Rethinking quantum smooth entropies

Tight one-shot analysis of quantum privacy amplification

Bartosz Regula and Marco Tomamichel

RIKEN CQT

Beyond IID, Shenzhen, June 2026

arXiv:**2603.04493**

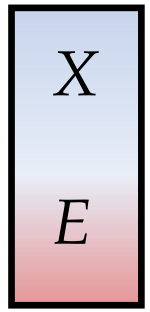
Randomness extraction

weakly random source

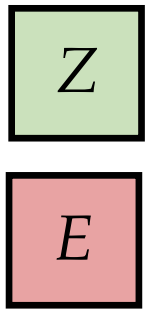
uniform randomness

privacy amplification

ρ_{XE}



universal protocol



$$\log |Z| = \ell_\varepsilon(\rho_{XE})$$

extractable randomness

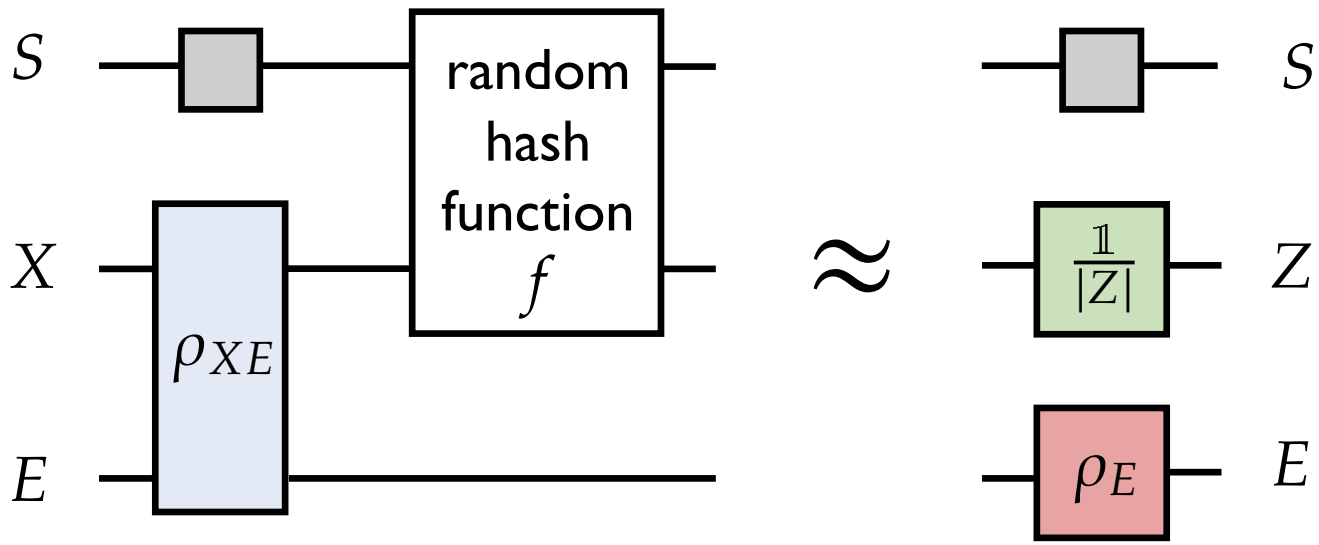
(quantum) eavesdropper

underlies security of QKD, finds use in a wide number of fundamental achievability results

arXiv:2603.04493

Randomness extraction

quantum privacy amplification



(Renner, 2005)
(Renner and König, 2005)

$$\ell_\varepsilon(\rho_{XE}) = \max\left\{ \log|Z| \;\middle|\; \mathop{\mathbb{E}}_f \frac{1}{2}\left\|\rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|}\otimes\rho_E\right\|_1 \leq \varepsilon \right\}$$

extractable randomness

error (distance to uniform)

arXiv:2603.04493

How much randomness can we extract?

folklore: $\ell_\varepsilon(\rho_{XE}) \overset{?}{\approx} H_{\min}^{\varepsilon}(X|E)_\rho$ — smooth min-entropy

asymptotics: $H(X|E)_\rho$ $\quad \ell_\varepsilon\left(\rho_{XE}^{\otimes n}\right) \to n\, H(X|E)_\rho$ — conditional entropy

one-shot: $H_{\min}(X|E)_\rho = -\log p_{\text{guess}}(X|E)$ — min-entropy

classical $\quad H_2^{\varepsilon-\mu}(X|E)_p - \log \dfrac{1}{4\mu^2} \leq \ell_\varepsilon(p_{XE}) \leq H_{\min}^{\varepsilon}(X|E)_p$ (Renner and Wolf, 2004)

VI

$H_{\min}^{\varepsilon-\mu}(X|E)_p - \log \dfrac{1}{4\mu^2}$ (Hayashi, 2010; 2013)

arXiv:2603.04493

How much randomness can we extract?

folklore: $\ell_\varepsilon(\rho_{XE}) \overset{?}{\approx} H_{\min}^{\varepsilon}(X|E)_\rho$ smooth min-entropy

quantum $H_{\min}^{(\varepsilon-\mu)/2}(X|E)_\rho - \log \frac{1}{4\mu^2} \leq \ell_\varepsilon(\rho_{XE}) \leq H_{\min}^{2\sqrt{\varepsilon}}(X|E)_\rho$ (Tomamichel et al., 2011) (Anshu et al., 2020)

not tight — not good enough for asymptotics, suboptimal bounds in many contexts, does not get correct scaling (Hayashi, 2014) (Dupuis, 2023)

change distance? trace distance needed for cryptography

(Hayashi, 2014)

use pinching? captures second-order behaviour, but one-shot bounds not tight

(Hayashi, 2017; Shen, Gao, and Cheng, 2024)

use Rényi divergences? good bounds on exponents, but other properties not recovered

(Dupuis, 2023)

arXiv:2603.04493

PUBLIC SERVICE ANNOUNCEMENT

We have been smoothing entropies **wrong**

How much randomness can we extract?

classical

$$\ell_\varepsilon(p_{XE}) \geq H_{\min}^{\varepsilon-\mu}(X|E)_p - \log \frac{1}{4\mu^2}$$

quantum

This work:

$$\ell_\varepsilon(\rho_{XE}) \geq H_{\min}^{\varepsilon-\mu,\mathbb{M}}(X|E)_\rho - \log \frac{1}{4\mu^2}$$

improves on all previous results

captures optimal asymptotic scaling, recovers best known bounds

redefines quantum smooth entropies

arXiv:2603.04493

Quantum relative entropies

classical Rényi

$$D_\alpha(p\|q) := \frac{1}{\alpha-1}\log\sum_x p(x)^\alpha\, q(x)^{1-\alpha}$$

(Rényi, 1961)

sandwiched Rényi

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log \mathrm{Tr}\left[\left(\sigma^{\frac{1-\alpha}{2\alpha}}\,\rho\,\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right]$$

(Müller-Lennert et al., 2013)
(Wilde et al., 2014)

$$\alpha=\infty:\quad D_{\max}(\rho\|\sigma) = \inf\left\{\lambda \;\middle|\; \rho\le 2^\lambda\sigma\right\}$$

max-relative entropy

measured Rényi
(minimal)

$$D_\alpha^{\mathbb{M}}(\rho\|\sigma) := \sup_{\mathcal{M}\in\mathbb{M}} D_\alpha(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$

lifting by measurements

(Fuchs, 1996)
(Matsumoto, 2014)

$$\|\rho-\rho'\|_1 = \sup_{\mathcal{M}\in\mathbb{M}} \|\mathcal{M}(\rho)-\mathcal{M}(\rho')\|_1$$

$$F(\rho,\rho') = \inf_{\mathcal{M}\in\mathbb{M}} F(\mathcal{M}(\rho),\mathcal{M}(\rho'))$$

arXiv:2603.04493

On smoothing

generalised trace distance $\|\rho - \rho'\|_+ = \frac{1}{2}\|\rho - \rho'\|_1 + \frac{1}{2}\left|\mathrm{Tr}(\rho - \rho')\right|$ (Tomamichel, 2016)

smooth max-relative entropy

$D_{\max}(\rho\|\sigma) = \inf\left\{\lambda \,\middle|\, \rho \le 2^{\lambda}\sigma\right\}$

$$D^{\varepsilon,T}_{\max}(\rho\|\sigma) = \min\left\{ D_{\max}(\rho'\|\sigma) \,\middle|\, \rho' \ge 0,\ \mathrm{Tr}\,\rho' \le 1,\ \|\rho - \rho'\|_+ \le \varepsilon\right\}$$ (Datta, 2009)

$$H^{\varepsilon,T}_{\min}(X|E)_\rho = -\min_{\sigma_E} D^{\varepsilon,T}_{\max}(\rho_{XE}\|\mathbb{1}_X \otimes \sigma_E)$$

classically: tightly characterises privacy amplification ✓
allows for precise asymptotic understanding ✓

(Renner and Wolf, 2004)
(Hayashi, 2014)

quantumly: smoothing not as nicely behaved ✗
lack of tight asymptotic results ✗
known bounds looser than classical ones ✗

(Hayashi, 2014)
(Hayashi, 2016)
(Dupuis, 2023)
(Shen et al., 2024)

How classical smoothing works

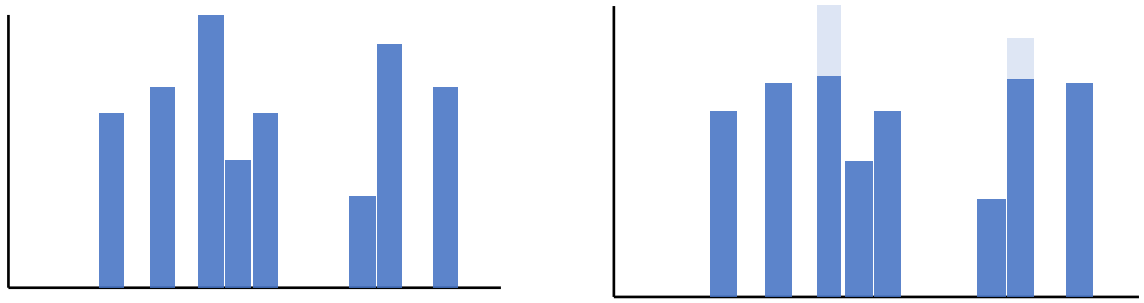
$$H_{\min}^{\varepsilon,T}(X|E)_p = -\min_{q_E} D_{\max}^{\varepsilon,T}(p_{XE}\|\mathbb{1}_X \otimes q_E)$$

$$D_{\max}^{\varepsilon,T}(p\|q) = \min\left\{ D_{\max}(p'\|q) \,\middle|\, p' \geq 0,\ \operatorname{Tr} p' \leq 1,\ \|p - p'\|_+ \leq \varepsilon \right\}$$

$$H_\infty^\varepsilon(X|Y) := \max_{\Omega} \min_{y} \min_{x} \left(-\log P_{X\Omega|Y=y}(x)\right) , \qquad (2)$$

where the first minimum/maximum ranges over all events Ω with probability $\Pr[\Omega] \geq 1 - \varepsilon$.

(Renner and Wolf, 2004)



discarding mass

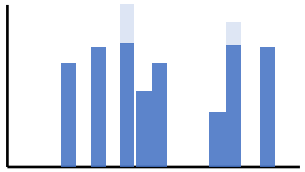
$$= \min\left\{ D_{\max}(p'\|q) \,\middle|\, 0 \leq p' \leq p,\ \|p - p'\|_+ \leq \varepsilon \right\}$$

optimal smoothing: $p' = \min\{p, \lambda q\}$

arXiv:2603.04493

How to define quantum smoothing?

Idea 1: discarding mass



$$D_{\max}^{\varepsilon,T}(p\|q) = \min\left\{ D_{\max}(p'\|q) \,\middle|\, 0 \le p' \le p,\ \|p - p'\|_+ \le \varepsilon \right\}$$

$\rho' \le \rho$???

$p' = \min\{p, \lambda q\}$ $\min\{\rho, \lambda\sigma\}$???

a minimum of two positive operators may be non-positive

(Moreland and Gudder,, 1999)
(Cheng, 2023)

Hermitian-smoothed max-relative entropy?

$$D_{\max}^{\varepsilon,\mathrm{Herm}}(p\|q) = \min\left\{ D_{\max}(R\|\sigma) \,\middle|\, R = R^\dagger,\ R \le \rho,\ \|\rho - R\|_+ \le \varepsilon \right\}$$???

How to define quantum smoothing?

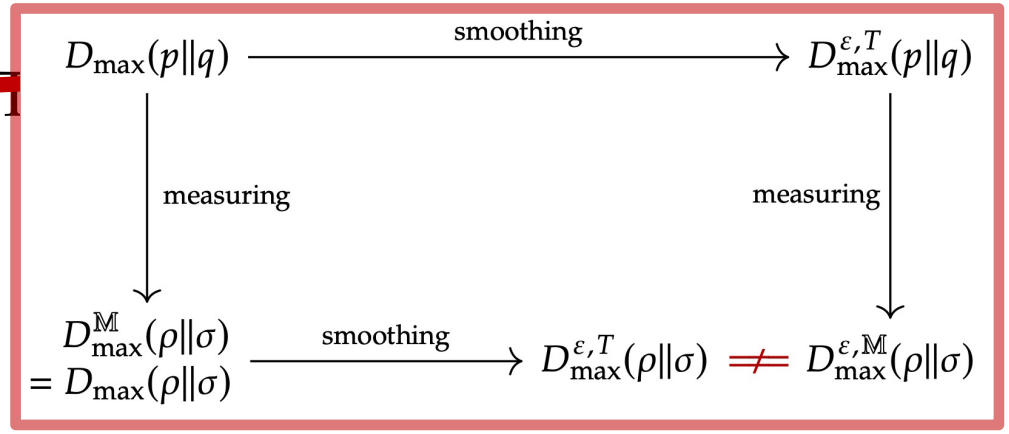
Idea 2: lift by measurements

$$\frac{1}{2}\|\rho-\rho'\|_1 = \sup_{\mathcal{M}\in\mathbb{M}} \frac{1}{2}\|\mathcal{M}(\rho)-\mathcal{M}(\rho')\|_1$$

$$D_{\max}(\rho\|\sigma) = D^{\mathbb{M}}_{\max}(\rho\|\sigma) = \sup_{\mathcal{M}\in\mathbb{M}} D_{\max}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$

~~$D^{\varepsilon,T}_{\max}(\rho\|\sigma) = \min\{ D_{\max}(\rho'\|\sigma) \,|\, \rho' \geq 0, \ldots$~~

$$D^{\varepsilon,\mathbb{M}}_{\max}(\rho\|\sigma) := \sup_{\mathcal{M}\in\mathbb{M}} D^{\varepsilon,T}_{\max}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$



$$D^{\varepsilon,\mathbb{M}}_{\max}(\rho\|\sigma) \overset{!}{=} D^{\varepsilon,\mathrm{Herm}}_{\max}(\rho\|\sigma) = \min\left\{ \gamma \,\middle|\, \mathrm{Tr}(\rho - 2^{\gamma}\sigma)_+ \leq \varepsilon \right\}$$

(Regula, Lami, and Datta 2026)

classical trace distance smoothing

discarding mass →

measurements →

$D^{\varepsilon,\mathbb{M}}_{\max}(\rho\|\sigma)$

$\neq$ conventional quantum trace distance

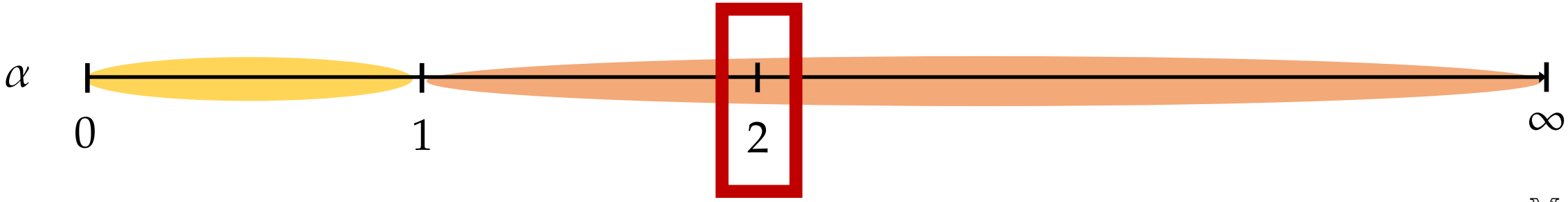
arXiv:2603.04493

How to define quantum smoothing?

Idea 2: lift by measurements

measured smooth Rényi divergence

$$D_\alpha^{\varepsilon,\mathbb{M}}(\rho\|\sigma) := \sup_{\mathcal{M}\in\mathbb{M}} D_\alpha^{\varepsilon,T}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$



hypothesis testing relative entropy

$$D_H^\varepsilon(\rho\|\sigma) = -\log\inf\left\{\operatorname{Tr} M\sigma \;\middle|\; 0 \le M \le \mathbb{1},\ \operatorname{Tr}(\mathbb{1}-M)\rho \le \varepsilon\right\}$$

(Wang and Renner, 2011)
(Buscemi and Datta, 2011)

arXiv:2603.04493

Measured smooth collision divergence

$$D_2^{\varepsilon,T}(p\|q) = \inf\left\{ \log \sum_x p'(x)^2\, q(x)^{-1} \;\middle|\; p' \geq 0,\ \operatorname{Tr} p' \leq 1,\ \|p - p'\|_+ \leq \varepsilon \right\}$$

measured smooth collision divergence

$$D_2^{\varepsilon,\mathbb{M}}(\rho\|\sigma) := \sup_{\mathcal{M}\in\mathbb{M}} D_2^{\varepsilon,T}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$

$$D_2^{\mathbb{M}}(\rho\|\sigma) = \log \operatorname{Tr} \rho\, \mathcal{J}_\sigma^{-1}(\rho)$$
$$= \log \|\rho\|_\sigma^2$$

matrix division operator

$$\mathcal{J}_\sigma(X) = \frac{1}{2}(\sigma X + X\sigma)$$

(Petz, 1996)
(Lesniewski and Ruskai, 1999)
(Temme and Verstraete, 2015)

Bures inner product
(Bures norm)

SLD metric
(maximal monotone metric)

$$\widetilde{D}_2(\rho\|\sigma) = \log \operatorname{Tr} \rho\, \sigma^{-1/2}\rho\sigma^{-1/2}$$

arXiv:2603.04493

Measured smooth collision divergence

measured smooth collision divergence

$$D_2^{\varepsilon,\mathbb{M}}(\rho\|\sigma) := \sup_{\mathcal{M}\in\mathbb{M}} D_2^{\varepsilon,T}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$$

Key technical result: variational form + unified smoothing notions

$$D_2^{\varepsilon,\mathbb{M}}(\rho\|\sigma) = \log\inf\left\{ \|R\|_\sigma^2 \,\middle|\, R = R^\dagger,\ \|\rho - R\|_+ \le \varepsilon,\ R \le \rho \right\} = D_2^{\mathbb{M},\,\varepsilon,\,\mathrm{Herm}}(\rho\|\sigma)$$

$$= \log \sup_{0\le W\le \mathbb{1}} \frac{(\mathrm{Tr}(W\rho) - \varepsilon)_+^2}{\mathrm{Tr}\, W^2\sigma}$$

proof ingredients:

Bures norm + convex duality + one-shot classical smoothing + results in matrix analysis

arXiv:2603.04493

Improving randomness extraction

key achievability result: leftover hash lemma

classical

$$\mathbb{E}_f \frac{1}{2} \left\| p^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes p_E \right\|_1 \leq \frac{1}{2} \sqrt{|Z| \exp\left(-H_2(X|E)_p\right)}$$

(Impagliazzo et al., 1989)
(Bennett et al., 1995)

quantum

$$\mathbb{E}_f \frac{1}{2} \left\| \rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes \rho_E \right\|_1 \leq \frac{1}{2} \sqrt{|Z| \exp\left(-H_2(X|E)_\rho\right)}$$

(Renner, 2005)
(Tomamichel et al., 2011)

measured collision entropy

$$\mathbb{E}_f \frac{1}{2} \left\| \rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes \rho_E \right\|_1 \leq \frac{1}{2} \sqrt{|Z| \exp\left(-H_2^{\mathbb{M}}(X|E)_\rho\right)}$$

previous works: $\|\cdot\|_1$ is a Schatten norm => use Hölder's inequality => sandwiched

key idea: lift by measurements (minimal)

$\|\cdot\|_1$ is a measured norm => just lift classical

arXiv:2603.04493

Smoothed leftover hashing

leftover hash

$$\mathbb{E}_f \frac{1}{2} \left\| R^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes R_E \right\|_1 \leq \frac{1}{2} \sqrt{|Z|} \, \|R_{XE}\|_{\mathbb{1}_X \otimes \sigma_E}$$

+

variational form

$$D_2^{\varepsilon,\mathbb{M}}(\rho\|\sigma) = \log \inf \left\{ \|R\|_\sigma^2 \,\middle|\, R = R^\dagger,\ \|\rho - R\|_+ \leq \varepsilon,\ R \leq \rho \right\}$$

$$\mathbb{E}_f \frac{1}{2} \left\| \rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes \rho_E \right\|_1 \leq \varepsilon + \frac{1}{2} \sqrt{|Z| \, \exp\left(D_2^{\varepsilon,\mathbb{M}}(\rho_{XE} \| \mathbb{1}_X \otimes \sigma_E) \right)}$$

$$\ell_\varepsilon(\rho_{XE}) \geq H_2^{\varepsilon-\mu,\mathbb{M}}(X|E)_\rho - \log \frac{1}{4\mu^2} \geq H_{\min}^{\varepsilon-\mu,\mathbb{M}}(X|E)_\rho - \log \frac{1-\varepsilon+\mu}{4\mu^2}$$

matches tightest classical achievability results

arXiv:2603.04493

But how much better?

One-shot

previous: $$\ell_\varepsilon(\rho_{XE}) \geq H_{\min}^{(\varepsilon-\mu)/2,\,P}(X|E)_\rho - \log\frac{1}{4\mu^2}$$

(Tomamichel et al., 2011)
(Anshu et al., 2020)

ours: $$\ell_\varepsilon(\rho_{XE}) \geq H_{\min}^{\varepsilon-\mu,\,\mathbb{M}}(X|E)_\rho - \log\frac{1}{4\mu^2}$$

$$\geq H_{\min}^{\sqrt{\varepsilon-\mu},\,P}(X|E)_\rho - \log\frac{1}{4\mu^3}$$

improved scaling

"Second-order"

previous: $$\ell_\varepsilon(\rho_{XE}) \geq H_H^{1-\varepsilon+3\mu}(X|E)_\rho - \frac{1}{\mu^4} - 2\log|\mathrm{spec}(\rho_E)|$$

(Shen, Gao, Cheng, 2024)

ours: $$\ell_\varepsilon(\rho_{XE}) \geq H_{\min}^{\varepsilon-\mu,\,\mathbb{M}}(X|E)_\rho - \log\frac{1}{4\mu^2}$$

$$\geq H_H^{1-\varepsilon+\mu}(X|E)_\rho - \frac{1}{4\mu^2}$$

arXiv:2603.04493

Rényi divergences and exponents

$$\mathbb{E}_f \frac{1}{2} \left\| \rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes \rho_E \right\|_1 \leq \exp\left(- \sup_{\alpha \in (1,2]} \frac{\alpha - 1}{\alpha} \left(\widetilde{H}_\alpha(X|E)_\rho - \log|Z| \right) \right)$$

(Dupuis, 2023)

technique: complex interpolation of Schatten norms

smooth entropy approach

$$\mathbb{E}_f \frac{1}{2} \left\| \rho^f_{ZE} - \frac{\mathbb{1}_Z}{|Z|} \otimes \rho_E \right\|_1 \leq \exp\left(- \sup_{\alpha \in (1,2]} \frac{\alpha - 1}{\alpha} \left(H^{\mathbb{M}}_\alpha(X|E)_\rho - \log|Z| \right) \right)$$

one-shot improvement $D^{\mathbb{M}}_\alpha(\rho\|\sigma) < \widetilde{D}_\alpha(\rho\|\sigma)$ with equality iff commuting

$$\lim_{n\to\infty} \frac{1}{n} H^{\mathbb{M}}_\alpha(X^n|E^n)_{\rho^{\otimes n}} = \widetilde{H}_\alpha(X|E)_\rho$$

(Tomamichel and Hayashi, 2016)

On optimality

$$\ell_\varepsilon(\rho_{XE}) \geq H_{\min}^{\varepsilon-\mu,\mathbb{M}}(X|E)_\rho - \log\frac{1}{4\mu^2}$$

classical $\quad \ell_\varepsilon(p_{XE}) \leq H_{\min}^{\varepsilon,\mathbb{M}}(X|E)_p$ (Renner and Wolf, 2004)

quantum $\quad \ell_\varepsilon(\rho_{XE}) \not\leq H_{\min}^{\varepsilon,\mathbb{M}}(X|E)_\rho$ (Renes, 2018)

previously: restricted converses, other distance measures (Tomamichel and Hayashi, 2013) (Hayashi, 2016) (Shen, Gao, and Cheng, 2024)

approximate converse

$$\ell_\varepsilon(\rho_{XE}) \leq H_{\min}^{\varepsilon+\delta,\mathbb{M}}(X|E)_\rho + \log\frac{\varepsilon+\delta}{\delta}$$

(Tomamichel and Hayashi, 2013) (Regula, Lami, and Datta, 2026)

Idea: use purified distance + one-shot inequalities

$$\ell_\varepsilon(\rho_{XE}) \leq H_{\min}^{\sqrt{\varepsilon},P}(X|E)_\rho + \log\frac{1}{1-\varepsilon} \leq H_{\min}^{\varepsilon+\delta,\mathbb{M}}(X|E)_\rho + \log\frac{\varepsilon+\delta}{\delta}$$

arXiv:2603.04493

More asymptotics

$$\ell_\varepsilon\left(\rho_{XE}^{\otimes n}\right) \to n\, H(X|E)_\rho$$

Optimal second-order expansion

$$\ell_\varepsilon(\rho_{XE}^{\otimes n}) = n\, H(X|E)_\rho + \sqrt{n\, V(X|E)_\rho}\; \Phi^{-1}(\varepsilon) + O(\log n)$$ (Shen, Gao, and Cheng, 2024)

Asymptotic error exponent $\quad \ell_{\varepsilon_n}(\rho_{XE}^{\otimes n}) = \exp(nR)$

$$\liminf_{n\to\infty} -\frac{1}{n}\log(\varepsilon_n) \geq \sup_{\alpha\in(1,2]} \frac{\alpha-1}{\alpha}\left(\widetilde{H}_\alpha(X|E)_\rho - R\right)$$ (Dupuis, 2023)

$$\limsup_{n\to\infty} -\frac{1}{n}\log(\varepsilon_n) \leq \sup_{\alpha>1} (\alpha-1)\left(\widetilde{H}_\alpha(X|E)_\rho - R\right)$$

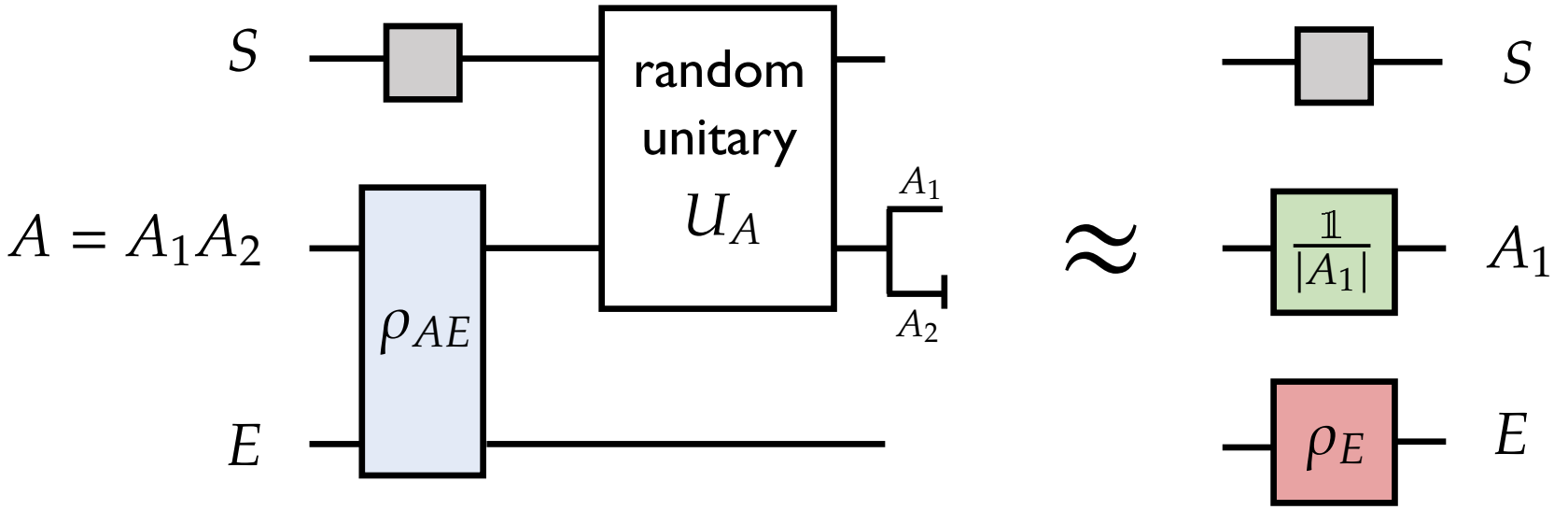
Strong converse exponent

$$\liminf_{n\to\infty} -\frac{1}{n}\log(1-\varepsilon_n) \geq \sup_{\alpha\in(0,1)} (\alpha-1)\left(\widetilde{H}_\alpha(X|E)_\rho - R\right)$$ (Shen, Gao, and Cheng, 2024)

$$\limsup_{n\to\infty} -\frac{1}{n}\log(1-\varepsilon_n) \leq \sup_{\alpha\in(0,1)} \frac{\alpha-1}{\alpha}\left(\overline{H}_\alpha(X|E)_\rho - R\right)$$

arXiv:2603.04493

Fully quantum extension to decoupling



(Dupuis et al., 2014)
(Dupuis, 2023)

$$\mathop{\mathbb{E}}_{U_A} \frac{1}{2}\left\|\mathrm{Tr}_{A_2}\left[\mathcal{U}_A(\rho_{AE})\right] - \frac{\mathbb{1}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \varepsilon + \frac{1}{2}\sqrt{\frac{|A_1|}{|A_2|}\exp\left(-H_2^{\varepsilon,\mathbb{M}}(A|E)_\rho\right)}$$

$$\mathop{\mathbb{E}}_{U_A} \frac{1}{2}\left\|\mathrm{Tr}_{A_2}\left[\mathcal{U}_A(\rho_{AE})\right] - \frac{\mathbb{1}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \exp\left(-\frac{\alpha-1}{\alpha}\left(H_\alpha^{\mathbb{M}}(A|E)_\rho + \log|A_2| - \log|A_1|\right)\right)$$

arXiv:2603.04493

Summary

- Introduced and characterised a new type of smoothing, naturally generalising classical trace distance smoothing: measured smooth Rényi divergences

- Showed that this gives the tightest known bounds on quantum privacy amplification and decoupling: we improve on quantum leftover hash lemma and all known one-shot results, giving a unified derivation of best known asymptotic bounds

- Key quantity: measured smooth collision divergence, its variational forms, one-shot inequalities, useful properties…

- Need to reconsider smoothing in quantum information — conventional smoothing notions lead to suboptimal results!

arXiv:2603.04493

Open questions

Need to rethink smoothing

- Improvements in other one-shot quantum information tasks?
- Overcoming limitations of trace distance smoothing?

Basic idea: use measured Rényi divergences!

- Chain rules? Entropy accumulation?
- Ways to improve on security proofs, key rates, etc.?
- Applications to restricted measurements (e.g. computational entropies)

Some caveats:

- Why purified distance needed for converse?
- Many questions regarding optimality of exponents, monotonicity of Rényi divergences…

Thank you

arXiv:**2603.04493**

TL;DR: you've been smoothing entropies wrong