Tight Exponential Analysis for Smoothing the Max-Relative Entropy and for Quantum Privacy Amplification

[1] **Ke Li**, [1, 2] **Yongsheng Yao**, and [2, 3] **Masahito Hayashi**

[arxiv : 2111.01075]

[1] Harbin Institute of Technology
[2] Southern University of Science and Technology
[3] Nagoya University

Beyond IID in Information Theory 10

Outline

- Sandwiched Rényi relative entropy
- Exponential analysis for smoothing the max-relative entropy
- Exponential analysis for quantum privacy amplification
- Summary and open questions

Sandwiched Rényi relative entropy

Sandwiched Rényi Relative Entropy

$$D_\alpha(\rho||\sigma) = \frac{1}{\alpha - 1} \log \mathrm{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha$$

$\Downarrow$

Sandwiched Rényi Conditional Entropy

$$H_\alpha(A|B)_\rho := -D_\alpha(\rho_{AB}||I_A \otimes \rho_B)$$

Muller-Lennert et al, JMP, 2013;
Wilde, Winter, Yang, CMP, 2014.

- quantum relative entropy

$$D(\rho||\sigma) := \mathrm{Tr}(\rho \log \rho - \rho \log \sigma)$$

- max-relative entropy

$$D_{max}(\rho||\sigma) := \inf\{t : \rho \leq 2^t \sigma\}$$

- purified distance

$$P(\rho, \sigma) := \sqrt{1 - F^2(\rho, \sigma)}$$

Sandwiched Rényi relative entropy

Operational interpretations of the sandwiched Rényi relative entropy:

Prior works: strong converse exponents

- Mosonyi, Ogawa, CMP 2015 (quantum hypothesis testing)
- Mosonyi, Ogawa, CMP 2017 (classical-quantum channels)
- Cheng, Hanson, Datta, Hsieh, IEEE Trans. Inf. Theory 2020 (data compression)

Exponential analysis for smoothing the max-relative entropy

Smoothed max-relative entropy:

Renner, Ph. D thesis, 2005.
Datta, IEEE Trans. Inf. Theory, 2009.

$$D^{\epsilon}_{\max}(\rho\|\sigma) := \inf_{\tilde{\rho}\in S_{\leq}(\mathcal{H}):P(\rho,\tilde{\rho})\leq\epsilon} D_{\max}(\tilde{\rho}\|\sigma).$$

Its inverse function (smoothing quantity):

$$\epsilon(\rho\|\sigma, r) := \inf\{\epsilon : D^{\epsilon}_{\max}(\rho\|\sigma) \leq r\} = \inf\{P(\rho, \tilde{\rho}) : \tilde{\rho} \leq 2^{r}\sigma \text{ and } \tilde{\rho} \in \mathrm{S}_{\leq}(\mathcal{H})\}$$

Significance of the smoothed max-relative entropy :

- A basic tool in one-shot information theory (information spectrum relative entropy, hypothesis testing relative entropy, smoothed max-relative entropy).
- Operational meaning: the ϵ-approximate distinguishability cost [Wang, Wilde, Physics Review Reasearch, 2019].

Exponential analysis for smoothing the max-relative entropy

Smoothed max-relative entropy:

Renner, Ph. D thesis, 2005.
Datta, IEEE Trans. Inf. Theory, 2009.

$$D^{\epsilon}_{\max}(\rho\|\sigma) := \inf_{\tilde{\rho}\in S_{\leq}(\mathcal{H}):P(\rho,\tilde{\rho})\leq\epsilon} D_{\max}(\tilde{\rho}\|\sigma).$$

Its inverse function (smoothing quantity):

$$\epsilon(\rho\|\sigma, r) := \inf\{\epsilon : D^{\epsilon}_{\max}(\rho\|\sigma) \leq r\} = \inf\{P(\rho,\tilde{\rho}) : \tilde{\rho} \leq 2^{r}\sigma \text{ and } \tilde{\rho} \in \mathrm{S}_{\leq}(\mathcal{H})\}$$

Asymptotic Equipartition Property (AEP):

when $r > D(\rho\|\sigma)$,

$\epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr) \to 0$ exponentially

Tomamichel, Colbeck, Renner,
IEEE Trans. Inf. Theory, 2009.

Exponential analysis for smoothing the max-relative entropy

The derivation for the upper bound of $\epsilon(\rho\|\sigma, r)$:

Construct a subnormalized state $\tilde{\rho} := Q\rho Q, \quad \text{where } Q := \{\mathcal{E}_\sigma(\rho) \leq \frac{1}{v(\sigma)} 2^r \sigma\}$

$v(\sigma)$ denotes the number of different eigenvalues of σ

$\mathcal{E}_\sigma(\rho) = \sum_{i=1}^{v(\sigma)} \Pi_i \rho \Pi_i$, where Π_i is the projection onto the eignsubspace

(by pinching inequality)

$$\rho \leq v(\sigma)\mathcal{E}_\sigma(\rho)$$

$$\tilde{\rho} \leq v(\sigma) Q \mathcal{E}_\sigma(\rho) Q \leq 2^r \sigma$$

$$\epsilon(\rho\|\sigma, r) \leq P(\rho, \tilde{\rho}) \leq \sqrt{2 \operatorname{Tr} \rho(\mathbb{1} - Q)}$$

Exponential analysis for smoothing the max-relative entropy

Let $p = \operatorname{Tr}\rho(\mathbb{1} - Q)$ and $q = \operatorname{Tr}\sigma(\mathbb{1} - Q)$, then for any $s \geq 0$, we have

$$\epsilon(\rho\|\sigma,\lambda) \leq \sqrt{2p^{1+s}p^{-s}} \leq \sqrt{2\left(p^{1+s}\left(\frac{1}{v(\sigma)}2^{\lambda}q\right)^{-s}\right)}$$

$$\leq \sqrt{2\left(p^{1+s}\left(\frac{1}{v(\sigma)}2^{\lambda}q\right)^{-s} + (1-p)^{1+s}\left(\frac{1}{v(\sigma)}2^{\lambda}(\operatorname{Tr}\sigma - q)\right)^{-s}\right)}$$

$$= \sqrt{2v(\sigma)^{s}\, 2^{s\left(D_{1+s}((p,1-p)\|(q,\operatorname{Tr}\sigma-q))-\lambda\right)}}$$

$$\leq \sqrt{2v(\sigma)^{s}\, 2^{s\left(D_{1+s}(\rho\|\sigma)-\lambda\right)}}$$

(by data processing inequality)

Exponential analysis for smoothing the max-relative entropy

The derivation for the lower bound of $\epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr)$:

Let ρ_n be any subnormalized state with $\rho_n \leq 2^{nr}\sigma^{\otimes n}$, $Q_n := \{\rho^{\otimes n} > 9.2^{nr}\sigma^{\otimes n}\}$ and $p_n = \operatorname{Tr}\rho^{\otimes n}Q_n$, $q_n = \operatorname{Tr}\rho_n Q_n$

$$\begin{aligned} Q_n\rho^{\otimes n}Q_n &\geq 9\cdot 2^{nr}Q_n\sigma^{\otimes n}Q_n \\ &\geq 9Q_n\rho_n Q_n, \end{aligned}$$

$$p_n \geq 9q_n$$

by the monotonicity of the fidelity under measurements

$$\begin{aligned} F(\rho^{\otimes n}, \rho_n) &\leq F\big((p_n, 1-p_n), (q_n, \operatorname{Tr}\rho_n - q_n)\big) \\ &\leq \sqrt{p_n}\sqrt{q_n} + \sqrt{1-p_n} \\ &\leq \frac{p_n}{3} + \sqrt{1-p_n}, \end{aligned}$$

Exponential analysis for smoothing the max-relative entropy

$$\begin{aligned} F(\rho^{\otimes n}, \rho_n) &\le F\big((p_n, 1-p_n), (q_n, \operatorname{Tr}\rho_n - q_n)\big) \\ &\le \sqrt{p_n}\sqrt{q_n} + \sqrt{1-p_n} \\ &\le \frac{p_n}{3} + \sqrt{1-p_n}, \end{aligned}$$

$$\begin{aligned} P(\rho^{\otimes n}, \rho_n) &= \sqrt{1 - F^2(\rho^{\otimes n}, \rho_n)} \\ &\ge \sqrt{1 - \left(\frac{p_n}{3} + \sqrt{1-p_n}\right)^2} \\ &= \sqrt{-\frac{p_n^2}{9} + p_n - \frac{2p_n}{3}\sqrt{1-p_n}} \\ &\ge \sqrt{p_n}\sqrt{-\frac{p_n}{9} + 1 - \frac{2}{3}} \\ &= \sqrt{p_n}\sqrt{\frac{1}{3} - \frac{p_n}{9}}. \end{aligned}$$

$$\epsilon(\rho^{\otimes n} \| \sigma^{\otimes n}, nr) \ge \sqrt{p_n}\sqrt{\frac{1}{3} - \frac{p_n}{9}}.$$

Exponential analysis for smoothing the max-relative entropy

For any $s \geq 0$, we have

$$\sqrt{p_n}\sqrt{\frac{1}{3}-\frac{p_n}{9}} \leq \epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr) \leq \sqrt{2v(\sigma^{\otimes n})^s 2^{ns(D_{1+s}(\rho\|\sigma)-r)}}$$

$$\frac{-1}{n}\log p_n \to \sup_{s\geq 0}\{s(r - D_{1+s}(\rho\|\sigma))\}$$

Mosonyi, Ogawa, CMP 2015.

Main result 1:

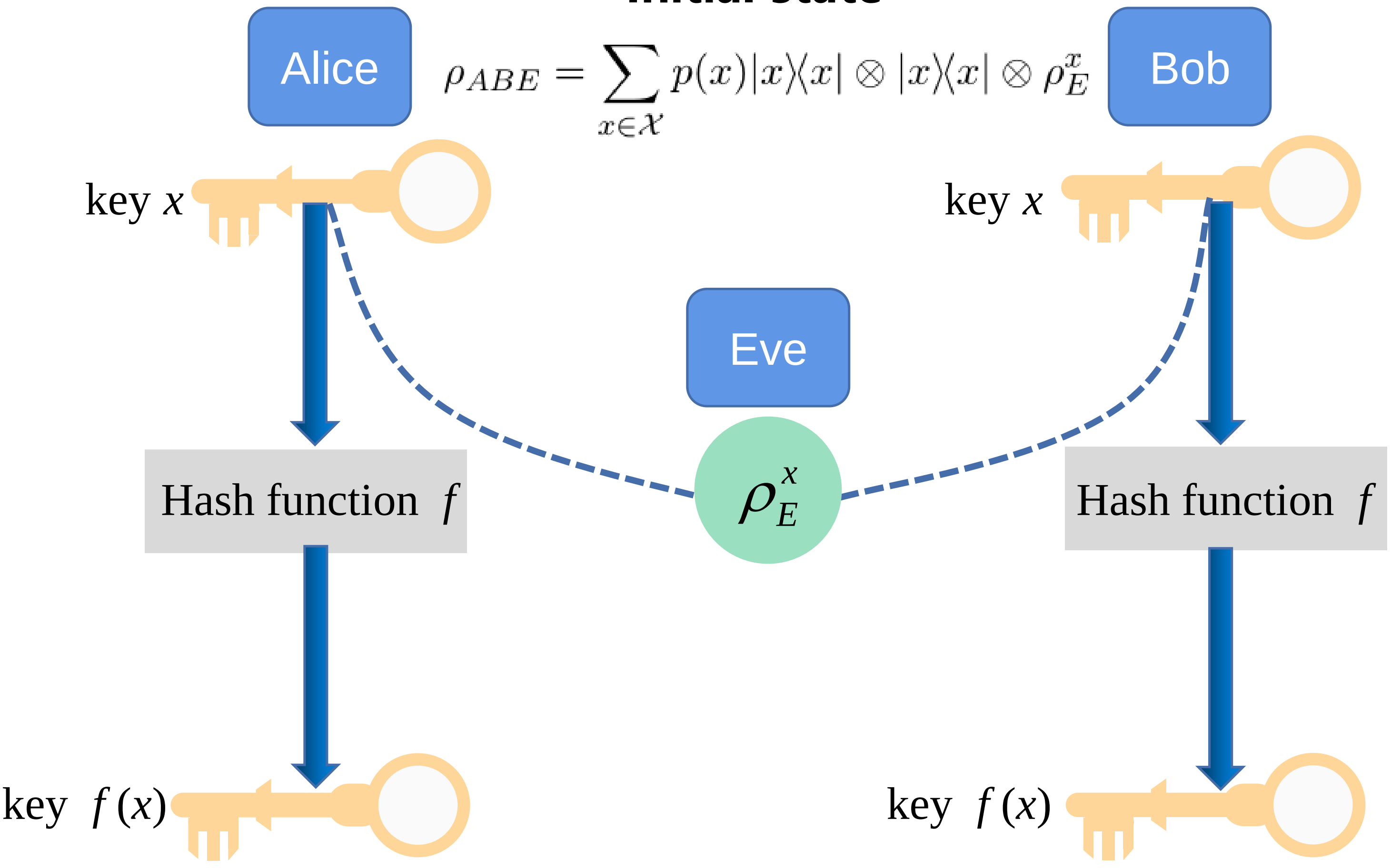
Theorem 1 *For quantum states ρ, σ and $r \in \mathbb{R}$, we have*

$$\lim_{n\to\infty}\frac{-1}{n}\log\epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr) = \frac{1}{2}\sup_{s\geq 0}\left\{s\big(r - D_{1+s}(\rho\|\sigma)\big)\right\}.$$

Exponential analysis for quantum privacy amplification

Initial state

$$\rho_{ABE} = \sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x| \otimes |x\rangle\langle x| \otimes \rho_E^x$$



Final state

$$\rho_{ZZ'E}^f = \sum_{z\in\mathcal{Z}} |z\rangle\langle z| \otimes |z\rangle\langle z| \otimes \Big(\sum_{x\in f^{-1}(z)} p(x)\rho_E^x\Big)$$

Devetak, Winter, P. Roy. Soc. A, 2005

The performance

$$\boxed{d\left(\rho_{ZE}^f, \frac{\mathbb{1}_Z}{|\mathcal{Z}|} \otimes \rho_E\right)}$$

d is a distance measure

d
- trace norm distance
- purified distance
- Umegaki relative entropy
- ⋮

Exponential analysis for quantum privacy amplification

Security exponent of quantum privacy amplification:

Devetak, Winter 2004;
Renner 2005

$\rho^{f_n}_{Z_n E^n}$: the state resulting from applying f_n to $\rho^{\otimes n}_{XE}$

Definition 2 *For a classical-quantum state ρ_{XE} and a key rate $0 < R < H(X|E)_\rho$, the* security exponent *$E(R)$ under distance d is defined as*

$$E(R) := -\lim_{n\to\infty} \frac{1}{n} \log \min_{f_n} d(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}),$$

where f_n runs over all hash function from $\mathcal{X}^{\times n} :\to \mathcal{Z}_n = \{1, \ldots, 2^{nR}\}$.

Exponential analysis for quantum privacy amplification

upper bound of the security exponent:

For any hash function $f : \mathcal{X} \to \mathcal{Z}$, we have

$$H^{\epsilon}_{\min}(X|E)_{\rho} \geq H^{\epsilon}_{\min}(Z|E)_{\rho^f},$$

where $H^{\epsilon}_{\min}(X|E)_{\rho} = -D^{\epsilon}_{\max}(\rho_{XE}\|\mathbb{1}_X \otimes \rho_E)$.

For any hash function $f : \mathcal{X} \to \mathcal{Z}$ and $\lambda \in \mathbb{R}$, we have

$$\epsilon(\rho^f_{ZE}\|\mathbb{1}_Z \otimes \rho_E, \lambda) \geq \epsilon(\rho_{XE}\|\mathbb{1}_X \otimes \rho_E, \lambda).$$

Exponential analysis for quantum privacy amplification

$$P\left(\rho^f_{ZE}, \frac{\mathbb{1}_Z}{|\mathcal{Z}|} \otimes \rho_E\right) \geq \epsilon(\rho^f_{ZE} \| \mathbb{1}_Z \otimes \rho_E, -\log|\mathcal{Z}|) \geq \epsilon(\rho_{XE} \| \mathbb{1}_X \otimes \rho_E, -\log|\mathcal{Z}|)$$

$$\min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \geq \epsilon(\rho_{XE}^{\otimes n} \| \mathbb{1}_X^{\otimes n} \otimes \rho_E^{\otimes n}, -nR)$$

Main result 2

Theorem 2 *Let ρ_{XE} be a classical-quantum state, $0 < R < H(X|E)_\rho$. We have*

$$\lim_{n \to +\infty} \frac{-1}{n} \log \min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \leq \frac{1}{2} \max_{t \geq 0} t\big(H_{1+t}(X|E)_\rho - R\big).$$

Exponential analysis for quantum privacy amplification

Our upper bound:

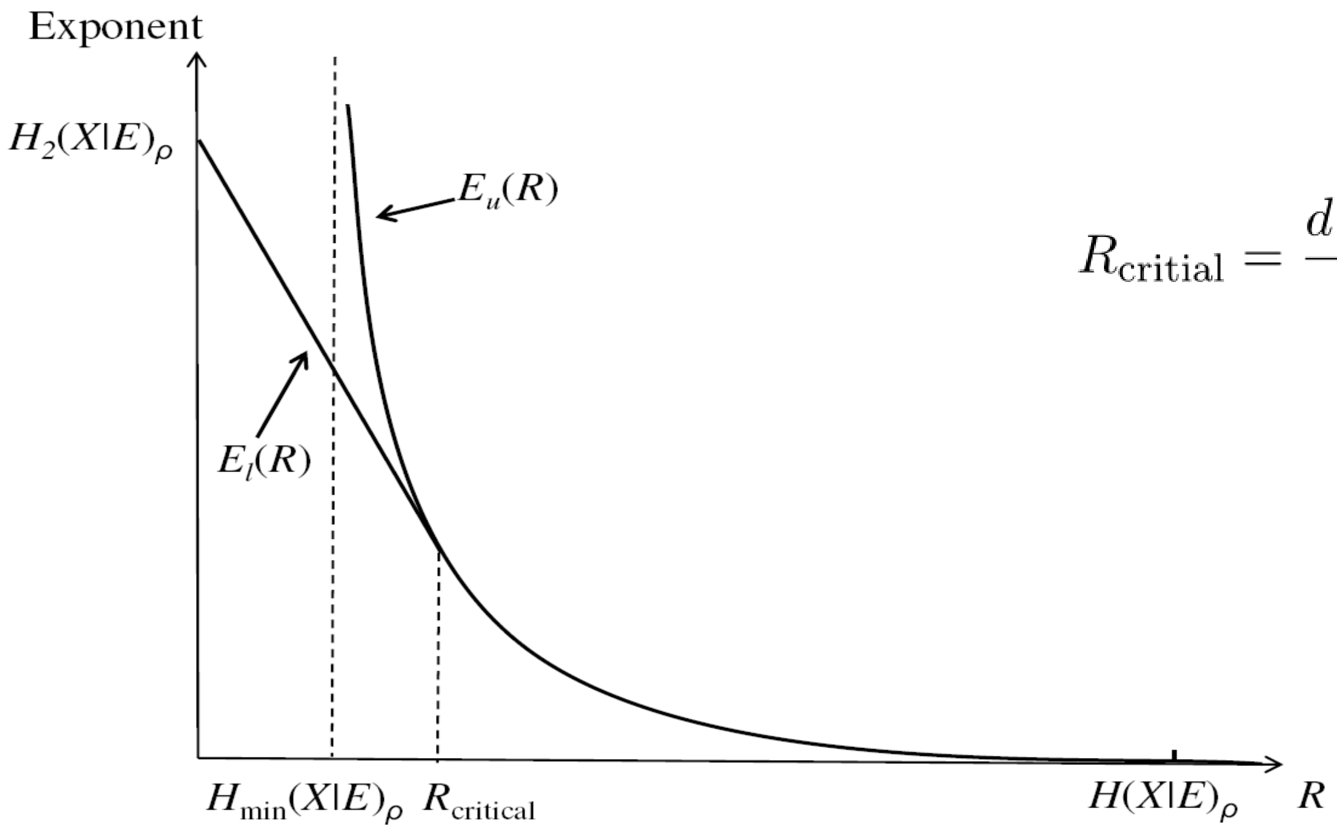
Theorem 2 *Let ρ_{XE} be a classical-quantum state, $0 < R < H(X|E)_\rho$. We have*

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} P\Big(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\Big) \leq \frac{1}{2} \max_{t\geq 0} t\big(H_{1+t}(X|E)_\rho - R\big).$$

Hayashi's lower bound [Hayashi, CMP 2015] $\left(P(\rho,\sigma) \leq \sqrt{(\ln 2) D(\rho||\sigma)} \right)$

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} P\Big(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\Big) \geq \frac{1}{2} \max_{0\leq t\leq 1} t\big(H_{1+t}(X|E)_\rho - R\big).$$

Exponential analysis for quantum privacy amplification



$$R_{\text{critial}} = \frac{d(sH_{1+s}(X|E)_\rho)}{ds}\Big|_{s=1}$$

$$E_u(R) := \frac{1}{2} \max_{t\geq 0} \{t(H_{1+t}(X|E)_\rho - R)\}$$ (Our upper bound)

$$E_l(R) := \frac{1}{2} \max_{0\leq t\leq 1} \{t(H_{1+t}(X|E)_\rho - R)\}$$ (Hayashi's lower bound [Hayashi, CMP 2015])

Exponential analysis for quantum privacy amplification

Main result 3:

security exponent under (sandwiched Rényi) relative entropies :

Theorem *3 Let ρ_{XE} be a classical-quantum state, $0 < R < H_{1+s}(X|E)_\rho$ and $0 \leq s \leq 1$. We have*

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} D_{1+s}\Big(\rho^{f_n}_{Z_n E^n} \Big\| \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\Big) \leq \max_{s\leq t} t\big(H_{1+t}(X|E)_\rho - R\big),$$

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} D_{1+s}\Big(\rho^{f_n}_{Z_n E^n} \Big\| \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\Big) \geq \max_{s\leq t\leq 1} t\big(H_{1+t}(X|E)_\rho - R\big).$$

Summary and open questions

- We derive the best exponents for smoothing the max-relative entropy and for quantum privacy amplification.
- We provide a new type of operational interpretation for the sandwiched Rényi divergence, in characterizing how fast the performance of certain quantum task approaches the perfect (see also Yongsheng's talk tomorrow on [K. L., Y. Yao, arxiv: 2111.06343, 2112.04475]).
- The obtained exponent for smoothing the max-relative entropy has applications in quantum information decoupling and quantum channel simulation [see Yongsheng's talk tommorrow].

- Question 1: security exponent for privacy amplification below the critical rate?
- Question 2: best exponents for more quantum information tasks? (might discover new quantum Rényi relative entropies.)

Thank you !