi||\psi\rangle = |\varphi\rangle\langle\varphi|\psi\rangle = \underline{\langle\varphi|\psi\rangle|\varphi\rangle} \right)$$

DENSITY MATRIX ρ

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \, , \qquad \sum_i p_i = 1 \qquad p_i \geq 0 \, . \ \forall i$$

$$|\psi_i\rangle \in \mathcal{H} \, . \quad \| |\psi_i\rangle \|_2 = 1 \, .$$

Note $\rho \in \mathcal{L}(\mathcal{H})$ (linear operators ON $\mathcal{H}$)

All density matrices ("general" quantum states)

Trace of linear operator
= sum of evs
= sum of diagonal elements

$\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB)$
$= \mathrm{Tr}(BCA)$

$\Rightarrow$ basis indep.

$$S(\mathcal{H}) = \{ \rho \in \mathcal{L}(\mathcal{H}) \, / \, \rho \text{ is } \underbrace{\text{Positive-semidefinite}}_{\text{PSD}} , \ \mathrm{Tr}(\rho) = 1 \}$$

PSD = Hermitian (symmetric) & all eigenvalues ≥ 0.

$\rho = U \, \mathrm{diag}(\lambda_1 \ldots \lambda_n) \, U^\dagger$ $\Leftarrow$ spectral theorem.

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(U \, \mathrm{diag}(\vec{\lambda}) \, U^\dagger) = \mathrm{Tr}(U^\dagger U \, \mathrm{diag}(\vec{\lambda})) = \mathrm{Tr}(\mathrm{diag}(\vec{\lambda})) = \sum \lambda_i$$

$S(\mathcal{H})$ is a convex set ... $\Longleftrightarrow$ you can arbitralily mix any two states!

$\Rightarrow$ $\quad \mathrm{Tr}(\rho) = 1 \Rightarrow \sum \lambda_i = 1$
$\quad$ PSD $\Rightarrow \lambda_i \geq 0.$ $\Big\}$ λ's <u>are</u> probabilities

in general $\quad \rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ $\quad$ (unique up to order for non-degenerate.)

$$\updownarrow$$

$$\sum p_i |\psi_i\rangle\langle\psi_i|$$

... just right!

$\boxed{\text{PURE STATES}}$:= <u>extremal points</u> of $S(H)$.
= rank-1 states = $|\psi\rangle\langle\psi|$ for some $|\psi\rangle$

$\boxed{\text{MIXED STATES}}$:= everything else

$$\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle = |0\rangle$$

$$\begin{bmatrix}1\\1\end{bmatrix} \quad \begin{bmatrix}1\\-1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$$

$$\frac{1}{2}|+x+| + \frac{1}{2}|-x-| = \frac{1}{2}$$

Axioms of QM revisited

1) State space $S(\mathcal{H})$ [over $\mathcal{H}$...]

2) Evolution of closed system: defined by $U \in \mathcal{L}(\mathcal{H}) \Leftrightarrow \mathcal{U} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$

[technically U & $\mathcal{U}$ are distinct ...]

pure : $|\psi\rangle \longrightarrow U|\psi\rangle$

density : $\rho \longrightarrow \mathcal{U}(\rho) := U \rho U^\dagger$

Consistency : $|\psi\rangle \xrightarrow{U} |\varphi\rangle \; (= U|\psi\rangle)$ [NB: $(U|\psi\rangle)^\dagger = \langle\psi| U^\dagger$]

$$\begin{array}{c} |\psi\rangle \\ \downarrow \\ |\psi\rangle\langle\psi| \end{array} \rightarrow U|\psi\rangle\langle\psi|U^\dagger = |\varphi\rangle\langle\varphi| \; \checkmark$$

Convex-linearity:

operative meaning...

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{\mathcal{U}} \mathcal{U}(\rho) = U\rho U^\dagger = \sum p_i \, U|\psi_i\rangle\langle\psi_i|U^\dagger$$

3) Measurement

(projective)

$M = \{ |\psi_i\rangle \}_i$ i e.g. $\{|0..0\rangle, |0..01\rangle \ldots$

Pure picture : $P_M(i \mid |\psi\rangle) = |\langle \psi_i | \psi_i \rangle|^2$

$\Downarrow$

$M = \{ |\psi_i\rangle\langle\psi_i| \}_i$

Mixed, M on $\underline{\rho}$ =

$$P_M(i \mid \rho) = \mathrm{Tr}\left(\underline{|\psi_i\rangle\langle\psi_i| \rho}\right)$$

why? $\rho = \sum p_j |\varphi_j\rangle\langle\varphi_j|$ $\quad P_M(i|\rho) = \sum p_j \, P(i \,|\, |\varphi_j\rangle)$

$$= \sum p_j \, |\langle\varphi_j|\psi_i\rangle|^2$$

$$P_M(i|\rho) = \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i|\rho\right) = \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i| \sum p_j |\varphi_j\rangle\langle\varphi_j|\right)$$

$$= \sum p_j \, \mathrm{Tr}\left(|\psi_i\rangle\langle\psi_i||\varphi_j\rangle\langle\varphi_j|\right) = \sum p_j \langle\psi_i|\varphi_j\rangle\langle\varphi_j|\psi_i\rangle = \underline{\underline{\sum p_j |\langle\varphi_j|\psi_i\rangle|^2}}$$

Nb: $\mathrm{Tr}\left(|\psi_i\rangle\langle\varphi_j|\right) = \langle\varphi_j|\psi_i\rangle$ ✓

4) Composite systems.

$$\otimes(\rho, \psi) \longrightarrow \rho \otimes \psi$$

Intuitively:

$$\underset{\downarrow}{\otimes} \quad \underset{\downarrow}{\times} \quad \underset{\downarrow}{\otimes}$$

Check: $\rho = |\rho\rangle\langle\rho|$, $\psi = |\psi\rangle\langle\psi|$; $\quad |\rho\rangle_1|\psi\rangle_2 \longrightarrow \left(|\rho\rangle_1|\psi\rangle_2\right)\left(\langle\rho|_1\langle\psi|_2\right) = |\rho\rangle\langle\rho| \otimes |\psi\rangle\langle\psi|$

$$= \rho \otimes \psi$$

ok...

Density matrix of a multi-qubit (multi-partite) system:

$$|\psi_{A,B}\rangle = \sum_{i,j} \gamma_{i,j} |i\rangle |j\rangle \quad ; \quad \langle \psi_{AB}| = \sum_{i',j'} \gamma^*_{i',j'} \langle i'| \langle j'|$$

$$|\psi_{A,B}\rangle\langle\psi_{A,B}| = \sum_{i,j} \sum_{i',j'} \gamma_{ij} \gamma^*_{i'j'} \underbrace{|i\rangle\langle i'| \otimes |j\rangle\langle j'|}_{= (|i\rangle_A |j\rangle_B)(\langle i'|_A \langle j'|_B)}$$

DENSITY MATRICES GENERALIZE QUANTUM STATES & PROBABILITY DISTRIBUTIONS

Classical distribution over bitstring

say $P(b_1 \dots b_n)$

$$\Leftrightarrow \quad \rho = \sum_{b_1 \dots b_n} P(b_1 \dots b_n) \, |b_1 \dots b_n \rangle\langle b_1 \dots b_n|$$

A & B correlated ? $P(A=a, B=b)$ $\quad a \in L_A \quad b \in L_B$

$\hookrightarrow$ def $H_A := \mathrm{span}\{|a\rangle \mid a \in L_A\}$, $\langle a|a'\rangle = \delta_{a,a'}$

$H_B := \mathrm{Span}\{|b\rangle \mid b \in L_B\}$, $\langle b|b'\rangle = \delta_{b,b'}$

$$\rho_{AB} = \sum_{\substack{a \in L_a \\ b \in L_b}} P(a,b) \, |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B$$

$$\rho_{AB} = \sum_{\substack{a \in \mathcal{L}_a \\ b \in \mathcal{L}_b}} p(a,b)\, |a\rangle\langle a|_A \otimes |b\rangle\langle b|_B$$

A C.C. (classical - classical state)

$$\rho_{AB} = \sum_{a \in \mathcal{L}_A} p(a)\, |a\rangle\langle a| \otimes \rho^a$$

$\downarrow$

any $\in S(H_B)$

$\rightarrow$ a C-Q - state

RECALL BASIS - DATA ENCODING

$b = 0, 1 \quad , \quad d = 0, 1$

$b = 0 \quad \rho_{b=0} = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \mathbb{1}$

$b = 1 \quad \rho_{b=1} = \frac{1}{2} |+\rangle\langle +| + \frac{1}{2} |-\rangle\langle -| = \frac{1}{2} \cdot \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{2} \cdot \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2} \mathbb{1}$

SAME STATE ...

Data bit?

$\rho_{d=0} = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |+\rangle\langle +| = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} 3/4 & \frac{1}{4} \\ 1/4 & 1/4 \end{pmatrix}$

$\rho_{d=1} = \frac{1}{2} |1\rangle\langle 1| + \frac{1}{2} |-\rangle\langle -| = \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} + \begin{pmatrix} \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} 1/4 & -1/4 \\ -1/4 & 3/4 \end{pmatrix}$

$\Rightarrow \exists$ a non trivial measurement..

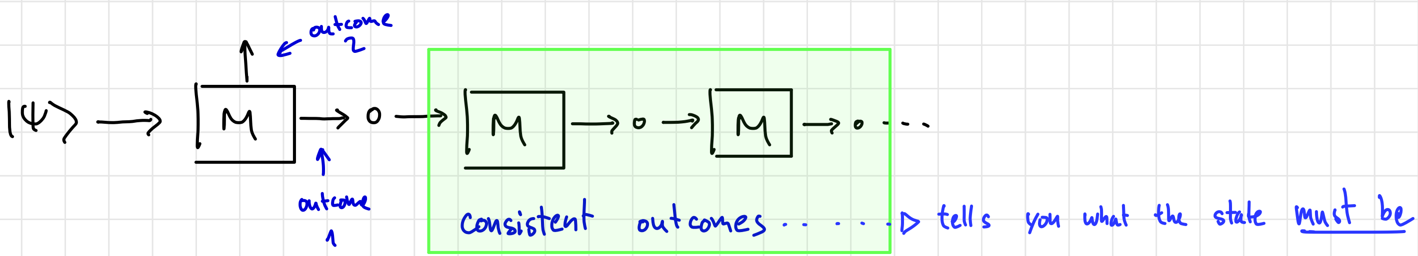
...

success prob $> \frac{1}{2}$ ..

More on measurements: post-measurement state (projective)

$\mathbb{M} = \{ |\psi_i\rangle \}_i$ "collapsing measurement" for non-demolishion measurements..

Eg:



--- Consistency-of-outcomes suggests a class of measurements called "projective measurements", which "collapse the state"

$$|\varphi\rangle \longrightarrow |\psi_i\rangle \quad \text{with probability } |\langle\psi_i|\varphi\rangle|^2$$

$$|\psi_i\rangle\langle\psi_i||\varphi\rangle = \langle\psi_i|\varphi\rangle\,|\psi_i\rangle \Rightarrow \text{probability of } i:$$

$$|\langle\psi_i|\cdot\langle\psi_i|\varphi\rangle\,|\psi_i\rangle|^2 = |\langle\psi_i|\varphi\rangle|^2.$$

$\Rightarrow$ $\boxed{\text{Projective measurements}}$ .. $M = \{|\psi_i\rangle\langle\psi_i|\}$

$$\Rightarrow \text{ on ANY } \rho \xrightarrow{M} \frac{|\psi_i\rangle\langle\psi_i|\rho|\psi_i\rangle\langle\psi_i|}{\mathrm{Tr}(|\psi_i\rangle\langle\psi_i|\rho)}, \text{ with prob. } \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|\rho)$$

More general measurements: (clearly, this is allowable by QM)

$$\begin{tikzcd}
|\varphi\rangle \arrow[r] & \boxed{M} \arrow[r] & i \arrow[r] & \boxed{\text{prep}} \arrow[r] & |\eta_i\rangle \\
 & \{|\psi_i\rangle\}_i \arrow[u] & & \text{any set} \arrow[u] &
\end{tikzcd}$$

$\{|\eta_i\rangle\}$

(not a basis)

Represented by: $\{\, |\eta_i\rangle\langle\psi_i| \,\}$: $\quad |\varphi\rangle \to |\eta_i\rangle\langle\psi_i|\varphi\rangle$

$= |\eta_i\rangle$ with prob $|\langle\psi_i|\varphi\rangle|^2$

A class of incomplete measurements:
measurements of subsystems

$$\mathcal{H}_A \otimes \mathcal{H}_B \qquad \mathcal{H}_A = \text{span}\{|\alpha_i\rangle\} \qquad \mathcal{H}_B = \text{span}\{|\beta_j\rangle\}$$

$$|\psi_{AB}\rangle = \sum_{ij} \gamma_{ij} |\alpha_i\rangle |\beta_j\rangle$$

$$\{|\psi_i\rangle\} \subseteq \mathcal{H}_A$$

$$M = \{|\psi_k\rangle\langle\psi_k| \otimes \mathbb{1}\}_k$$

$$P(k \mid |\psi_{AB}\rangle) = \left\| \left(|\psi_k\rangle\langle\psi_k| \otimes \mathbb{1} \right) |\psi_{AB}\rangle \right\|^2 = \left\| \sum_{ij} \gamma_{ij} |\psi_k\rangle\langle\psi_k|\alpha_i\rangle |\beta_j\rangle \right\|^2$$

Lemma: $\sum_{ij} \gamma_{ij} |\alpha_i\rangle|\beta_j\rangle = \sum_{ij} \gamma_{ij}' |\psi_i\rangle|\beta_j\rangle$

Proof: if $|\psi_j\rangle$ is a basis

$$\sum_k |\psi_k\rangle\langle\psi_k| \otimes \mathbb{1} = \mathbb{1}\otimes\mathbb{1}$$

$$\Rightarrow \sum_{ij} \gamma_{ij} |\alpha_i\rangle|\beta_j\rangle = \sum_{kij} \gamma_{ij} |\psi_k\rangle\langle\psi_k|\alpha_i\rangle|\beta_j\rangle$$

$$= \sum_{kj} \underbrace{\left(\sum_i \gamma_{ij} \langle\psi_k|\alpha_i\rangle\right)}_{\gamma_{kj}'} |\psi_k\rangle|\beta_j\rangle = \sum_{kj} \gamma_{kj}' |\psi_k\rangle|\beta_j\rangle$$

Any $\forall$ $\{|\psi_i\rangle\} \subseteq \mathcal{H}_A$ every $|\psi_{AB}\rangle$

$$= \sum_{ij} \gamma_{ij} |\psi_i\rangle |\beta_j\rangle$$

$$M = \{ |\psi_k\rangle\langle\psi_k| \otimes \mathbb{1} \}_k$$

$$P_A(k) = \left\| \sum_{ij} \gamma_{ij} |\psi_k\rangle\langle\psi_k|\psi_i\rangle |\beta_j\rangle \right\|^2 =$$

$$= \left\| \sum_j \gamma_{kj} |\psi_k\rangle |\beta_j\rangle \right\|^2 = \left\| |\psi_k\rangle \sum_j \gamma_{kj} |\beta_j\rangle \right\|^2$$

$$= \Big\| \underbrace{\sum_j \gamma_{kj} |\beta_j\rangle}_{\text{subnormalized residual state} \ldots} \Big\|^2 .$$

Residual state

$$|\psi'_B\rangle = \frac{\sum_j \gamma_{kj} |\beta_j\rangle}{\| \sum_j \gamma_{kj} |\beta_j\rangle \|^2}$$

Incomplete projective measurements:

$$M = \{ \Pi_j \}_j \qquad \Pi_j \Pi_j = \Pi_j \quad , \quad \sum \overset{\text{orthogonality...}}{\downarrow}\Pi_j = \mathbb{1}$$

$$\rho \longrightarrow \frac{\Pi_j \rho \Pi_j}{\mathrm{Tr}(\rho \Pi_j)} \text{, with prob } \mathrm{Tr}(\rho \Pi_j)$$

Eg: $\{ |0\rangle\langle 0| \otimes \mathbb{1}_B \, , \, |1\rangle\langle 1| \otimes \mathbb{1}_B \}$

For pure states a bit simpler:

$$|\psi\rangle \to \Pi_j |\psi\rangle$$

with prob $\| \Pi_j |\psi\rangle \|_2^2$

$[= \mathrm{Tr}(\Pi_j |\psi\rangle\langle\psi|)]$

Example: $|\psi\rangle : \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

$$M_1 = \{ \underbrace{|0\rangle\langle 0| \otimes \mathbb{1}}_{\text{Outcome 1}}, \underbrace{|1\rangle\langle 1| \otimes \mathbb{1}}_{\text{outcome 2}} \}$$

Say O_1.

$$\text{Prob}(O_1) = \left\| \left(|0\rangle\langle 0| \otimes \mathbb{1} \right) |\psi\rangle \right\|_2^2$$

$$= \left\| \frac{1}{\sqrt{2}} \left[\left(|0\rangle \underbrace{\langle 0|0\rangle}_{1} \otimes |0\rangle \right) + \left(|0\rangle \underbrace{\langle 0|1\rangle}_{0} \otimes |1\rangle \right) \right] \right\|^2$$

$$= \left\| \frac{1}{\sqrt{2}} |0\rangle|0\rangle \right\|^2 = \frac{1}{2}$$

↑ residual, post-measurement state

$$M_2 = \{ \underbrace{|+\rangle\langle +| \otimes \mathbb{1}}_{\text{Outcome 1}}, \underbrace{|-\rangle\langle -| \otimes \mathbb{1}}_{\text{outcome 2}} \}$$

Say O_2

$$\text{Prob}(O_2) = \left\| \left(|-\rangle\langle -| \otimes \mathbb{1} \right) |\psi\rangle \right\|_2^2$$

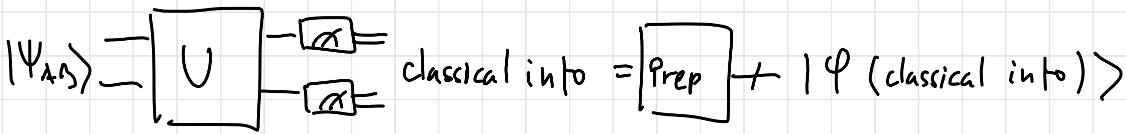
$$= \left\| \frac{1}{\sqrt{2}} \left[|-\rangle \underbrace{\langle -|0\rangle}_{\frac{1}{\sqrt{2}}} |0\rangle + |-\rangle \underbrace{\langle -|1\rangle}_{-\frac{1}{\sqrt{2}}} |1\rangle \right] \right\|_2^2$$

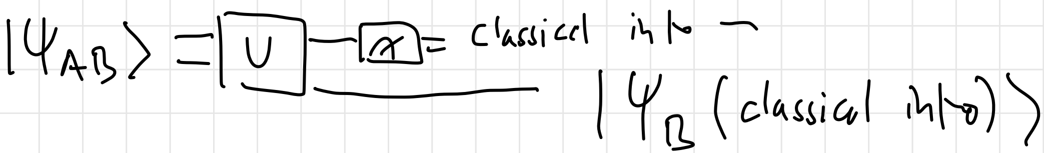
$$= \left\| \frac{1}{\sqrt{2}} \underbrace{\left[\frac{1}{\sqrt{2}} |-\rangle|0\rangle - \frac{1}{\sqrt{2}} |-\rangle|1\rangle \right]}_{|-\rangle|-\rangle} \right\|_2^2 = \frac{1}{2}$$

← residual, post-measurement state

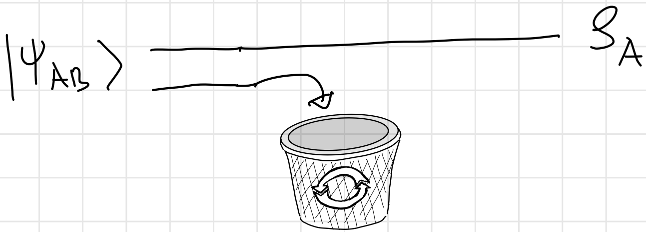
Comment. In complete measurements ALL info about the initial state has been converted to classical information.

Incomplete measurements.. some quantum info remains

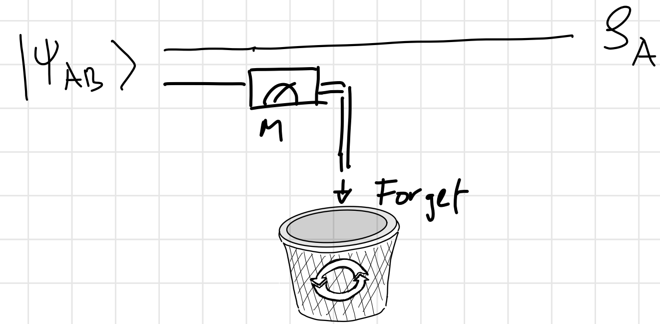




PARTIAL TRACE



OR



DEFINED ON DENSITY MATRICES

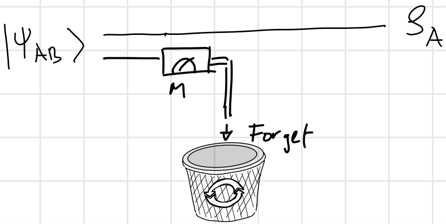
$$|\psi_{AB}\rangle = \sum_{ij} \gamma_{ij} |i\rangle|j\rangle$$

$$|\psi_{AB}\rangle\langle\psi_{AB}| = \sum_{i,j}\sum_{i',j'} \gamma_{ij}\gamma^*_{i'j'} |i\rangle\langle i'|_A \otimes |j\rangle\langle j'|_B$$

$$\rho_A = \mathrm{Tr}_B\left[\sum_{\substack{i,i'\\j,j'}} \gamma_{ij}\gamma^*_{i'j'} |i\rangle\langle i'|_A\otimes|j\rangle\langle j'|_B\right] = \sum_{\substack{i,i'\\j,j'}} \gamma_{ij}\gamma^*_{i'j'}|i\rangle\langle i'| \cdot \underbrace{\mathrm{Tr}\left[|j\rangle\langle j'|\right]}_{\delta_{j,j'} \Rightarrow j=j'} = \sum_{i,i'}\Big(\overbrace{\sum_j \gamma_{ij}\gamma^*_{i'j}}^{\eta_{ij}} |i\rangle\langle i'| = \sum_{i,i'} \eta_{i,i'}|i\rangle\langle i'|$$

keeping A

Tracing out B



say : $M = \{ \mathbb{1}_A \otimes |k\rangle\langle k| \}_k = \{ \Pi_k \}$

$$\rho_A = Tr_B\Big[\sum_{\substack{i i' \\ j j'}} \gamma_{ij}\gamma^*_{i'j'} |i\rangle\langle i'|_A \otimes |j\rangle\langle j'|_B\Big] = \sum_{\substack{i i' \\ j j'}} \gamma_{ij}\gamma^*_{i'j'} |i\rangle\langle i'| \cdot \underbrace{Tr\big[|j\rangle\langle j'|\big]}_{\delta_{j,j'} \Rightarrow j=j'} = \sum_{i,i'} \boxed{\overbrace{\sum_j \gamma_{ij}\gamma^*_{i'j}}^{\eta_{ij}}} |i\rangle\langle i'|$$

Recall $\rho_{AB} \to (\Pi_k \, \rho_{AB} \, \Pi_k) \cdot Tr^{-1}[\Pi_k \rho] = \rho'_{AB}$

$$\rho'_{AB} = \sum_k \sum_{\substack{i i' \\ j j'}} \gamma_{ij}\gamma^*_{i'j'} |i\rangle\langle i'| \otimes \underbrace{\big[|k\rangle\langle k| \cdot |j\rangle\langle j'| \cdot |k\rangle\langle k|\big]}_{= 0 \text{ unless } k = j = j'}$$

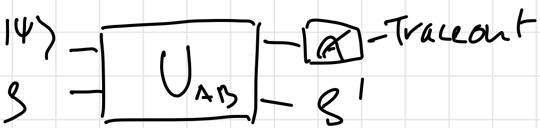
$$= \rho'_{AB} = \sum_k \boxed{\sum_{i,i'} \gamma_{ik}\gamma^*_{i'k}} |i\rangle\langle i'| \otimes |k\rangle\langle k|$$ ← outcome

same if forget

EVERYTHING ALLOWABLE BY QUANTUM MECHANICS

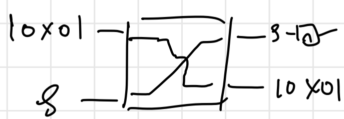
"Quantum channel" [deterministic Q. operation]
- generalizes unitary evolution

$\mathcal{E}: \rho \to \rho'$. [specified by ψ, U on larger space]



$$\mathcal{E}(\rho_B) = \mathrm{Tr}_A\left[U_{AB} \left(|\psi\rangle\langle\psi| \otimes \rho \right) U_{AB}^\dagger \right]$$

Eg.:



$\Downarrow$

$\mathcal{E}(\rho) = |0\rangle\langle 0| \quad \forall \rho$

Q. channel $\mathcal{E}: \mathcal{L}(H) \to \mathcal{L}(H)$

= Completely positive, trace preserving map (CPTP)

0) Linear

1) $\forall \rho \in S(H)$
$\mathrm{Tr}(\mathcal{E}(\rho)) = 1$

2) • $\forall$ PSD ρ, $\mathcal{E}(\rho)$ is PSD

• $\forall \mathbb{1}_A$ (any dimension)

$(\mathbb{1}_A \otimes \mathcal{E}_B)$ is positive

$\Rightarrow$ completely positive

Why completely positive?

$$\mathcal{E}(|i\rangle\langle j|) = |j\rangle\langle i| \qquad (\text{transposition})$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$(\mathbb{1}\otimes\mathcal{E})\,|\psi\rangle\langle\psi| = (\mathbb{1}\otimes\mathcal{E})\,\frac{1}{2}\,\overbrace{\left[\left(|00\rangle + |11\rangle\right)\left(\langle 00| + \langle 11|\right)\right]}^{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & & & & \vdots \\ 0 & & & & \vdots \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}} =$$

$$= \frac{1}{2}(\mathbb{1}\otimes\mathcal{E})\left[|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |0\rangle\langle 1|\otimes|0\rangle\langle 1| + |1\rangle\langle 0|\otimes|1\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|\right]$$

$$= \frac{1}{2}\left[|00\rangle\langle 00| + |0\rangle\langle 1|\otimes|1\rangle\langle 0| + |1\rangle\langle 0|\otimes|0\rangle\langle 1| + |11\rangle\langle 11|\right] = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \simeq \underbrace{\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix}}_{\text{ev}}$$

$$|0\rangle\langle 1|\otimes|1\rangle\langle 0| \;\downarrow\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\otimes\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad |1\rangle\langle 0|\otimes|0\rangle\langle 1| \;\downarrow\; \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\otimes\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Valid maps: turn quantum states into valid quantum states even if applied on subsystem..

$\Leftrightarrow$ CPTP.

Krauss operators: $\{B_i\}_i$ st $\sum_i B_i^\dagger B = \mathbb{1}$

$$\mathcal{E}(\rho) = \sum_i B_i \rho B_i^*$$

$\mathcal{E}$ CPTP $\Leftrightarrow$ ($\exists$) Krauss representation $\Leftrightarrow$ $\mathcal{E}(\rho) = Tr_A(U_{AB}(\psi \otimes \rho)U_{AB})$
For some $U_{AB}, |\psi\rangle$

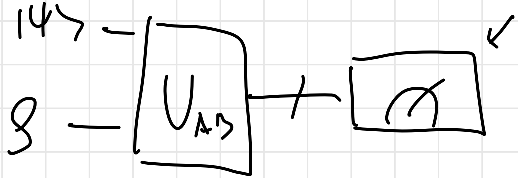
Stinespring dilation theorem (Church of larger Hilbert space)

ALL (complete) measurements : positive-operator valued measure (POVM's)

$\{\Pi_i\}$ $\quad$ Π_i is PSD ; $\sum \Pi_i = \mathbb{1}$

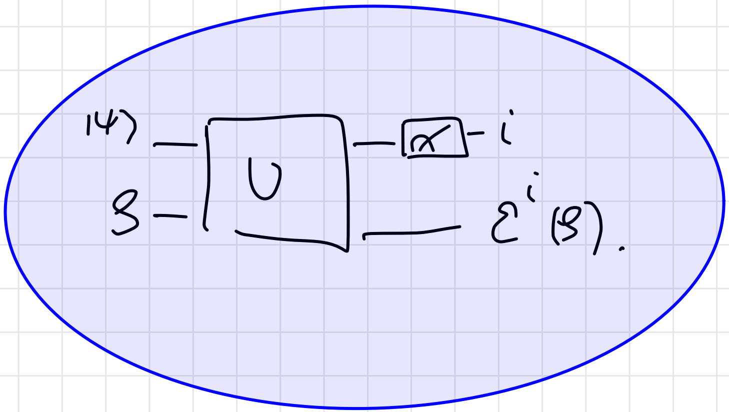
$\rho \to i$ w. prob. $\mathrm{Tr}(\Pi_i \rho)$

Equivalence : ALL POVM's :



complete projective measurement on larger space

Quantum Operations & Quantum instruments



NB: $\sum \mathcal{E}^i$ is CPTP.

$\mathcal{E}^i$ is completely positive

trace-nonincreasing

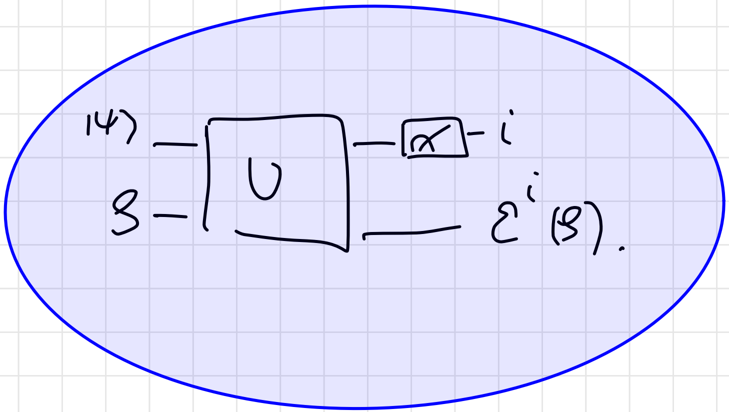
$\Rightarrow$ Quantum operation.

Kraus: $\{ \{B_{j_i}\}_{j_i} \}_i$

$$\underbrace{\sum_{j_i} B_{j_i}^* B_{j_i}}_{\Pi_i \text{ (POVM)}} \text{ is PSD} \qquad \sum_i \sum_{j_i} B_{j_i}^* B_{j_i} = \mathbb{1}$$

$$\rho \to \frac{\sum_{j_i} B_{j_i} \rho B_{j_i}^*}{\mathrm{Tr}\left(\sum_{j_i} B_{j_i} \rho B_{j_i}^*\right)} = \frac{\mathcal{E}^i(\rho)}{\mathrm{Tr}(\mathcal{E}^i(\rho))}$$

QUANTUM Operations & QUANTUM instruments



"All that ANY BOB CAN DO"

Kraus: $\{\{B_{ji}\}_{j_i}\}_i$

$$\rho \to \frac{\sum_{ji} B_{ji}\,\rho\, B_{ji}^*}{\mathrm{Tr}\left(\sum_{ji} B_{ji}\,\rho\, B_{ji}^*\right)} = \frac{\mathcal{E}^i(\rho)}{\mathrm{Tr}(\mathcal{E}^i(\rho))}$$

ALSO: output of Quantum instrument is a C-Q state:

$$\rho_{out} = \sum_i \mathrm{Tr}(\mathcal{E}^i(\rho))\,|i\rangle\langle i| \otimes \mathcal{E}^i(\rho) \ldots$$

$\Rightarrow$ Unitaries & projective measurements "complete" in the larger, dilated, space

Analogy: Randomized computation uses "larger space": random tape...

Distance measures:

1.) Pure state fidelity (<u>not</u> a metric)

$$F(|\psi\rangle, |\varphi\rangle) = |\langle\psi|\varphi\rangle|^2 \qquad \text{(overlap.)}$$

$F = 0 \iff$ orthogonal

$F = 1 \iff$ the same.

2.) Trace distance:

singular values

Trace norm: $\|A\|_{tr} = tr\left(\sqrt{\underbrace{A^{\dagger}A}_{PSD}}\right) = \sum_i \sigma_i$

$= \sum_i |\lambda_i|$ For normal matrices

Trace distance: $D(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_{tr}$

$$1-\sqrt{F(\rho,\sigma)} \leq D(\rho,\sigma) \leq \sqrt{1-F(\rho,\sigma)}$$

For pure ρ, σ. (also mixed via $F(\rho,\sigma) = \left[\mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right]^2$)

Operational meaning

$$D(\rho,\sigma) = \sup_{0 \leq \Pi \leq \mathbb{I}} \left(\mathrm{Tr}(\Pi\rho) - \mathrm{Tr}(\Pi\sigma)\right)$$

Alices probability of guessing ρ or σ, under optimal measurement is

$\frac{1}{2} + \frac{1}{2} D(\rho,\sigma)$ "distinguishing advantage"

$$\rho_{d=0} = \begin{pmatrix} 3/4 & \frac{1}{4} \\ 1/4 & 1/4 \end{pmatrix}$$

$$\rho_{d=1} = \begin{pmatrix} 1/4 & -\frac{1}{4} \\ -\frac{1}{4} & 3/4 \end{pmatrix}$$

How well can Charlie do?

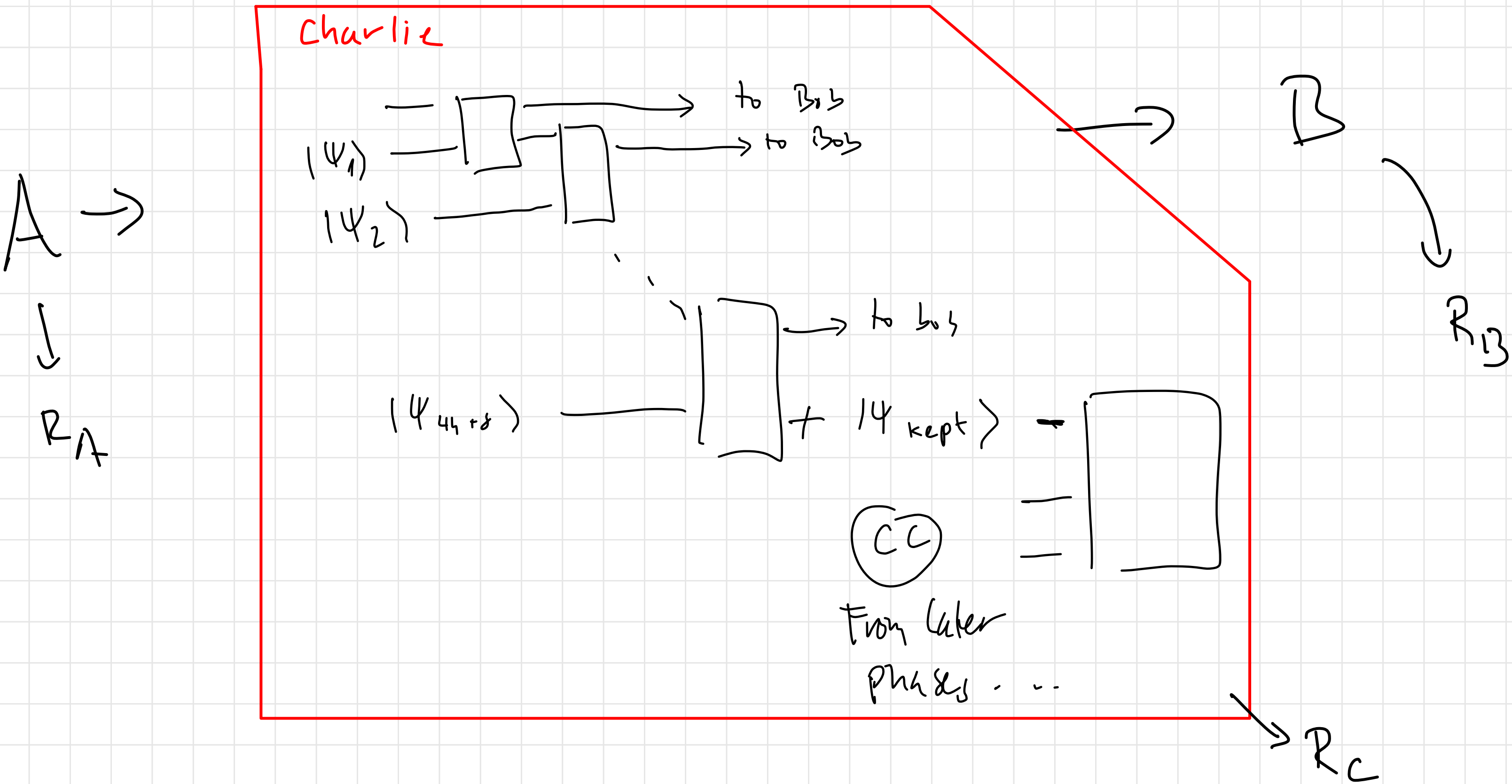
$$\frac{1}{2} + \frac{1}{4} \left\| \rho_{d=0} - \rho_{d=1} \right\|_{tr}$$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

$$\mathrm{tr} \sqrt{\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} \approx 0{,}707$$

$$\frac{1}{2} + 0{,}31 = 0{,}84 \ldots$$

BACK TO QKD.


Charlie
to Bob
to Bob
$|\psi_1\rangle$
$|\psi_2\rangle$
to bob
$|\psi_{4th\ rd}\rangle$
+ $|\psi_{kept}\rangle$
CC
from later
phases ...
A
R_A
B
R_B
R_C

The security proof is a proof proving the following property of the joint state... $\forall$ Charlie ...

(1) $$\rho_{ABC} \approx_{\varepsilon} \rho_{AB} \otimes \rho_C \quad \text{(for some } \rho_C\text{)}$$

not correlated

with $$\rho_{AB} = \sum_k \frac{1}{2^n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B$$

(1) $$\psi_A \approx_{\varepsilon} \psi_B \iff \frac{1}{2} \| \psi_A - \psi_B \|_{tr} \leq \varepsilon$$

There is MUCH more to quantum crypto

- Quantum coins & Q. money
- voting
- Secret sharing
- Bit commitment
- coin tossing
- oblivious transfer
- secure multiparty computation
- secure delegated quantum computing

- BOUNDED STORAGE
- NOISY STORAGE ..

- Information-theoretic security
- Computational security
  ↳ "Post-Quantum Crypto"
- MODELS:
  - UNIVERSAL COMPOSABILITY
  - ABSTRACT & CONSTRUCTIVE CRYPTO ...
- RELATIVISTIC CRYPTO