Graeme Smith:

1. $Q^{(1)}(N \otimes A)$ additive

2. Private Capacity of Q Channel

3. PPT states + privacy

4. Superactivation of Q capacity

   $Q(N_1 \otimes N_2) > 0, \quad Q(N_i) = 0$

5. Erasure channel.

$A: \; V|(i,j)\rangle \propto |i\rangle_\perp |j\rangle_T + |j\rangle_\perp |i\rangle_T$

$A(\rho) = \mathrm{Tr}_2 V\rho V^+$

Define $Q^{(1)}_{ss}(N) = Q^{(1)}(N\otimes A)$

Then we have the following lemmas:

lemma

1 $Q^{(1)}_{ss}(N\otimes M) = Q^{(1)}_{ss}(N) + Q^{(1)}_{ss}(M)$

Need lemma 2.

• Recall coherent info for channel N:

$$\max_\phi \left[S(B) - S(E)\right]_{I\otimes N(\Phi)}.$$

Pf

2 $Q^{(1)}_{ss}(N) = Q^{(1)}(N\otimes A)$.

$$= \max_\phi \left[I^{coh}(N\otimes A, \phi)\right]$$

$$= \max_{|\phi\rangle_{AA'A''}} \left[I(A\rangle B\perp)\right]$$

$$= \max_{\substack{|\phi_{AA'}IT\rangle \\ \text{symmetric}}} \left[I(A\rangle B\perp)\right]$$

Lemma 2

$$Q^{(1)}_{SS}(N) = \max_{\rho_{AA'F}} \frac{1}{2}\left[I(A\rangle BF) - I(A\rangle EF)\right]$$

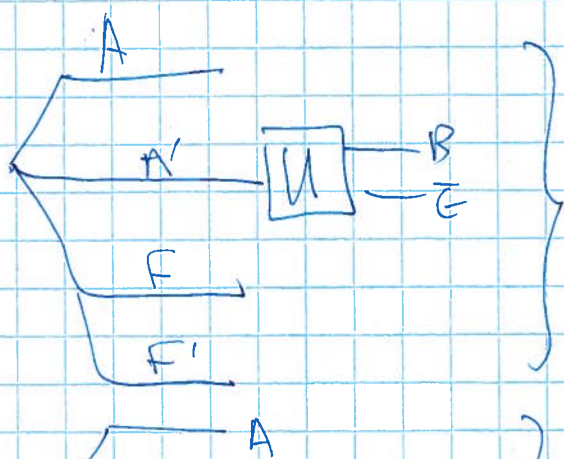
Why?

Purifying $\rho_{AA'F}$ as $|\psi\rangle_{AA'FF'}$.

$$= \max_{|\psi\rangle_{AA'FF'}} \frac{1}{2}\left[I(A\rangle BF) + I(A\rangle BF')\right]$$

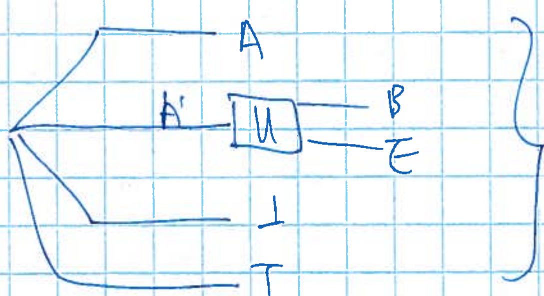
pure:

$\rho_{AA'FF'}$



$\frac{1}{2}\left[I(A\rangle BF) + I(A\rangle EF')\right]$

$|\phi\rangle_{AA'\perp T}$



$I(A\rangle B\perp)$.

$$|\tilde{\psi}\rangle_{AA'ff'aa'} = \frac{1}{\sqrt{2}}\Big[\, |\psi\rangle_{AA'ff'}|0\rangle_a|1\rangle_{a'}$$

$$(I_{AA'} \otimes SWAP_{ff'})\,|\psi\rangle_{AA'ff'}\,|1\rangle_a|0\rangle_{a'}\Big]$$

Sym unit swapping these.

Feed A' to channel 1:

$$\rho_{AA'f_a} = \frac{1}{2}\Big[\rho_{AA'f} \otimes |0\rangle\langle 0|_a + \rho_{AA'f'} \otimes |1\rangle\langle 1|_a\Big]$$

$$I(A\rangle Bf_a)$$

$$= \frac{1}{2}\Big[I(A\rangle Bf) + I(A\rangle Bf')\Big]$$

$\square$

Pf lemma (1).

$$Q^{(1)}_{SS}(N_1 \otimes N_2):$$

$$\rho_{AA_1A_2f}$$

$$A_1 \downarrow N_1 \qquad A_2 \downarrow N_2 .$$

Now $\frac{1}{2}\left[I_c(A\rangle B_1B_2f) - I_c(A\rangle E_1E_2f)\right]$

$$= \frac{1}{2}\left[I_c(A\rangle B_1B_2f) - I_c(A\rangle E_1B_2f) + I_c(A\rangle E_1B_2f) - I_c(A\rangle E_1E_2f)\right]$$

cancels out

Focus on $\frac{1}{2}\left[I_c(A\rangle B_1\underbrace{B_2f}_{\tilde{f}}) - I_c(A\rangle E_1\underbrace{B_2f}_{\tilde{f}})\right]$

$$\leq Q_{ss}^{(1)}(N_1)$$

For $\frac{1}{2}\left[I_c(A\rangle \underbrace{E_1B_2f}_{\tilde{\tilde{f}}}) - I_c(A\rangle \underbrace{E_1E_2f}_{\hat{\hat{f}}})\right]$

$$\leq Q_{ss}^{(1)}(N_2).$$

But the top line, optimized, is $Q_{ss}^{(1)}(N_1 \otimes N_2)$

$\therefore$ It is $\leq Q_{ss}^{(1)}(N_1) + Q_{ss}^{(1)}(N_2)$.

The opposite direction:

$$Q^{(1)}_{ss}(N_1 \otimes N_2) \geq Q^{(1)}_{ss}(N_1) + Q^{(1)}_{ss}(N_2)$$

is easy, by choosing a particular input for the coherent info for $N_1 \otimes N_2$: $\phi_{AA_1F_1} \otimes \phi_{\hat{A}A_2F_2}$

where $\phi_{AA_1F_1}$ is optimal for N_1

$\phi_{\tilde{A}A_2F_2}$ - - - - . N_2.

$\therefore$ Lemma 1 holds.

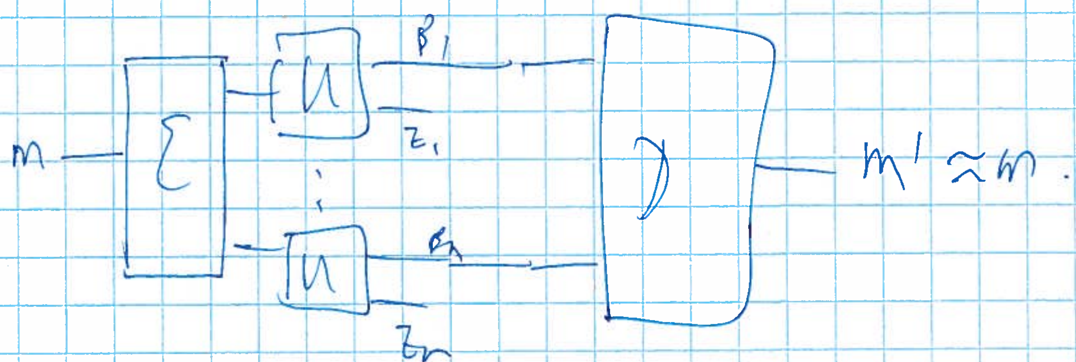
NB max should be sup ! dim f is ~~tho~~ not unknown here.

② Private Capacity of Q channel.

Ref: Csiszar & Korner 78

"broadcast channels with confidential messages"

Devetak 0304127



$$P^{(1)}(N) = \max_{\{p_x, \phi_x\}} \left[I(X;B) - I(X;E) \right]$$

evaluated on

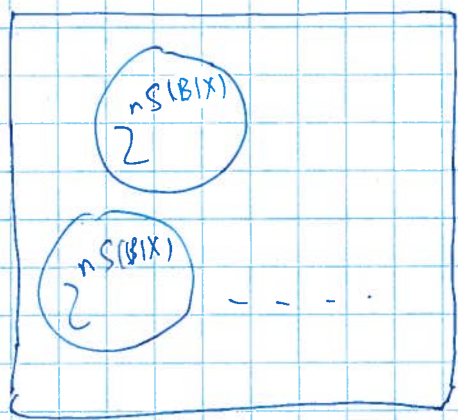
$$\sum_x p_x |x\rangle\langle x|_X \otimes U_N \phi_x U_N^\dagger$$

Intuition:

for Bob.

output space of channel

$2^{nS(B)}$

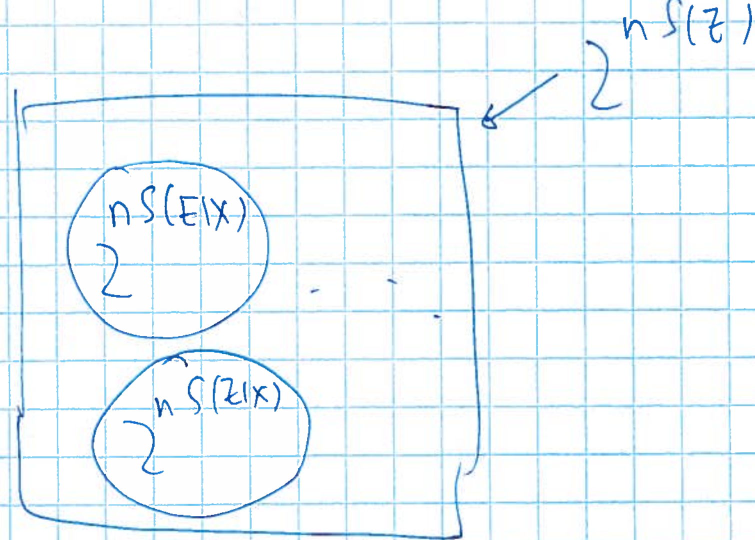


fix $x_1 \; x_2 \; \ldots \; x_n$

$\phi_{x_1} \; \phi_{x_2} \; \ldots \; \phi_{x_n}$

How much space? $2^{nS(B|X)}$

Can code $\dfrac{2^{nS(B)}}{2^{nS(B|X)}} \approx 2^{nI(X;B)}$ messages for Eve



- Transmission to Bob requires his spheres don't overlap

- Privacy: collect different spheres in bins as a message for Bob.

- Idea: how many spheres per bin ??

If we put $\approx \left\{ \dfrac{2^{n(S(Z))}}{2^{nS(Z|X)}} \right\} = 2^{nS(X:Z)}$ in a single bin

each bin fills Eve's space, so she may find out which sphere in the bin

but every bin looks the same (each fill the entire space).

$$\therefore \text{The \# of bins} = \frac{2^{n I(X:B)}}{2^{n I(X;E)}}$$

= # private messages that can be sent from Alice to Bob.

$$\text{So } P(N) = \lim_{n\to\infty} \frac{1}{n} P^{(1)}(N^{\otimes n})$$

③ PPT states.

HHHO 2003

- $|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB} \right)$

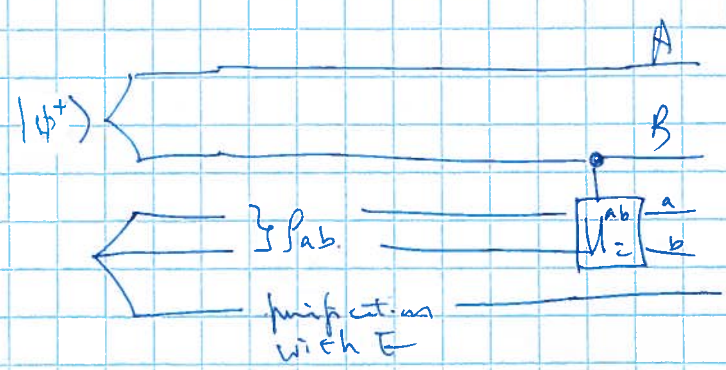
If A & B each measure in computation basis, each gets the same outcome & no one else knows. (Ekert QKD)

- $|\phi^+\rangle\langle\phi^+|_{AB} \otimes \cancel{\left(p \rho^0_{ab} + (1-p) \rho^1_{ab}\right)} \ \rho_{ab}.$

Same as before.

- $U_{ABab} \left[|\phi^+\rangle\langle\phi^+|_{AB} \otimes \left(\cancel{p} \rho^0_{ab} \cancel{+ (1-p) \rho^1_{ab}} \right) \right] U^\dagger_{ABab}$ $\quad \rho_{ab}$

for $U_{ABab} = \sum_{ij} |ij\rangle\langle ij|_{AB} \otimes U_i^{ab}$



State given to Alice & Bob.

Measuring $\{|0\rangle, |1\rangle\}$ basis on A & B.

Commutes with the unitary!

∴ Same out come

also does NOT leak info to Eve!

So the state has "privacy" but ~~little~~

for properly chosen U_{ABab}, has little distillable

entanglement.

Now add a little separable state σ

s.t. $\rho(1-p) + \sigma p$ is PPT.

ρ the big state

Yet there is residual privacy.

$\underset{(1)}{!}\ \exists N$ s.t. $Q(N)=0$ & $P^{(1)}(N)>0$.

See Pankowski, H, H, IEEE.

2 qubits x 2 qubits.

(4) Superactivation.

Consider $Q_{ss}^{(1)}(N) = \max\limits_{\rho_{AA'f}} \frac{1}{2}\left[\underbrace{I(A\rangle Bf)}-\underbrace{I(A\rangle Ef)}\right]$

$$= \max_{\rho_{AA'f}} \frac{1}{2}\left[-S(A|Bf)+S(A|Ef)\right]$$

$$= \max_{\rho_{AA'f}} \frac{1}{2}\left[\begin{matrix} -S(A|Bf) & +S(A|Ef) \\ +S(A|f) & -S(A|f). \end{matrix}\right]$$

$$= \max_{\rho_{AA'f}} \frac{1}{2}\left[I(A:B|f)-I(A:E|f)\right]$$

$$P^{(1)}(N) = \max_{\underbrace{\{p_x, \phi_x\}}_{\sum_x p_x |x\rangle\langle x| \otimes \phi_x}} \left[I(X;B) - I(X;E) \right]$$

= above with trivial F.

and without $\frac{1}{2}$ factor.

$$\therefore P^{(1)}(N) \leq 2 \times Q_{SS}^{(1)}(N)$$

$$= 2\, Q^{(1)}(N \otimes A)$$

take the N s.t. $Q(N) = 0$ & $P^{(1)}(N) > 0$.

Note also $Q(A) = 0$.

$$0 < Q^{(1)}(N \otimes A) \leq Q(N \otimes A)$$

Can use erasure channel (50-50) with in qubit input instead of A.