Locking vs. private capacity of quantum channels

Andreas Winter (ICREA & UAB Barcelona)

[Based on S. Guha et al., arXiv:1307.5368
and AW, arXiv:1403.6361]

Locking vs. private capacity of quantum channels

Andreas Winter (ICREA & UAB Barcelona)

[Based on S. Guha et al., arXiv:1307.5368
and AW, arXiv:1403.6361]

Poster by Cosmo Lupo

Outline

1. Quantum channels and capacities

2. Notions of privacy

3. The (weak) locking capacity

4. An achievable rate for L_W: two examples

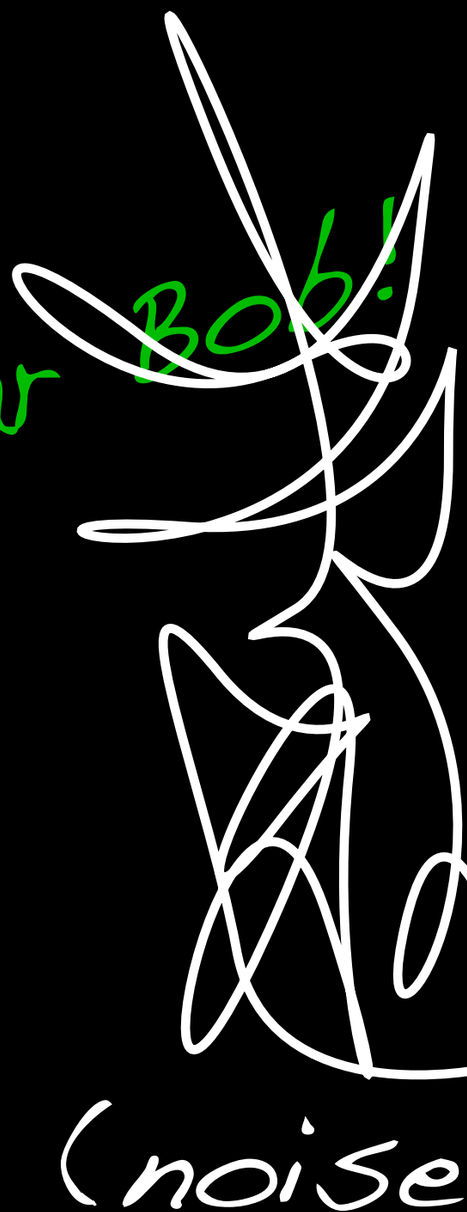
5. Discussion

1. Communication

Dear Bob!

Shannon (1948): Fundamental problem is that of reproducing at one point a message selected at another point.

1. Communication

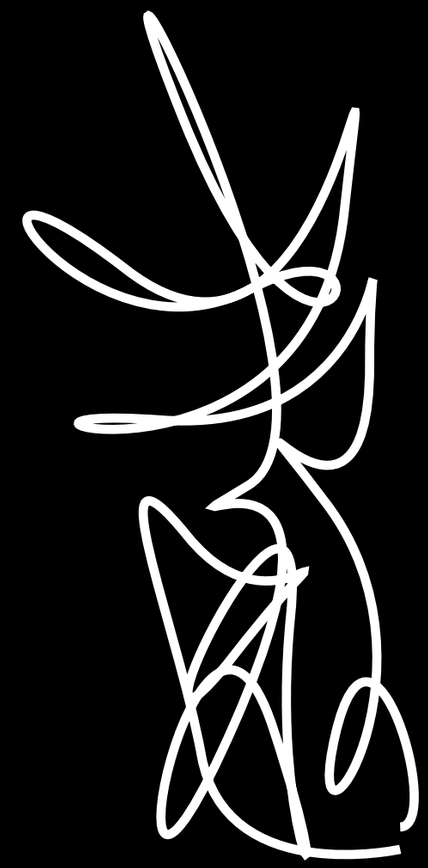


1. Communication

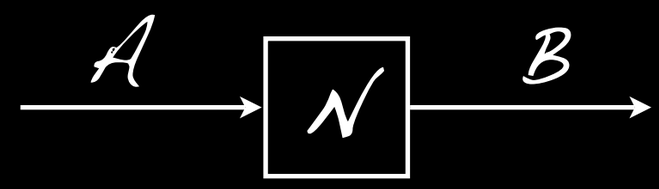
Deep throat?

1½. Channels & capacities

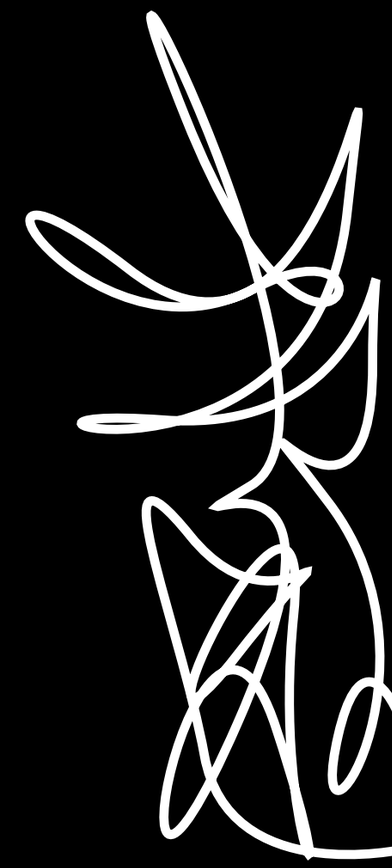
Noise

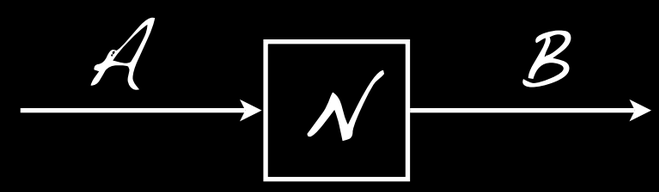


modelled as "channel":



1½. Channels & capacities

Noise  modelled as "channel":



Channel = cptp map $N: L(A) \longrightarrow L(B)$,

where A, B are finite-dim. Hilbert spaces.

Kraus representation, you know...

1½. Channels & capacities

Stinespring: $N(\rho) = Tr_E\, V \rho V^\dagger$,

with an isometry $V : A \hookrightarrow B \otimes E$.

1½. Channels & capacities

Stinespring: $N(\rho) = Tr_E\, V \rho V^\dagger$,

with an isometry $V: A \hookrightarrow B \otimes E$.

Complementary channel:

$$\widehat{N}(\rho) = Tr_B\, V \rho V^\dagger$$

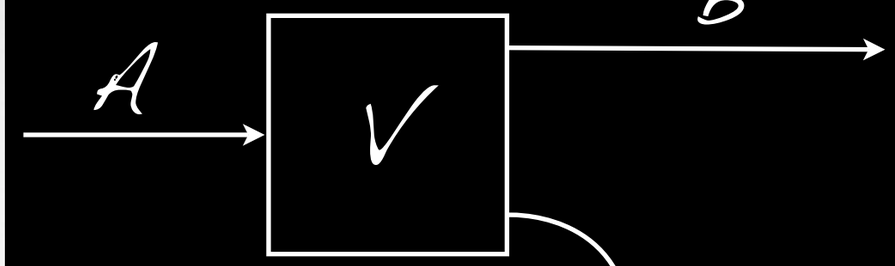
1½. Channels & capacities

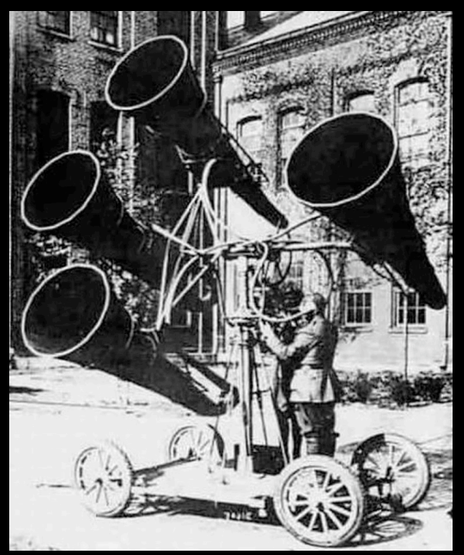
Stinespring: $N(\rho) = Tr_E\, V \rho V^\dagger$,

with an isometry $V: A \hookrightarrow B \otimes E$.

Complementary channel:

$\widehat{N}(\rho) = Tr_B\, V \rho V^\dagger$.





1½. Channels & capacities

Ex: 1) Noiseless channel = identity id_A.

2) Constant channel $K(\rho) = \omega_0$.

3) Depolarizing channels

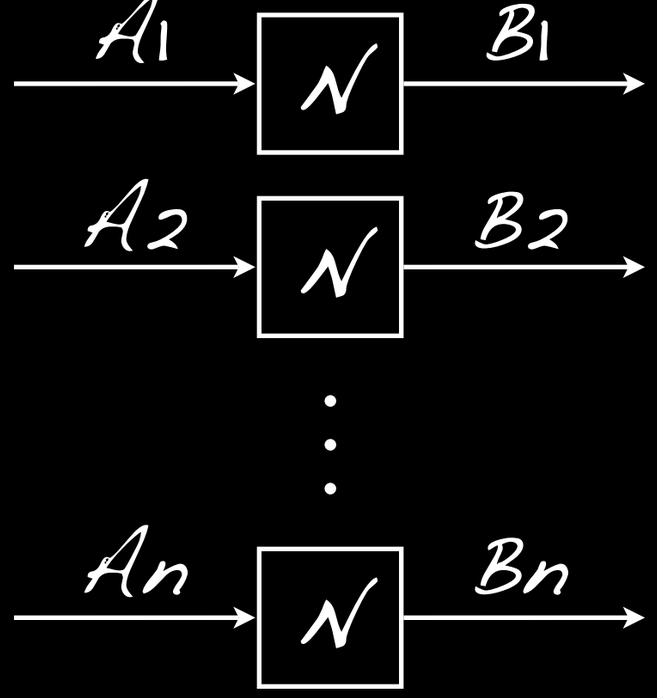
4) Amplitude damping channels

5) Phase damping channels

6) Erasure channel $\epsilon_g(\rho) = (1-g)\rho \oplus g|*\rangle\langle *|$

Classical capacity $C(\mathcal{N})$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free transmission over $\mathcal{N}^{\otimes n}$.

Classical capacity $C(\mathcal{N})$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free transmission over $\mathcal{N}^{\otimes n}$.



Classical capacity $C(\mathcal{N})$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free transmission over $\mathcal{N}^{\otimes n}$.

message of $k=K(n,\varepsilon)$ bits

Classical capacity $C(\mathcal{N})$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free transmission over $\mathcal{N}^{\otimes n}$.

message of $k=k(n,\varepsilon)$ bits

$=m$ with prob $\geq 1-\varepsilon$

Thm (Holevo and Schumacher/Westmoreland, 1973 and 1996/7):

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\chi(\mathcal{N}^{\otimes n}), \text{ with}$$

$\chi(\mathcal{N}) = \max I(X:B)$ wrt. $\{p_x, \rho_x\}$ and

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{N}(\rho_x).$$

Thm (Holevo and Schumacher/Westmoreland, 1973 and 1996/7):

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\chi(\mathcal{N}^{\otimes n}), \text{ with}$$

$$\chi(\mathcal{N}) = \max I(X:B) \text{ wrt. } \{p_x, \rho_x\} \text{ and}$$

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{N}(\rho_x).$$

Holevo information $S(\rho^B) - \sum_x p_x S(\mathcal{N}(\rho_x))$

Von Neumann entropy: $S(\rho) = -\mathrm{Tr}\ \rho \log \rho$

Unfortunately,

$\chi(\mathcal{N}) = \max I(X:B)$ wrt. $\{p_x, \rho_x\}$ and

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{N}(\rho_x)$$

is not additive in general [Hastings, Nat. Phys 2009], hence $C(\mathcal{N}) > \chi(\mathcal{N})$ possible.

Unfortunately,

$\chi(\mathcal{N}) = \max I(X:B)$ wrt. $\{p_x, \rho_x\}$ and

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{N}(\rho_x)$$

is not additive in general [Hastings, Nat. Phys 2009], hence $C(\mathcal{N}) > \chi(\mathcal{N})$ possible.

However, for some classes of channels it is, and we know the classical capacity $C(\mathcal{N})$ as $\chi(\mathcal{N})$.

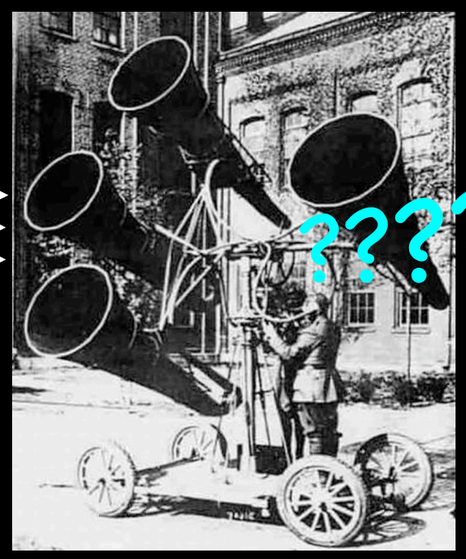
Private capacity $P(N)$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free and secret transmission over $N^{\otimes n}$.

m → ρ_m

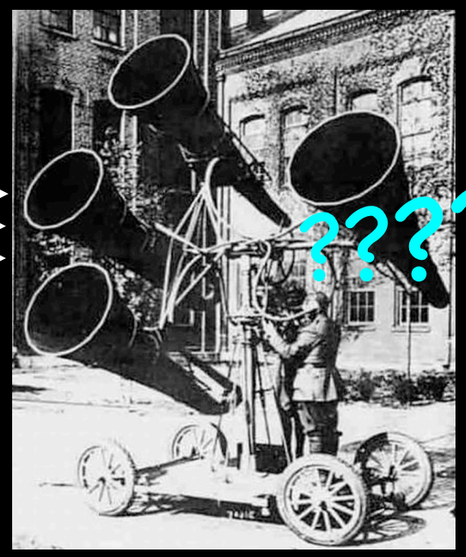
$\hat{m}$

error $\leq \varepsilon$

message of $k=K(n,\varepsilon)$ bits



??????



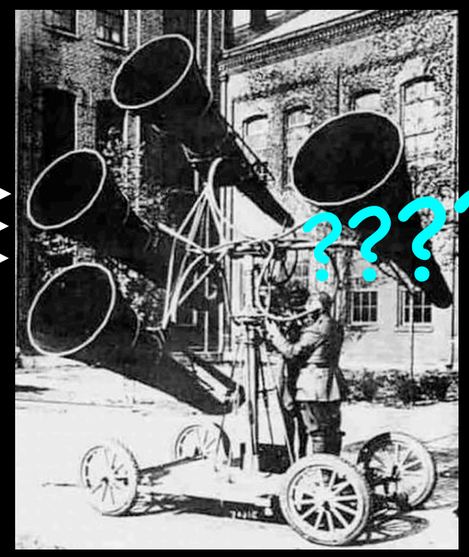
$m \rightarrow \rho_m$

A_1 A_2 A_n — V — B_1 B_2 B_n E_1 E_n

$D \rightarrow \hat{m}$

??????

In QKD: Eve provides the channel; i.i.d. means (known) "collective attack".



$m \rightarrow \rho_m$ A_1 A_2 A_n V V V B_1 B_2 B_n D $\hat{m}$ E_1 E_n

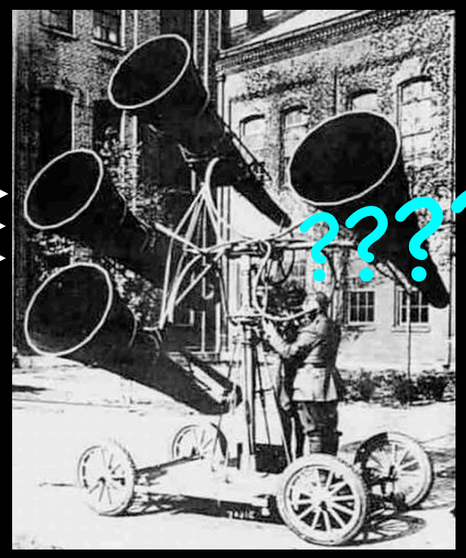
??????

In QKD: Eve provides the channel; i.i.d. means (known) "collective attack".

Privacy definition is subtle...

$m \longrightarrow \rho_m$ $\quad A_1 \to V \to B_1$ $\quad A_2 \to V \to B_2$ $\quad \vdots$ $\quad A_n \to V \to B_n$ $\quad D \to \hat{m}$

$V \to E_1, \ldots, E_n$



??????

Privacy definition: In the past, would assume that "at the end", Eve measures, so demand $I_{acc}(M:E^n) \approx 0$.

Nowadays: $I(M:E^n) \approx 0$.

2. Notions of privacy

Assume that messages $m=1,\dots,M$ are uniformly distributed (as if it was secret key). Then, at the end of any protocol, Alice, Bob & Eve share a state

$$\omega = \frac{1}{M}\sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

2. Notions of privacy

Assume that messages $m=1,\dots,M$ are uniformly distributed (as if it was secret key). Then, at the end of any protocol, Alice, Bob & Eve share a state

$$\omega = \frac{1}{M}\sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

Neglect errors between A & B ✓

2. Notions of privacy

Assume that messages $m=1,\ldots,M$ are uniformly distributed (as if it was secret key). Then, at the end of any protocol, Alice, Bob & Eve share a state

$$\omega = \frac{1}{M}\sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

Old style: Eve has to measure, some POVM (Q_j); require that j almost independent of m.

$$\omega = \frac{1}{M} \sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M} \mathrm{Tr}\ \rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \leq \varepsilon \quad (*)$

[Cf. Mayers, J. ACM 2001;
Scarani et al. Rev. Mod. Phys, 2009]

$$\omega = \frac{1}{M} \sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M} \mathrm{Tr}\ \rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \leq \varepsilon \quad (*)$

[Cf. Mayers, J. ACM 2001;
Scarani et al. Rev. Mod. Phys, 2009]

Information locking [DiVincenzo et al., PRL 2004; Hayden et al., CMP 2004; Koenig et al., PRL 2007]: states uniformly mixed over k d-dimensional bases, $k<\mathrm{polylog}(d)$, with $(*)$.

$$\omega = \frac{1}{M}\sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M}\,\mathrm{Tr}\,\rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \le \varepsilon \quad (*)$

[Cf. Mayers, J. ACM 2001; Scarani et al. Rev. Mod. Phys, 2009]

Information locking [DiVincenzo et al., PRL 2004; Hayden et al., CMP 2004; Koenig et al., PRL 2007]: states uniformly mixed over k d-dimensional bases, $k<\mathrm{polylog}(d)$, with $(*)$. Clearly insecure: if Eve can delay measurement until she learns basis, she can measure m!

$$\omega = \frac{1}{M} \sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M} \operatorname{Tr} \rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \leq \varepsilon \quad (*)$

[Cf. Mayers, J. ACM 2001;
Scarani et al. Rev. Mod. Phys, 2009]

Prompted "composable" security definition

[Renner, PhD thesis, quant-ph/0512258]: $I(M:E) \leq \varepsilon$.

$$\omega = \frac{1}{M} \sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M} \operatorname{Tr} \rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \leq \varepsilon \quad (*)$

[Cf. Mayers, J. ACM 2001;
Scarani et al. Rev. Mod. Phys, 2009]

Prompted "composable" security definition

[Renner, PhD thesis, quant-ph/0512258]: $I(M:E) \leq \varepsilon$.

$$I(M:E) = S(\omega^E) - \sum_m p(m)\, S(\rho_m)$$

$$\omega = \frac{1}{M} \sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$\Pr\{M=m,\ J=j\} = \frac{1}{M} \mathrm{Tr}\ \rho_m Q_j$$

Require: $\max_Q I(M:J) =: I_{acc}(M:E) \leq \varepsilon$ (*)

[Cf. Mayers, J. ACM 2001;
Scarani et al. Rev. Mod. Phys, 2009]

Prompted "composable" security definition

[Renner, PhD thesis, quant-ph/0512258]: $I(M:E) \leq \varepsilon$.

This doesn't have the unlocking problem; in fact, says that ρ_m^E almost independent of m.

[More history in review by Scarani et al. Rev. Mod. Phys, 2009]

$$\omega = \frac{1}{M}\sum_m |m\rangle\langle m|^{AB} \otimes \rho_m^E$$

$$Pr\{M=m,\ J=j\} = \frac{1}{M}\,Tr\,\rho_m Q_j$$

Remark: The gap between $I(M:E)$ and $I_{acc}(M:E) = \max_Q I(M:J)$ is precisely the discord of the state ω.

Private capacity $P(N)$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free and secret transmission over $N^{\otimes n}$.

Privacy (composable):

$I(M:E^n) \leq \delta$

Capacity formula for $P(N)$:

Thm (Devetak and Cai/Yeung/AW, 2003):

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

$$P^{(1)}(N) = \max I(X:B) - I(X:E) \text{ wrt. } \{p_x, \rho_x\}$$

Capacity formula for $P(\mathcal{N})$:

Thm (Devetak and Cai/Yeung/AW, 2003):

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

$$P^{(1)}(\mathcal{N}) = \max I(X:B) - I(X:E) \text{ wrt. } \{p_x, \rho_x\}$$

Quantum analogue of a famous result by Wyner [Bell Syst. Tech. J., 1975] & Csiszár/Körner [IEEE-IT, 1978]. Only that for classical channels, $P^{(1)}$ equals the private capacity; in general, the above has an additivity issue. Also P is not additive!

Capacity formula for $P(\mathcal{N})$:

Thm (Devetak and Cai/Yeung/AW, 2003):

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

$$P^{(1)}(\mathcal{N}) = \max I(X:B) - I(X:E) \text{ wrt. } \{p_x, \rho_x\}$$

For degradable channels (i.e. $\hat{\mathcal{N}} = \mathcal{D}\circ\mathcal{N}$):
$P(\mathcal{N}) = P^{(1)}(\mathcal{N}) = \max S(\mathcal{N}(\rho)) - S(\hat{\mathcal{N}}(\rho))$,
equals the quantum capacity of $\mathcal{N}$.

Capacity formula for $P(\mathcal{N})$:

Thm (Devetak and Cai/Yeung/AW, 2003):

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

$$P^{(1)}(\mathcal{N}) = \max I(X:B) - I(X:E) \text{ wrt. } \{p_x, \rho_x\}$$

For degradable channels (i.e. $\hat{\mathcal{N}} = \mathcal{D}\circ\mathcal{N}$):
$P(\mathcal{N}) = P^{(1)}(\mathcal{N}) = \max S(\mathcal{N}(\rho)) - S(\hat{\mathcal{N}}(\rho))$,
equals the quantum capacity of $\mathcal{N}$.

For symmetric $\mathcal{N} = \hat{\mathcal{N}}$: $P(\mathcal{N}) = 0$.

3. (Weak) locking capacity

If we assume - following the old quantum cryptography - that Eve measures after obtaining all information from the protocol, we effectively ask only that her accessible information is small.

3. (Weak) locking capacity

If we assume - following the old quantum cryptography - that Eve measures after obtaining all information from the protocol, we effectively ask only that her accessible information is small.

Let's take that seriously: "quantum enigma machines" [Lloyd, arXiv:1307.0380; Guha et al., arXiv:1307.5368] ...

Locking capacity $L_W(N)$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free and accessible-secret transmission over $N^{\otimes n}$?

m

ρ_m

$k = K(n, \varepsilon)$ bits

A_1 A_2 A_n

V V V

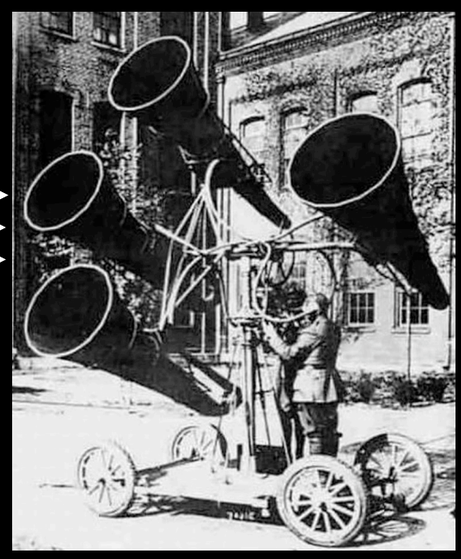
B_1 B_2 B_n

D

$\hat{m}$

error $\leq \varepsilon$

E_1 E_n



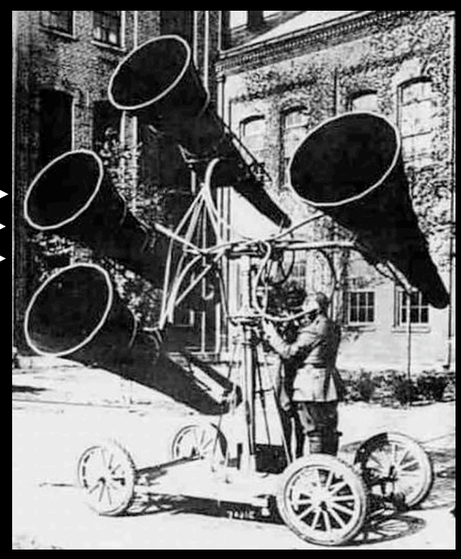
Locking capacity $L_W(N)$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free and accessible-secret transmission over $N^{\otimes n}$.

$k = K(n, \varepsilon)$ bits

error $\leq \varepsilon$

Privacy (wrt measurement):

$I_{acc}(M:E^n) \leq \delta$

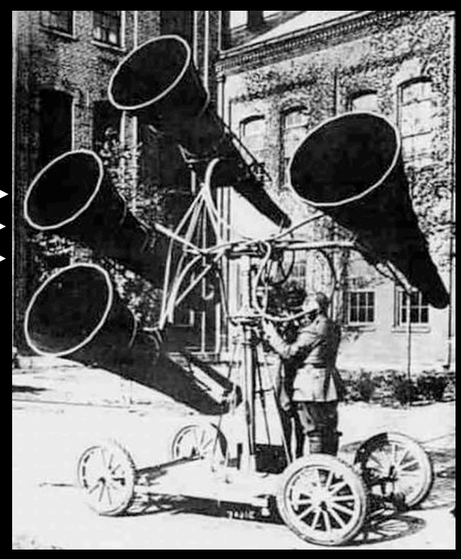


Locking capacity $L_W(N)$:= maximum cbit rate $\frac{k}{n}$ for asymptotically error-free and accessible-secret transmission over $N^{\otimes n}$.

A&B preshare $o(n)$ key

Privacy (wrt measurement):

$I_{acc}(M:E^n) \leq \delta$



Bounds on $L_w(N)$ - clearly $\geq P(N)$:

* If N is entanglement-breaking, then
  $P(N) = L_w(N) = 0$.

[Guha et al., arXiv:1307.5368]

Bounds on $L_W(N)$ - clearly $\geq P(N)$:

* If N is entanglement-breaking, then $P(N) = L_W(N) = 0$.

  [Because then N has rank-one Kraus operators, and so Eve can make a measurement, only depending on N, s.t. Alice & Bob are independent conditioned on Eve's outcome.]

[Guha et al., arXiv:1307.5368]

Bounds on $L_w(N)$ - clearly $\geq P(N)$:

* If N is entanglement-breaking, then $P(N) = L_w(N) = 0$.

* $L_w(N) \leq \lim_{n\to\infty} \frac{1}{n} L_w^{(u)}(N^{\otimes n})$, with

$$L_w^{(u)}(N) = \max I(X:B) - I_{acc}(X:E)$$
$$\text{wrt. } \{p_x, \rho_x\}$$

[Guha et al., arXiv:1307.5368]

Bounds on $L_w(N)$ – clearly $\geq P(N)$:

* If N is entanglement-breaking, then $P(N) = L_w(N) = 0$.

* $L_w(N) \leq \lim_{n\to\infty} \frac{1}{n} L_w^{(u)}(N^{\otimes n})$, with

$$L_w^{(u)}(N) = \max \underbrace{\{I(X:B) - I_{acc}(X:E)\}}_{\text{wrt. } \{p_x, \rho_x\}}$$

Cf. Csiszár-Körner-Devetak expression

[Guha et al., arXiv:1307.5368]

Bounds on $L_W(N)$ – clearly $\geq P(N)$:

* If N is entanglement-breaking, then $P(N) = L_W(N) = 0$.

* $L_W(N) \leq \lim_{n\to\infty} \frac{1}{n} L_W^{(u)}(N^{\otimes n})$, with

$$L_W^{(u)}(N) = \max I(X:B) - I_{acc}(X:E) \quad \text{wrt. } \{p_x, \rho_x\}$$

Not known to be attainable! Before, no separation between P and L_W was known.

[Guha et al., arXiv:1307.5368]

4. Achievable rates for L_W

Summary of main findings:

1) A family of channels with $P(N) = 1$, but $L_W(N) = 1 + \frac{1}{2} \log d$.

2) A symmetric channel, hence $P(N) = 0$, but $L_W(N) > 0$.

4. Achievable rates for L_W

1) A family of channels with $P(N) = 1$, but $L_W(N) = 1 + \frac{1}{2}\log d$.

4. Achievable rates for L_W

1) A family of channels with $P(\mathcal{N}) = 1$, but $L_W(\mathcal{N}) = 1 + \frac{1}{2}\log d$.

Complementary $\hat{\mathcal{N}}$ is cq-channel:

$\hat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$

4. Achievable rates for L_W

1) A family of channels with $P(\mathcal{N}) = 1$, but $L_W(\mathcal{N}) = 1 + \frac{1}{2}\log d$.

Complementary $\hat{\mathcal{N}}$ is cq-channel:

$\hat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$, hence

$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|$ Schur multiplier.

4. Achievable rates for L_W

1) A family of channels with $P(\mathcal{N}) = 1$, but $L_W(\mathcal{N}) = 1 + \frac{1}{2}\log d$.

Complementary $\hat{\mathcal{N}}$ is cq-channel:

$\hat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$, hence

$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|$ Schur multiplier.

→ Degradable, thus $P(\mathcal{N})$ easy to compute.

4. Achievable rates for L_W

1) A family of channels with $P(\mathcal{N}) = 1$, but $L_W(\mathcal{N}) = 1 + \frac{1}{2}\log d$.

Complementary $\hat{\mathcal{N}}$ is cq-channel:

$\hat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$, hence

$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|$ Schur multiplier.

Degradable, thus $P(\mathcal{N})$ easy to compute.

Use only $|i\rangle\langle i|$ signals: no noise for Bob;

privacy from non-orthogonality of $|\psi_i\rangle$...

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

$$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|.$$

$$\widehat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$$

Alice: $I \sim (p_i)$

Average output:

$$\rho = \sum_i p_i \psi_i$$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

$$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|.$$

$$\widehat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$$

Alice: $I \sim (p_i)$

Average output:

$$\rho = \sum_i p_i \psi_i$$

For Eve's POVM (Q_j):

$$\Pr\{I=i, J=j\} = p_i \operatorname{Tr} \psi_i Q_j$$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

$$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|.$$

$$\widehat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$$

Alice: $I \sim (p_i)$

Average output:

$$\rho = \sum_i p_i \psi_i$$

For Eve's POVM (Q_j):

$$\Pr\{I=i, J=j\} = p_i \operatorname{Tr} \psi_i Q_j = q_j \operatorname{Tr} \sigma_j M_i$$

$$M_i = \rho^{-1/2}(p_i \psi_i)\rho^{-1/2} \;\&\; q_j \sigma_j = \rho^{1/2} Q_j \rho^{1/2}$$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

$$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|.$$

$$\widehat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$$

Alice: $I \sim (p_i)$

Average output:

$$\rho = \sum_i p_i \psi_i$$

For Eve's POVM (Q_j):

$$\Pr\{I=i, J=j\} = p_i \operatorname{Tr} \psi_i Q_j = q_j \operatorname{Tr} \sigma_j M_i$$

So: $H(I|J) \geq \min_{\sigma} H(\{\operatorname{Tr}\sigma M_i\}) =: H_0$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

$$\mathcal{N}(|i\rangle\langle j|) = \langle\psi_j|\psi_i\rangle\,|i\rangle\langle j|.$$

$$\widehat{\mathcal{N}}(|i\rangle\langle j|) = \delta_{ij}\,|\psi_i\rangle\langle\psi_j|$$

Alice: $I \sim (p_i)$

Average output:

$$\rho = \sum_i p_i \psi_i$$

For Eve's POVM (Q_j):

$$\Pr\{I=i, J=j\} = p_i \operatorname{Tr} \psi_i Q_j = q_j \operatorname{Tr} \sigma_j M_i$$

So: $H(I|J) \geq \min_{\sigma} H(\{\operatorname{Tr}\sigma M_i\}) =: H_0$

$\Rightarrow H_{\min}^{\varepsilon}(I^n|J) \geq n H_0 - o(n)$ for n copies.

[Damgaard et al., arXiv:quant-ph/0612014]

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

For Eve's POVM (Q_j) – on n copies:

$$H_{min}^{\varepsilon}(I^n|J) \geq n H_0 - o(n).$$

$$[H_0 := \min_{\sigma} H(\{\mathrm{Tr}\, \sigma M_j\})]$$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

For Eve's POVM (Q_j) – on n copies:

$$H_{\min}^{\varepsilon}(I^n|J) \geq n H_0 - o(n).$$

$$[H_0 := \min_{\sigma} H(\{\mathrm{Tr}\,\sigma M_j\})]$$

Hence: Hash I^n to M of length $\approx nH_0$, using seed of length $O(\log n)$, get

$$I_{\mathrm{acc}}(M:E^n) \leq o(1).$$

1) A family of channels with $P(\mathcal{N}) = 1$, but

$$L_W(\mathcal{N}) = 1 + \tfrac{1}{2}\log d.$$

For Eve's POVM (Q_j) – on n copies:

$$H_{\min}^{\varepsilon}(I^n|J) \geq n H_0 - o(n).$$

$$[H_0 := \min_{\sigma} H(\{\mathrm{Tr}\,\sigma M_j\})]$$

Hence: Hash I^n to M of length $\approx nH_0$, using seed of length $O(\log n)$, get

$$I_{acc}(M:E^n) \leq o(1).$$

Result: $L_W(\mathcal{N}) \geq H_0 = \min_{\sigma} H(\{\mathrm{Tr}\,\sigma M_j\})$

1) A family of channels with $P(N) = 1$, but $L_W(N) = 1 + \frac{1}{2}\log d$.

Result: $L_W(N) \geq H_0 = \min_{\sigma} H(\{T_i \sigma M_i\})$

Example: $|\psi_i\rangle$ X- and Z-eigenstates (2d), uniformly distributed, so $P(N) = 1$.

1) A family of channels with $P(N) = 1$, but

$L_W(N) = 1 + \frac{1}{2} \log d$.

Result: $L_W(N) \geq H_0 = \min_{\sigma} H(\{Tr_\sigma M_i\})$

Example: $|\psi_i\rangle$ X- and Z-eigenstates (2d),

uniformly distributed, so $P(N) = 1$.

$\Rightarrow$ M measures X or Z, with prob. ½.

Maassen/Uffink [PRL, 1988]: $H_0 = 1 + \frac{1}{2} \log d$.

1) A family of channels with $P(N) = 1$, but

$L_W(N) = 1 + \frac{1}{2} \log d$.

Result: $L_W(N) \geq H_0 = \min_{\sigma} H(\mathcal{E}\mathrm{Tr}_\sigma M)_\xi$

Example: $|\psi_i\rangle$ X- and Z-eigenstates (2d),

uniformly distributed, so $P(N) = 1$.

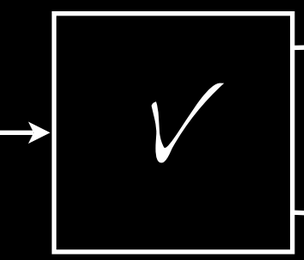
$\Rightarrow$ M measures X or Z, with prob. ½.

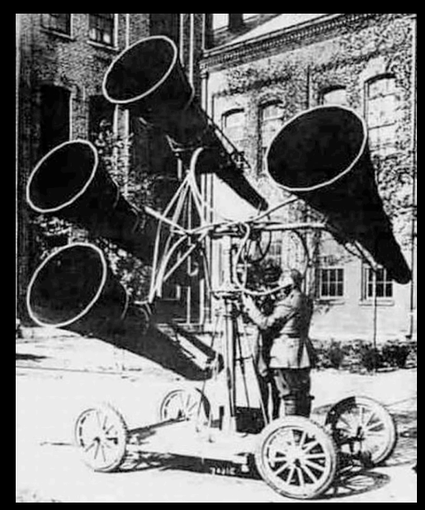
Maassen/Uffink [PRL, 1988]: $H_0 = 1 + \frac{1}{2} \log d$.

...happens to coincide with upper bound

of Guha et al.: $L_W(N) = 1 + \frac{1}{2} \log d$.

2) A symmetric channel, hence $P(N) = 0$,
but $L_W(N) > 0$.

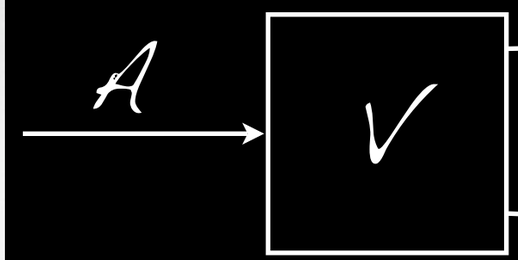


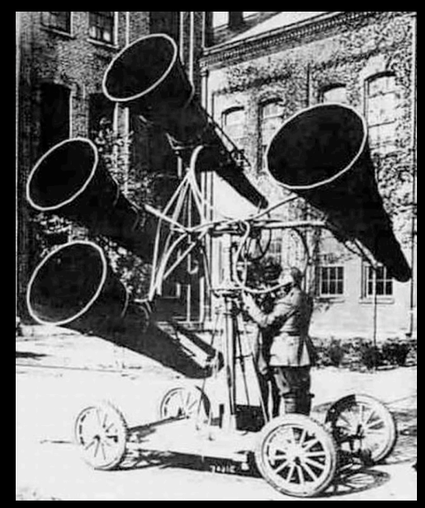


$|B| = |E| = d$,

A: symmetric subspace in BE

2) A symmetric channel, hence $P(N) = 0$,
but $L_W(N) > 0$.

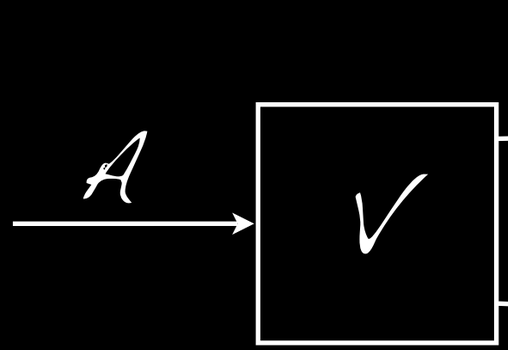


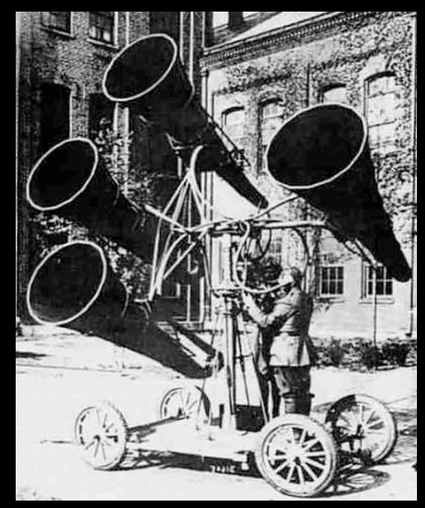


$|B| = |E| = d$,
A: symmetric subspace in BE

Same idea as before: use signals $|\psi_i\rangle|\psi_i\rangle$,
from X- and Z-eigenbases, but choose basis
by pre-shared key; same basis for blocks of
$1 \ll k \ll n$

2) A symmetric channel, hence $P(N) = 0$,
but $L_W(N) > 0$.

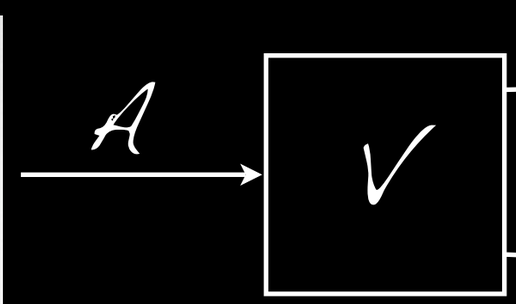


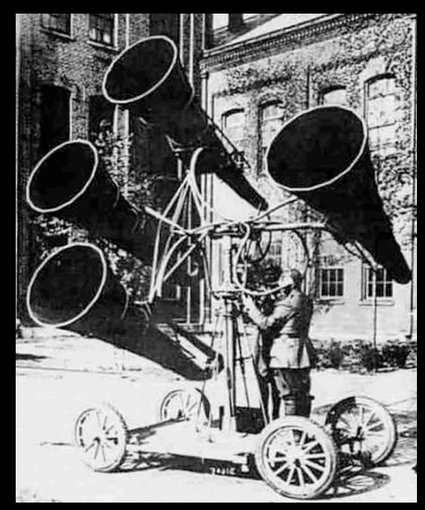


$|B| = |E| = d$,
A: symmetric subspace in BE

Same idea as before: use signals $|\psi_i\rangle|\psi_i\rangle$, from X- and Z-eigenbases, but choose basis by pre-shared key; same basis for blocks of $1 \ll k \ll n$ ... $L_W(N) \geq \frac{1}{2} \log d$.

2) A symmetric channel, hence $P(N) = 0$,
but $L_W(N) > 0$.





$|B| = |E| = d$,
A: symmetric subspace in BE

Same idea as before: use signals $|\psi_i\rangle|\psi_i\rangle$, from X- and Z-eigenbases, but choose basis by pre-shared key; same basis for blocks of $1 \ll k \ll n$ ... $L_W(N) \geq \frac{1}{2} \log d$. [Conj. $= \log d$]

5. Discussion

- Used entropic uncertainty relations/ information locking to show surprising lower bounds on locking capacity. In particular, even in completely insecure systems (Bob & Eve symmetric)!

5. Discussion

- Used entropic uncertainty relations/ information locking to show surprising lower bounds on locking capacity. In particular, even in completely insecure systems (Bob & Eve symmetric)!
- Compare with Koenig et al. [PRL, 2007], where it was shown in principle that locking can make a key appear secure. Here: realistic scheme of i.i.d. channels (i.e. collective attack).

5. Discussion

- Conjecture that Guha et al.'s upper bound

$$L_{w}^{(u)}(\mathcal{N}) = \max I(X:B) - I_{acc}(X:E)$$
$$\text{wrt. } \{p_x, \rho_x\}$$

is attainable, perhaps requiring a linear amount of activating pre-shared key.

5. Discussion

- Conjecture that Guha et al.'s upper bound

$$L_{\mathcal{W}}^{(u)}(\mathcal{N}) = \max I(X:B) - I_{acc}(X:E)$$
$$\text{wrt. } \{p_x, \rho_x\}$$

is attainable, perhaps requiring a linear amount of activating pre-shared key. (Would rely on proving an additivity relation for certain output Rényi entropies of qc-channels...)

5. Discussion

- Conjecture: for any i.i.d. ensemble $\{p_x, \rho_x\}^{\otimes n}$ and POVM (Q_j) on E^n,

$$H_{\min}^{\varepsilon}(X^n|J) \geq n\, S_{acc}(X|E) - o(n), \text{ where}$$

$$S_{acc}(X|E) := \min H(X|J) \text{ wrt } (Q_j) \text{ on } E.$$

[Compare Damgaard et al., arXiv:quant-ph/0612014]

5. Discussion

- Conjecture: for any i.i.d. ensemble $\{p_x, \rho_x\}^{\otimes n}$ and POVM (Q_j) on E^n,

$$H_{\min}^{\varepsilon}(X^n|J) \geq n\, S_{acc}(X|E) - o(n), \text{ where}$$

$$S_{acc}(X|E) := \min H(X|J) \text{ wrt } (Q_j) \text{ on } E.$$

[Compare Damgaard et al., arXiv:quant-ph/0612014]

- ...would follow from additivity of minimum conditional Rényi entropy $\min H_\alpha(X|J)$ wrt (Q_j) on E, $\alpha > 1$.

[Cf. AW, arXiv:1403.6361 & King, QIC 2003]