CO781 / QIC 890 Lec 22. Nov 29. 2016

Thm (superactivation) (Smith-Yard 0807.4935)

$\exists N_1, N_2$ s.t $Q(N_1) = Q(N_2) = 0$

but $Q^{(1)}(N_1 \otimes N_2) > 0$

Cor 1 Q is **not** convex.

ie $\exists p_i, N_i$ s.t $Q(\sum_i p_i N_i) > \sum_i p_i Q(N_i)$

Cor 2: $\exists N$ $Q^{(1)}(N) = 0$, $Q^{(2)}(N) > 0$.

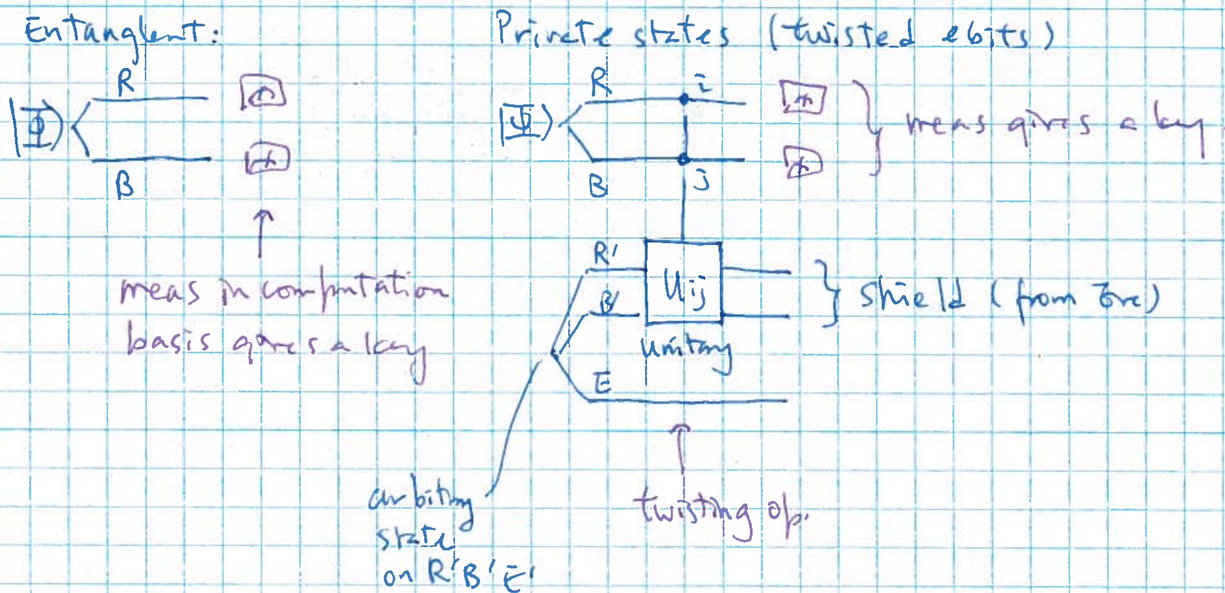
Proof ideas for theorem

HHHO 03 — ① ⓐ $\exists \rho_{AB}$ s.t. $E_D(\rho_{AB}) = 0$ & $P(\rho_{AB}) > 0$

(E_D: distillable entanglement; P: distillable key with 1-way comm from A to B.)

ⓑ $\exists N_H$ s.t. $Q(N_H) = 0$ & $P(N_H) > 0$

Idea:



Private states contain perfect keys & some distillable entanglement.

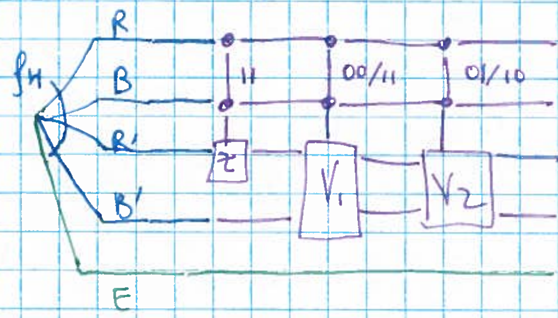
Idea: let $\rho = (1-p)\, \gamma + p \frac{I}{\dim(RR'BB')}$

(γ: private state on $RR'BB'$; $\frac{I}{\dim(RR'BB')}$: max mixed state.)

For some γ (with $P \gg E_D$), a small p is enough to make ρ PPT & $E_D(\rho) = 0$. But $P(\rho) > 0$ still if p is small.

Original HHH005
see 0608195

eg Define ρ_H on $R\,B\,R'\,B'$ (each a qubit) s.t upon the untwisting op, RB becomes



$$\left\{ p\,|\Phi\rangle\langle\Phi| + (1-p)\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)\left(\frac{\langle 01|+\langle 10|}{\sqrt{2}}\right)\right.$$

NB $p=1$ if ρ_H is a private state, but it is not.

ρ_H is more noisy, so the output key is also noisy.

* When $p = \frac{\sqrt{2}}{1+\sqrt{2}} \doteq 0.5858$, ρ_H PPT

* When $p > \frac{1}{2}$, $P(\rho_H) \geq 0.0213$ (1-way distillation).

Idea: $(\rho_H)_{RR'} = \frac{I}{4}$! So $\rho_H = \left(I_{RR'} \otimes N\right)\left(\Phi_{RA} \otimes \Phi_{R'A'}\right)$

$=$ Choi state of N.

Known: Choi state PPT $\Rightarrow Q=0$ (RMP) HHH98

But key rate > 0 $\therefore P > 0$.

NB: V_1 takes $|00\rangle \to |00\rangle$

$|11\rangle \to |11\rangle$

$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \to |01\rangle$

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \to |10\rangle$

V_2 takes $|\chi_+\rangle \to |01\rangle$

$|\chi_-\rangle \to |11\rangle$

$|\chi_\pm\rangle = \frac{1}{2}\left(\sqrt{2\pm\sqrt{2}}\,|00\rangle \pm \sqrt{2\mp\sqrt{2}}\,|11\rangle\right)$

same as V_1 on span$\{|01\rangle, |10\rangle\}$

② Thm (Smith-Smolin-Winter 0607039)

$$\frac{1}{2} P^{(1)}(N) \leq \frac{1}{2} P(N) \leq Q^{(1)}(N \otimes S) = Q_{ss}(N)$$

(S: any sym channel; Q_{ss}: side sym channel assisted)

More specifically:

$$\frac{1}{2} P^{(1)}(N) \leq Q^{(1)}(N \otimes E_{\frac{1}{2}}).$$

- See 2010 lec notes for proof.

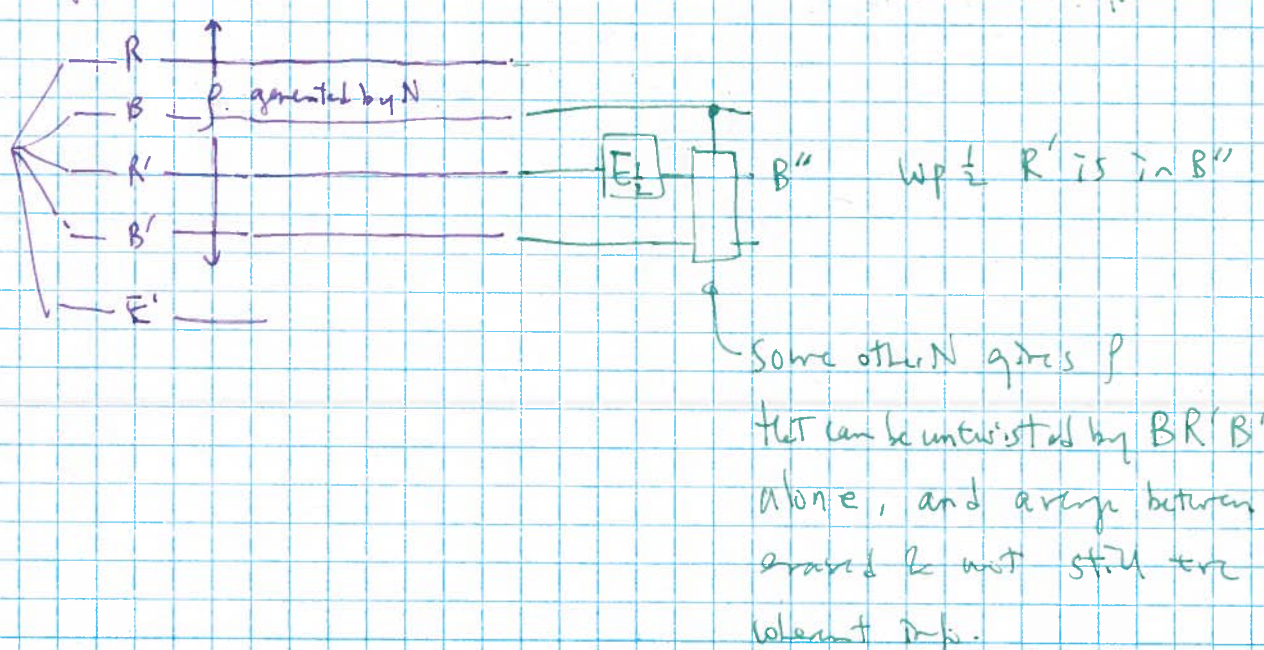
③ Take $N = N_H$ in part ①, $E_{\frac{1}{2}}$ on 4 dim.

$$\frac{1}{2} P^{(1)}(N) = 0.01065 < Q^{(1)}(N_H \otimes E_{\frac{1}{2}})$$

N_H: no entanglt, lots of key (privacy)

$E_{\frac{1}{2}}$: no privacy, sym wrt BE, Entanglmt (under 2-way distillat.)

④ In fact, by passing ②, intuition:



Cor 1: Q not convex.

Pf: let $N = q\, N_H \otimes |0\rangle\langle 0|_{B'} + (1-q)\, E_{\frac{1}{2}} \otimes |1\rangle\langle 1|_{B'}$

where we embed $N_H, E_{\frac{1}{2}}$ to have same input dims & same output dims.

Here, N_H or $E_{\frac{1}{2}}$ occurs but not sure which one before the channel. Bob knows afterwards.

$$I_c(R\rangle B^{\otimes 2} B'^{\otimes 2})_{I_R \otimes N^{\otimes 2}(\tilde{\psi})} \quad \text{pure}$$

$$= q^2\, I_c(R\rangle B^{\otimes 2})_{I_R \otimes N_H^{\otimes 2}(\psi)}$$

$$+ (1-q)q\, I_c(R\rangle B^{\otimes 2})_{I_R \otimes N_H \otimes E_{\frac{1}{2}}(\psi)}$$

$$+ \text{-- -- -- -- -- -- . . . --}\ E_{\frac{1}{2}} \otimes N_H(\psi)$$

$$+ (1-q)^2\, I_c(R\rangle B^{\otimes 2})_{I_R \otimes E_{\frac{1}{2}}^{\otimes 2}(\psi)}.$$

- last term $= 0$ ∵ sym wrt Bob & env.
- Choose $|\psi\rangle_{R A_1 A_2} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - $R A_1 A_2$ @ 4 dim
  - R, 1st qubits of A_1, A_2 ; 2nd qubits of A_1, A_2

Then 2nd, 3rd term both +ve constant α,
1st term -ve const β.

Choose q small gives +ve overall I_c.

Cor 2: Similar.