Graeme Smith:

1. \( Q''''(N \otimes A) \) additive
2. Private capacity of \( \mathcal{Q} \) channel
3. PPT states + privacy
4. Superactivation of \( \mathcal{Q} \) capacity:
   \[ Q(N_1 \otimes N_2) > 0, \quad Q(N_1) = 0 \]
5. Erasure channel.
\[ A : \mathcal{V} | (i,j) \rangle \rightarrow \sum_l |i\rangle |j\rangle + |i\rangle |j\rangle \tfrac{1}{2} \]

\[ A(p) = \text{Tr}_2 \mathcal{V}_p \mathcal{V}^+ \]

Define \( Q_{\text{SS}}^{(0)}(N) = Q^{(0)}(N \otimes A) \)

Then we have the following lemmas:

1. \( Q_{\text{SS}}^{(1)}(N \otimes M) = Q_{\text{SS}}^{(1)}(N) + Q_{\text{SS}}^{(1)}(M) \)

2. Recall coherent info for channel \( N \):

\[ \max_{\phi} \left[ S(\phi) - S(E) \right] \]

3. \( Q_{\text{SS}}^{(1)}(N) = Q^{(1)}(N \otimes A) \)

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

\[ = \max_{1(\phi) \text{AA}_A^B} \left[ I(A > B | E) \right] \]

\[ = \max_{\phi \text{AA}_A^B} \left[ I(A > B | E) \right] \]
Lemma 2

\[ Q_{SS} (N) = \max_{P_{AA'F'}} \frac{1}{2} \left[ I(A \rightarrow BF) - I(A \rightarrow EF) \right] \]

Why?

Pushing \( P_{AA'F'} \) as \( \{Y\} AA'FF' \).

\[ \Rightarrow \max_{\{Y\} AA'FF'} \frac{1}{2} \left[ I(A \rightarrow BF) + I(A \rightarrow BF') \right] \]

\[ \{Y\} AA'FF' \]

Proof:

\[ P_{AA'FF'} \]

\[ I(A \rightarrow BF) + I(A \rightarrow BF') \]

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

\[ I(A \rightarrow BF) \]

\[ I(A \rightarrow BF') \]

\[ I(A \rightarrow BF) \]
 Feed $A'$ to Channel 1:

\[ P_{AA', A} = \frac{1}{2} \left[ P_{AA}, f_1 \otimes |0\rangle \otimes |1\rangle + P_{AA'}, f_2 \otimes |1\rangle \otimes |1\rangle \right] \]

\[ \Sigma (A) B f_a \]

\[ = \frac{1}{2} \left[ \Sigma (A) B f + \Sigma (A) B f' \right] \]

By Lemma 10:

(17)

\[ \text{ISS} (N_1 \otimes N_2) : \]

\[ f_{AA, A2, f} \]

\[ \perp \]

\[ N_1 \perp N_2. \]
\[ N_0 = \frac{1}{2} \left[ I_c(A > B_1 B_2 F) - I_c(A > E_1 B_2 F) \right] \]

\[ = \frac{1}{2} \left[ I_c(A > B_1 B_2 F) - I_c(A > E_1 B_2 F) \right] \]

\[ + I_c(A > E_1 B_2 F) - I_c(A > E_1 E_2 F) \]

\[ \text{cancel out} \]

\[ \leq Q_{ss}^{(1)} (N_1) \]

\[ \leq Q_{ss}^{(1)} (N_2) \]

\[ \text{But the top line, otherwise, is } Q_{ss}^{(1)} (N_1 \cup N_2) \]

\[ \leq Q_{ss}^{(1)} (N_1) + Q_{ss}^{(1)} (N_2) \]
The opposite direction:

\[ x_{ss} (N_1 \otimes N_2) > q_{ss} (N_1) + q_{ss} (N_2) \]

is easy, by choosing a particular input for the coherent info \( \Phi_{AA,F_i} \otimes \Phi_{\tilde{A}_2,F_2} \)

where \( \Phi_{AA,F_i} \) is obtained for \( N_i \)

\( \Phi_{\tilde{A}_2,F_2} \) - - - - - \( N_2 \).

\[ \text{Lemma 1 holds.} \]

NB: max should be \( \leq \dim F \) is not unknown here.
Private capacity of a channel.

Ref: Csiszar & Körner 78
"broadcast channels with confidential messages"

Devetak 03 04 17

\[
P^{(1)}(N) = \max_{\{p_{X,Y}, q_Y\}} \left[ I(X;B) - I(X;Z) \right]
\]

Evaluated on
\[
\sum_x p_x p_x |x| x |x| x |U_N \otimes \phi_x \otimes U_N^x|
\]
Intuition:

Output space of channel $S(B)$

$$\phi_1, \phi_2, \ldots, \phi_n$$

How much space? $nS(B|x)$

Can code $\frac{2^n S(B)}{nS(B|x)} \approx 2^{nI(X;B)}$ messages.

$\mathcal{D}$
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 \( \left\lfloor \frac{\ln n}{\ln 2} \right\rfloor \) in a single bin, each bin fills Bob's space, so she may find out.
(3) PPT states.

HHHO 2003

\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}} \left( |10\rangle_{AB} + |11\rangle_{AB} \right) \]

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

\[ |\Phi^+\rangle \otimes \left( |\psi^+\rangle^{AB} + |\psi^-'\rangle^{AB} \right) \quad \text{for } \quad |\psi^+\rangle = \frac{\phi^+}{\sqrt{2}} \]

Same as before.

\[ U^{ABab} = \sum_{i,j} \begin{bmatrix} |i\rangle \langle j| \end{bmatrix}^{AB} \otimes \begin{bmatrix} \phi^+ \end{bmatrix}^{ab} \]

for \[ U^{ABab} = \sum_{i,j} \begin{bmatrix} |i\rangle \langle j| \end{bmatrix}^{AB} \otimes \begin{bmatrix} \phi^+ \end{bmatrix}^{ab} \]

\[ |\Phi^+\rangle \]

State given to Alice & Bob.
Measuring $\rho_{AB}$ basis on A & B.

Commutes with the unitary.

Sam out came

also does NOT leak info to Eve!

So the state has "privacy" but little
for properly chosen $\mathcal{U}_{ABAB}$, has little distillable
entanglement.

Now add a little separable state $\delta$.

St. $\rho + \delta$ is PPT,

the bipartite yet there is residual privacy.
\[ \exists N \text{ s.t. } Q(N) = 0 \quad \& \quad P^{(1)}(N) > 0. \]

See Pankowski, H., H., 1966.

2 qubits x 2 qubits.

(4) Entropy activation.

Consider
\[ Q_{ss}(N) = \max \frac{1}{2} \left[ \log \frac{1}{P_{A \rightarrow B | F}} - \log (A \rightarrow F) \right] \]
\[ P_{A \rightarrow F} \]

\[ = \max \frac{1}{2} \left[ -S(A \mid B F) + S(A \mid E F) \right] \]

\[ = \max \frac{1}{2} \left[ -S(A \mid B F) + S(A \mid E F) \right] \]

\[ = \max \frac{1}{2} \left[ -S(A \mid B) + S(A \mid E F) \right] \]

\[ -S(A \mid F) - S(A \mid E). \]
\[ P^{(1)}(N) = \max \left\{ I(X;F) - I(X;E) \right\} \]

\[ \sum_x p_x f_x \chi_x \phi_x \]

= above with final F, and without \( \frac{1}{2} \) factor.

\[ P^{(1)}(N) \leq 2 \times Q^{(1)}_{ss}(N) \]

\[ = 2 Q^{(1)}(N \setminus A) \]

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

Note also \( Q(A) = 0 \).

\[ 0 \leq Q^{(0)}(N \setminus A) \leq Q(N \setminus A) \]

Can use erasure channel (50-50) with in place of\( \text{ instead of } A \).