Distributed private randomness distillation

Dong Yang

Shenzhen Institute for Quantum Science and Engineering, SUSTech

joint work [PRL 123, 170501 (2019)] with
Karol Horodecki (Univ. Gdansk) and Andreas Winter (Univ. Autonoma Barcelona)

SUSTech-Nagoya workshop on Quantum Science 2022,
2 June 2022

Outline

Randomness

- randomness has various applications
- classical world: pseudo randomness
- quantum mechanics: true randomness

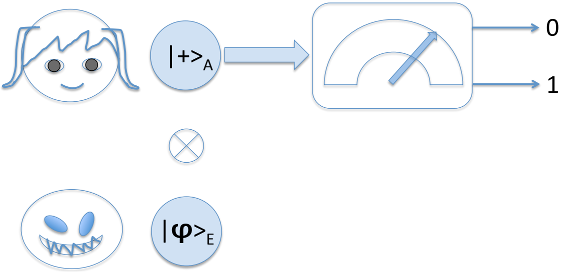


Figure: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, measurement basis $\{|0\rangle, |1\rangle\}$

private randomness

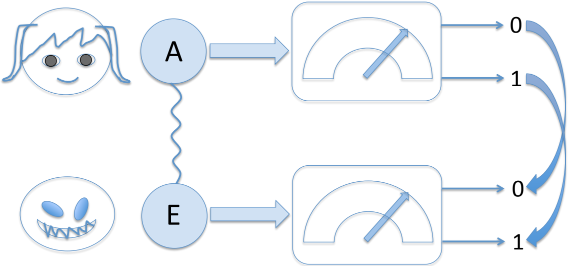
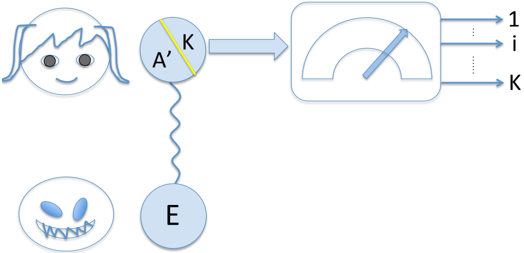


Figure: $|\Phi\rangle_{AE} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, measurement basis $\{|0\rangle, |1\rangle\}$

Local noise $\Phi_A = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ is useless by itself.

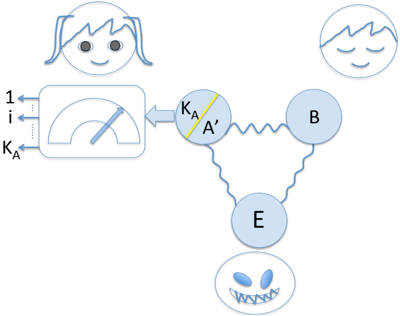
Berta/Fawzi/Wehner [IEEE Trans. Inf. Theory 60, 1168 (2014)]



$$\rho_{AE}^{\otimes n} \xmapsto{U_{A^n \to KA'}} \sigma_{KA'E^n} \xmapsto{\mathrm{Tr}_{A'}} \sigma_{KE^n} \xmapsto{M:|i\rangle_K} \sigma_{\hat{K}E^n} \overset{1-\epsilon}{\approx} \frac{1}{K}\sum_{i=1}^{K} |i\rangle\langle i| \otimes \rho_E^{\otimes n}$$

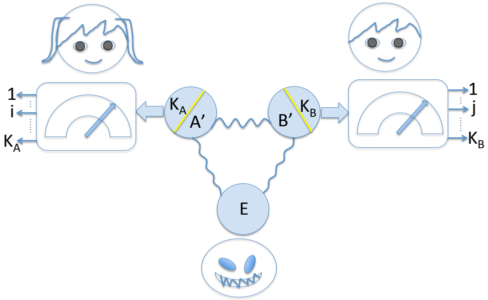
- question: $R_A = \sup \frac{\log K}{n}$, s.t. $n \to \infty,\ \epsilon \to 0$?
- answer: $R_A = \log |A| + [S(A|E)]_-$, where $[t]_- := \min\{0, t\}$, $S(A|E) = S(AE) - S(E)$, $S(X) = -\operatorname{Tr} X \log X$

motivation



- a hidden point in BFW: a trusted but passive Bob
- idea: a trusted and active Bob?

our scenario



$$\psi_{ABE}^{\otimes n} \frac{w/o\ noise}{w/o\ cc} \rightsquigarrow \overset{1-\epsilon}{\approx} \frac{1}{K_A}\sum_{i=1}^{K_A} |i\rangle\langle i| \otimes \frac{1}{K_B}\sum_{i=1}^{K_B} |j\rangle\langle j| \otimes \psi_E^{\otimes n}$$

- a dual setting to distributed data compression (Slepian/Wolf) in classical IT whose natural dual setting does not exist classically, but does quantumly!
- the rate region of (R_A, R_B), where $R_A = \frac{\log K_A}{n}$, $R_B = \frac{\log K_B}{n}$, s.t. $n \to \infty$, $\epsilon \to 0$?

allowed operations: restricted closed local operations and classical communication (RCLOCC)

- ~~adding $|0\rangle$~~
- local unitary
- ~~partial tracing~~
- local noise: $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$
- classical communication: exchanging subsystems by a dephasing channel $\mathcal{N}(\rho) = \sum \langle i|\rho|i\rangle |i\rangle\langle i|$

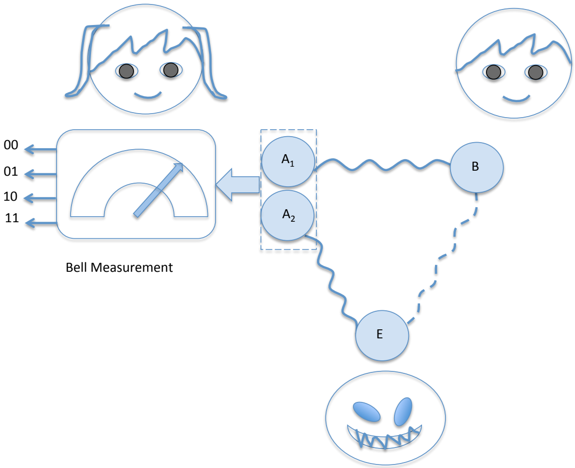
In the standard picture, a state of two independent random bits

$$\rho_{ABE} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)_A \otimes \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)_B \otimes \rho_E$$

in the dual picture, an ibit is

$$\alpha_{AA'BB'} = \frac{1}{4} \sum_{i,j,k,l=0}^{1} |i\rangle\langle j|_A \otimes |k\rangle\langle l|_B \otimes U_{ik} \sigma_{A'B'} U_{jl}^{\dagger}$$

warmup: entanglement swapping



Local noise can help.

Quantum State Merging

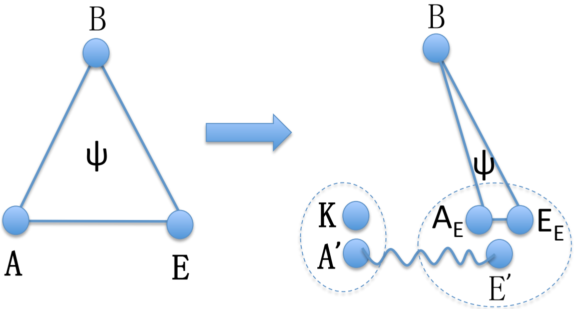


Figure: $S(A|E) < 0$, classical communication $I(A:B)$, entanglement between A' and E' is $-S(A|E)$.

Local noise can be created from QSM.
The communicating part is random against E if not sent.

Doubly decoupling Theorem

Given $\epsilon, \delta > 0$, for n copies of a pure tripartite state $|\psi\rangle_{ABE}$ where n is large, there exists a unitary $U : A^n \to KA'$ with a fixed basis $\{|i\rangle\}$ of subsystem K,

$$(U_{A^n} \otimes \mathbb{1}_{B^n E^n})|\psi\rangle_{ABE}^{\otimes n} = \sum_{i=1}^{|K|} \sqrt{p_i}|i\rangle_K |\psi_i\rangle_{A' B^n E^n},$$

such that after measurement on K in the fixed basis,

$$\left\| \sum_{i=1}^{|K|} p_i |i\rangle\langle i|_K \otimes \psi^i_{B^n} - \frac{1}{|K|} \sum_{i=1}^{|K|} |i\rangle\langle i|_K \otimes \psi_B^{\otimes n} \right\|_1 \leq \epsilon,$$

$$\left\| \sum_{i=1}^{|K|} p_i |i\rangle\langle i|_K \otimes \psi^i_{E^n} - \frac{1}{|K|} \sum_{i=1}^{|K|} |i\rangle\langle i|_K \otimes \psi_E^{\otimes n} \right\|_1 \leq \epsilon,$$

when $\frac{1}{n} \log |K| = \min\{I(A:E)_\psi, I(A:B)_\psi\} - \delta$.

idea

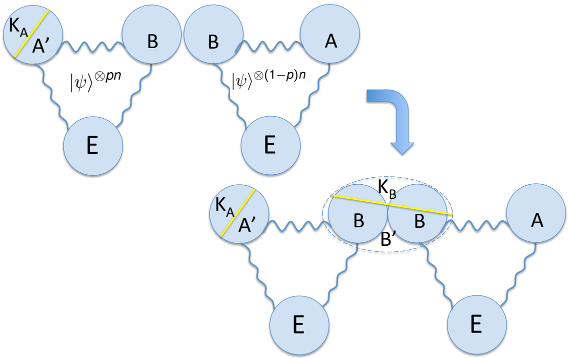


Figure: $S(A|B) > 0 > S(B|A)$. no communication, no noise.

Local noise can be created!

two-sided randomness distillation

no noise and no communication

$$\begin{aligned} R_A &\le \log|A| - S(A|B)_+, \\ R_B &\le \log|B| - S(B|A)_+, \\ R_A + R_B \le R_G &= \log|AB| - S(AB), \end{aligned}$$

where $[t]_+ = \max\{0, t\}$.

free noise but no communication

$$\begin{aligned} R_A &\le \log|A| - S(A|B), \\ R_B &\le \log|B| - S(B|A), \\ R_A + R_B \le R_G &= \log|AB| - S(AB). \end{aligned}$$

free noise and free communication

$$
\begin{aligned}
R_A &\leq R_G, \\
R_B &\leq R_G, \\
R_A + R_B &\leq R_G = \log|AB| - S(AB),
\end{aligned}
$$

free communication but no noise

$$
\begin{aligned}
R_A &\leq \log|AB| - \max\{S(B), S(AB)\}, \\
R_B &\leq \log|AB| - \max\{S(A), S(AB)\}, \\
R_A + R_B &\leq R_G = \log|AB| - S(AB).
\end{aligned}
$$

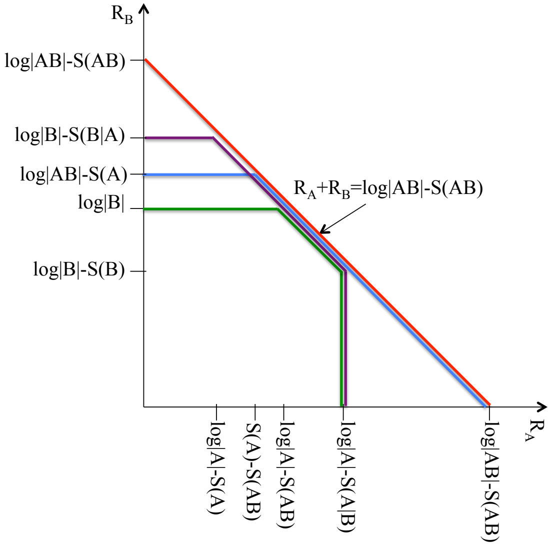
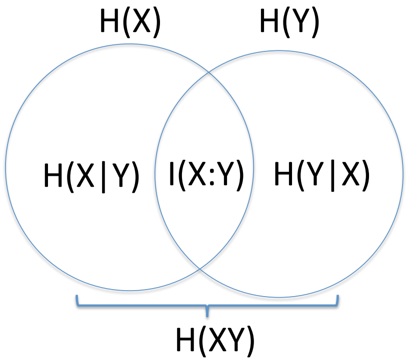


Figure: $S(A|B) > 0 > S(A) - \log|A| > S(B|A)$. no comm. no noise, no comm. free noise, free comm. free noise, free comm. no noise.

distributed data compression



- task: joint prob. distribution p_{XY}. Alice compresses her data at the rate R_X and Bob at R_Y. Charlie can recover the whole data reliably after receiving their compressed data.
- question: what is the compression rate region of (R_X, R_Y)?
- answer: $R_X \geq H(X|Y)$, $R_Y \geq H(Y|X)$, $R_{XY} \geq H(XY)$ **[Slepian-Wolf Theorem]**

Remarks

- no cc, no/free noise is dual to the Slepian-Wolf theorem!
- local noise can boost randomness extraction
- no bound randomness state
- the rate regions are tight in
  - no cc, no noise
  - no cc, free noise
  - free cc, free noise.

tight for free cc, no noise ?

one-sided randomness distillation

- task: Bob helps Alice to extract randomness against Eve.
- the rate $R_A = \log|AB| - \inf \frac{1}{n} \max\{ S(E'^{(n)}), S(B'^{(n)}) \}$ Infimum is taken over n and all $RCLOCC$: $\rho_{AB}^{\otimes n} \longmapsto \sigma_{A'^n B'^n}$
- If $S(B) < S(E)$, then $R_A = \log|AB| - S(AB)$. PPT class. $S(E'^{(n)}) \geq nS(E)$.
- not strongly additive $R_A(\rho \otimes \sigma) > R_A(\rho) + R_A(\sigma)$
- Bell state $R_A(\Phi) = \frac{3}{2}$, $R_A(I/2) = 0$, but $R_A(\Phi \otimes I/2) = 2$.
- upper bound

$$
\begin{aligned}
R_A &\leq \log|AB| - \max\left\{ \frac{1}{2}[E_r^{\infty}(\rho_{AB}) + S(AB)], S(AB) \right\} \\
&\leq \log|AB| - \frac{1}{2}\max\{S(A), S(B)\}
\end{aligned}
$$

private randomness capacity

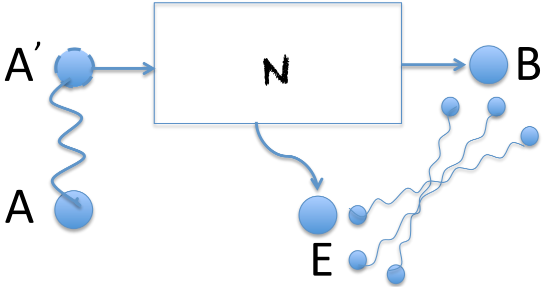


Figure: server-client model: $|\phi\rangle_{AA'} \xmapsto{\mathcal{N}:A' \to B} \rho_{AB}$

- task: Bob extract randomness secure against Eve.
- question: what is the maximal rate?
- in line with the standard model of transmitting information
- server-client structure in future quantum networks

private randomness capacity

Answer

- $\log d_B + \max_{|\phi\rangle_{AA'}} \{S(A) - S(\mathcal{N}_{A' \to B}(\phi_{AA'}))\}$ **!**
- reverse coherent information of a channel
  $I_{rev}(\mathcal{N}) = \max_{|\phi\rangle_{AA'}} \{S(A) - S(\mathcal{N}_{A' \to B}(\phi_{AA'}))\}$

Remark

- single-letter formula, computable.
- $I_{rev}(\mathcal{N} \otimes \mathcal{M}) = I_{rev}(\mathcal{N}) + I_{rev}(\mathcal{M})$
  [CMP266, 37 (2006)], [PRL102, 210501 (2009)]
- But its interpretation has been missing since then.

In contrast with coherent information

- $I_{coh}(\mathcal{N}) = \max_{|\phi\rangle_{AA'}} \{S(B) - S(\mathcal{N}_{A' \to B}(\phi_{AA'}))\}$
- $I_{coh}(\mathcal{M} \otimes \mathcal{N}) \neq I_{coh}(\mathcal{M}) + I_{coh}(\mathcal{N})$
- $Q(\mathcal{N}) = \sup \frac{1}{n} I_{coh}(\mathcal{N}^{\otimes n})$

Summary

Our scenario

distributed private randomness distillation

Results

- two-sided private randomness distillation
- one-sided private randomness distillation
- the private randomness capacity of a channel

Questions

- Q1. what is the tight region for free cc, no noise?
- Q2. is regularization necessary in the one-sided setting ?
- Q3. multipartite case, single-shot case?

Thank you !