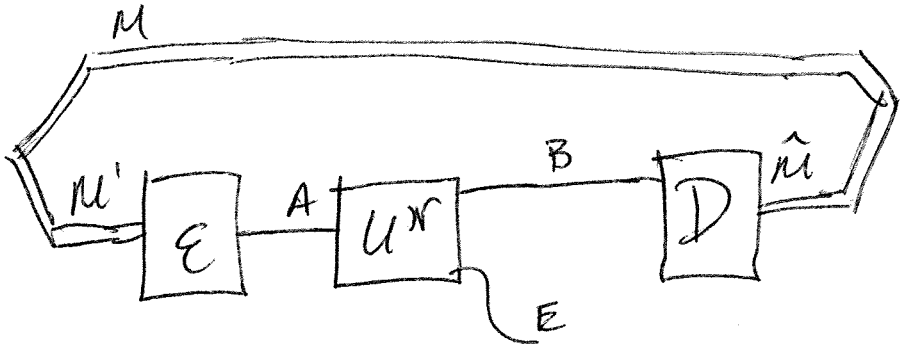
Lecture 28

- private communication.

As before, consider one-shot setting:



goal is to send a message m such that Bob can decode but Eve cannot.

Model Eve as having access to environment of channel "all powerful quantum eavesdropper"

Initial state of protocol is

$$\Phi^P_{MM'} = \sum_m p(m) |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{M'}$$

Final state of protocol is

$$\omega^P_{M\hat{M}E} = \left(D_{B\to\hat{M}} \circ \mathcal{U}^N_{A\to BE} \circ \mathcal{E}_{M'\to A}\right)\left(\Phi^P_{MM'}\right)$$

Defining $\mathcal{E}_{M'\to A}(|m\rangle\langle m|_{M'}) = \rho^m_A$

+

$$D_{B\to\hat{M}}(\tau_B) = \sum_{\hat{m}} \mathrm{Tr}\left[\Lambda^{\hat{m}}_B \tau_B\right] |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}$$

we can write final state as

$$\omega^P_{M\hat{M}E} = \sum_{m,\hat{m}} p(m) \underbrace{|m\rangle\langle m|_M \otimes |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}}_{q(\hat{m}|m)} \otimes \omega^{m,\hat{m}}_E$$

where $q(\hat{m}|m) = \mathrm{Tr}\left[\Lambda^{\hat{m}}_B \mathcal{U}^N_{A\to BE}(\rho^m_A)\right]$

$$\omega^{m,\hat{m}}_E = \mathrm{Tr}_B\left[\Lambda^{\hat{m}}_B \mathcal{U}^N_{A\to BE}(\rho^m_A)\right] / q(\hat{m}|m)$$

How to measure performance?

we want reliability & secrecy

1) reliability is the same as before

$$P_{err}(m) = 1 - q(m|m) \leq \varepsilon \quad \forall m \in \mathcal{M} \quad (I)$$

2) secrecy: we want that there exists a state σ_E such that

$$F\left(\sigma_E, \mathcal{N}^c_{A\to E}\left(\rho_A^m\right)\right) \geq 1-\varepsilon \quad \forall m \in \mathcal{M} \quad (II)$$

If this holds, then the eavesdropper's state is approximately independent of the message.

We can capture both of these requirements w/ a single-error criterion

$$p^*_{err} = \inf_{\sigma_E} \max_{m \in \mathcal{M}} \left\{ 1 - F\left(|m\rangle\langle m|_{\hat{M}} \otimes \sigma_E, \mathcal{P}_{M' \to \hat{M}E}(|m\rangle\langle m|_{M'}) \right) \right\}$$

where

$$\mathcal{P}_{M' \to \hat{M}E} = \mathcal{D}_{B \to \hat{M}} \circ \mathcal{U}^{\mathcal{N}}_{A \to BE} \circ \mathcal{E}_{M' \to A}$$

↑ protocol.

can show that $p^*_{err} \leq \varepsilon$

$\Rightarrow$ (I) + (II)

one-shot private capacity

$$P^{\varepsilon}(\mathcal{N}) = \sup_{(M, \mathcal{E}, \mathcal{D})} \left\{ \log_2 |M| : p^*_{err} \leq \varepsilon \right\}$$

Converse bounds

can show that

$$P^{\varepsilon}(N) \leq E_R^{\varepsilon}(N)$$

↑ ε-relative entropy of entanglement

$$E_R^{\varepsilon}(N) = \sup_{\psi_{SA}} \inf_{\sigma_{SB} \in SEP} D_H^{\varepsilon}(N_{A\to B}(\psi_{SA}) \| \sigma_{SB})$$

comparison between channel output state and a separable state

- basic idea is that we are comparing output state to one that is useless for generating privacy.
- separable states have no privacy b/c the hidden variable could be known to eavesdropper.

There is another converse bound

First define smooth max-mutual information of bipartite state ρ_{AE}

$$I_{\max}^{\sqrt{\varepsilon}}(A;E)_\rho = \inf_{\tilde{\rho}_{AE}:} \inf_{\tau_E} D_{\max}(\tilde{\rho}_{AE} \| \tilde{\rho}_A \otimes \tau_E)$$

$$F(\rho_{AE}, \tilde{\rho}_{AE}) \geq 1-\varepsilon$$

where $D_{\max}(\omega\|\tau) = \inf\{\lambda : \omega \leq 2^\lambda \tau\}$

Claim:

$$P^\varepsilon(\mathcal{N}) \leq \sup_{\{p(x), \rho_A^x\}_x} \left[I_H^\varepsilon(X;B)_\rho - I_{\max}^{\sqrt{\varepsilon}}(X;E)_\rho \right]$$

where

$$\rho_{XBE} = \sum_x p(x) |x\rangle\langle x| \otimes U_{A\to BE}^{\mathcal{N}}(\rho_A^x)$$

Proof: By same reasoning as before, we know that

$$\log_2 |\mathcal{M}| \leq I_{\#}^{\varepsilon}(M;B)_\tau$$

where $\tau_{MBE} = \frac{1}{|\mathcal{M}|} \sum_m |m\rangle\langle m|_M \otimes \mathcal{U}_{A\to BE}^{\mathcal{N}}(\rho_A^m)$

Also, from privacy criterion, $\exists$ state σ_E such that

$$\varepsilon \geq 1 - F(\tau_M \otimes \sigma_E, \tau_{ME})$$

$$\Rightarrow I_{\max}^{\sqrt{\varepsilon}}(M;E)_\tau \leq 0$$

b/c def. involves inf over $\tilde{\tau}_{ME}$

Pick $\tilde{\tau}_{ME} = \tau_M \otimes \sigma_E$

$$\Rightarrow I_{\max}^{\sqrt{\varepsilon}}(M;E)_\tau$$

$$\leq D_{\max}(\tau_M \otimes \sigma_E \| \tau_M \otimes \sigma_E)$$

$$= 0$$

$$\Rightarrow \log_2 |\mathcal{M}| \leq I_H^{\varepsilon}(\mathcal{M};B)_\tau - I_{max}^{\sqrt{\varepsilon}}(\mathcal{M};E)_\tau$$

Now optimize over all input ensembles to get

$$\log_2 |\mathcal{M}| \leq \sup_{\{p(x),\rho_A^x\}_x} \left[I_H^{\varepsilon}(X;B)_\rho - I_{max}^{\sqrt{\varepsilon}}(X;E)_\rho \right]$$

Lower bound

can show that

$$P^{\varepsilon}(N) \geq$$

$$\bar{I}_H^{\varepsilon'-\delta-\eta}(X;B)_\rho - \bar{I}_{max}^{\delta-\xi}(E;X) - \log_2\left(\frac{8(\varepsilon'-\delta)}{\eta^2}\right) - \log_2\left(\frac{2}{\xi^2}\right)$$

where $\varepsilon' = 1-\sqrt{1-\varepsilon/2}$,

$\delta \in (0,\varepsilon')$, $\eta \in (0,\varepsilon'-\delta)$, $\xi \in (0,\delta)$

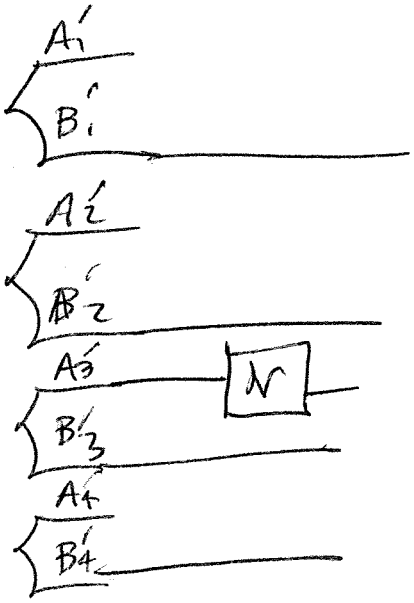
where

$$\rho_{XBE} = \sum_x p(x) |x\rangle\langle x|_X \otimes \mathcal{N}_{A\to BE}(\rho^x_A)$$

Main idea behind proof is to use position-based coding combined w/ another technique called convex split.

Let us discuss convex split

Consider scenario of position-based coding



Suppose Alice chooses message uniformly @ random, rather than deterministically

For fixed m, recall that the state is

$$\rho_{B_1'} \otimes \cdots \otimes \rho_{B_{m-1}'} \otimes \rho_{BB_m'} \otimes \rho_{B_{m+1}'} \otimes \cdots \otimes \rho_{B_M'}$$

If m is random, then state is the mixture

$$\tau = \frac{1}{M} \sum_{m=1}^{M} \rho_{B_1'} \otimes \cdots \otimes \rho_{B_{m-1}'} \otimes \rho_{BB_m'} \otimes \rho_{B_{m+1}'} \otimes \cdots \otimes \rho_{B_M'} \quad (*)$$

As M gets larger, it becomes more difficult to distinguish the above state from a product state

$$\rho_{B_1'} \otimes \cdots \otimes \rho_{B_M'} \otimes \rho_B$$

Intuition: look @ reduced state of $(*)$ on $B_i' + B$:

$$\tau_{BB'} = \frac{1}{M} \rho_{BB'} + \left(1 - \frac{1}{M}\right) \rho_B \otimes \rho_{B'}$$

Roughly speaking,

$$\rho_{BB'} \leq 2^{D_{max}(\rho_{BB'} \| \rho_B \otimes \rho_{B'})} \rho_B \otimes \rho_{B'}$$

$$\Rightarrow \quad \tau_{BB'} \leq \underbrace{\left(\frac{2^{D_{max}}}{M} \right)}_{\text{key relation}} + 1 - \frac{1}{M} \rho_B \otimes \rho_{B'}$$

if $\log_2 |M| \simeq D_{max}(\rho_{BB'} \| \rho_B \otimes \rho_{B'})$

then $\tau_{BB'}$ looks like product state $\rho_B \otimes \rho_{B'}$

---

can use this intuition to get the following:

if $$\log_2 |M| \geq \overline{I}_{max}^{\varepsilon - \eta}(B;B')_\rho + \log_2\left(\frac{2}{\eta^2}\right)$$

then there exists a state $\tilde{\rho}_B$ such that

$$F(\tau, \rho_{B_1} \otimes \cdots \otimes \rho_{B_M} \otimes \tilde{\rho}_B) \geq 1 - \varepsilon^2$$

Idea for protocols (Wyner) 1970s

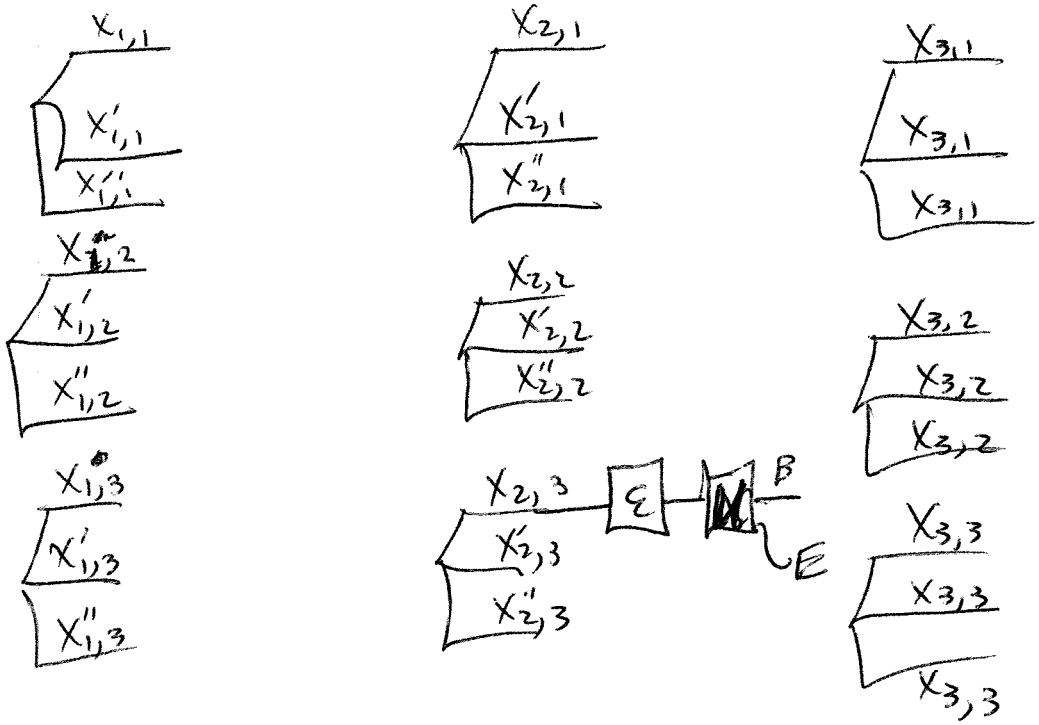
Message variable $m \in \{1, \ldots, M\}$

local randomness variable $r \in \{1, \ldots, R\}$

Alice, Bob, Eve share $M \cdot R$ copies of

$$\rho_{XX'X''} = \sum_x p(x) |xxx\rangle\langle xxx|_{XX'X''}$$

Example: $X_{m,r}$ Pick $m=2, r=3$



If Alice wants to send message m, she picks r @ random from $\{1, \ldots, R\}$ + sends system $X_{m,r}$ through encoder + channel,

For fixed m+r state is

$$\rho^{mr}_{X^M R X'^M R X''^M R B E} = \rho_{X_{1,1} X'_{1,1} X''_{1,1}} \otimes \cdots \otimes$$

$$\rho_{X_{m,r-1} X'_{m,r-1} X''_{m,r-1}} \otimes \rho_{X_{m,r} X'_{m,r} X''_{m,r} B E} \otimes$$

$$\rho_{X_{m,r+1} X'_{m,r+1} X'_{m,r+1}} \otimes \cdots \otimes \rho_{X_{M,R} X'_{M,R} X''_{M,R}}$$

adopt shorthand $\underline{X}_{i,j} = X_{i,j} X'_{i,j} X''_{i,j}$

~~For fixed m+r~~

Bob can then use position-based coding to figure out m+r as long as

$$\log_2 |MR| = \bar{I}_H^{\varepsilon - n}(X;B)_\rho - \log_2\left(\frac{4\varepsilon}{n^2}\right)$$

For fixed value of m, state of Eve is

$$\rho^m_{X''MR_E} =$$

$$\frac{1}{R}\sum_{r=1}^{R} \rho_{X''_{1,1}} \otimes \cdots \otimes \rho_{X''_{m,r-1}} \otimes \rho_{X''_{m,r}E} \otimes \rho_{X''_{m,r+1}} \otimes \cdots \otimes \rho_{X''_{MR}}$$

From convex split, if we take $\log_2 R = \bar{I}_{max}^{\sqrt{\varepsilon} - n}(E;X)_\rho + \log_2\left(\frac{2}{n^2}\right)$

then we are guaranteed that

$$1 - F\left(\rho^m_{X''MRE}, \rho_{X''_{1,1}} \otimes \cdots \otimes \rho_{X''_{MR}} \otimes \tilde{\rho}_E\right) \leq \varepsilon$$

Thus, the # of private bits transmitted is

$$\log_2 M = \overline{I}_H^{\varepsilon-\eta}(X;B) - \overline{I}^{\sqrt{\varepsilon}-\eta}(E;X)_\rho - \log_2\left(\frac{4\varepsilon}{\eta^2}\right) - \log_2\left(\frac{2}{\eta^2}\right)$$

From here, we combine different notions of error into a single error, derandomize, expurgate, & arrive @ the claim.