Smooth Entropies — A Tutorial

With Focus on Applications in Cryptography.

Marco Tomamichel

CQT, National University of Singapore

Singapore, September 14, 2011

Outline

1. Short Motivation and Overview of Applications
2. Preliminaries
3. Definition of the Min-Entropy and Smoothing
4. Some Useful Properties
   - Data-Processing
   - The Asymptotic Equipartition Property
   - An Entropic Uncertainty Relation
5. Example Application: Proving Security of Quantum Key Distribution on four slides.

Remember:

My goal: After this tutorial, you feel comfortable with the min-entropy and understand how it is applied.
Please interrupt and ask questions at any time!

Motivation and Overview

Just a quick overview.

Entropic Approach to Information I

- Probability theory offers many advantages to describe cryptographic problems.
- For example, how do we describe a secret key?

$$X = \text{"}010101001001110011101000\text{"}$$

  Is this string secret? From whom? We cannot tell unless we know how it is created.
- Instead, we look at the joint probability distribution over potential strings and side information, P_{XE}. Here, E is any information a potential adversary might hold about X.
- If P_X is uniform and independent of E, we call it secret.

Entropic Approach to Information II

- We can also describe this situation with entropy [Sha48].
- Shannon defined the surprisal of an event $X = x$ as $S(x)_P = -\log P(x)$.
- We can thus call a string secret if the average surprisal, $H(X)_P = \sum_x P(x)S(x)_P$, is large.
- Entropies are measures of uncertainty about (the value of) a random variable.
- There are other entropies, for example the min-entropy or Rényi entropy [Rén61] of order ∞.

$$H_{\min}(X) = \min_x S(x)_P.$$

- The min-entropy quantifies how hard it is to guess X. (The optimal guessing strategy is to guess the most likely event, and the probability of success is $p_{\text{guess}}(X)_P = 2^{-H_{\min}(X)_P}$.)

Entropic Approach to Information III

- Entropies can be easily extended to (classical) side information, using conditional probability distributions.
- In the quantum setting, conditional states are not available (there exist some definitions, but none of them appear very useful) and the entropic approach is often the only available option to quantify information.
- The von Neumann entropy generalizes Shannon's entropy to the quantum setting,

$$H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B), \quad H(\rho) = -\mathrm{tr}(\rho \log \rho).$$

- This tutorial is concerned with a quantum extension of the min-entropy.

Foundations

- The quantum generalization of the conditional min- and max-entropy was introduced by Renner [Ren05] in his thesis.
- The main purpose was to generalize a theorem on privacy amplification to the quantum setting.
- Since then, the smooth entropy framework has been consolidated and extended [Tom12].
  - The definition of $H_{\max}$ is not what it used to be [KRS09].
  - The smoothing is now done with regards to the purified distance [TCR10].
- A relative entropy based on the quantum generalization of the min-entropy was introduced by Datta [Dat09].

Applications

Smooth Min- and Max-Entropies have many applications.

Cryptography: Privacy Amplification [RK05, Ren05], Quantum Key Distribution [Ren05, TLGR12], Bounded Storage Model [DrFSS08, WW08] and Noisy Storage Model [KWW12], No Go for Bit Commitment [WTHR11] and OT [WW12] growing.

Information Theory: One-Shot Characterizations of Operational Quantities (e.g. [Ber08], [BD10]).

Thermodynamics: One-Shot Work Extraction [DRRV11] and Erasure [dRAR$^+$11].

Uncertainty: Entropic Uncertainty Relations with Quantum Side Information [BCC$^+$10, TR11].

Correlations: To Investigate Correlations, Entanglement and Decoupling (e.g. [Dup09, DBWR10, Col12]).

Mathematical Preliminaries

Stay with me through this part, after which I hope everybody is on the same level.

Hilbert Spaces and Operators

Definition

A finite-dimensional Hilbert space, denoted $\mathcal{H}$, is a vector space with an inner product, $\langle \cdot\, , \cdot \rangle$.

- Elements of $\mathcal{H}$ are written as kets, e.g. $|\psi\rangle \in \mathcal{H}$.
- The set of linear operators from $\mathcal{H}$ to $\mathcal{H}'$ is denoted $L(\mathcal{H}, \mathcal{H}')$.
- Adjoint operators $L^\dagger$ to L are (uniquely) defined via the relation $\langle |\psi\rangle, L|\phi\rangle \rangle = \langle L^\dagger |\psi\rangle, |\phi\rangle \rangle$.
- To simplify notation, we just write such an inner product as $\langle \psi | L | \phi \rangle = \langle |\psi\rangle, L|\phi\rangle \rangle$.
- $L(\mathcal{H}, \mathcal{H}')$ is a Hilbert space with the Hilbert-Schmidt inner product $\langle L, K \rangle = \mathrm{tr}(L^\dagger K)$.

Positive Operators

- We use $L(\mathcal{H}) := L(\mathcal{H}, \mathcal{H})$ for operators mapping $\mathcal{H}$ onto itself.
- An operator $L \in L(\mathcal{H})$ is called Hermitian (or self-adjoint) if it satisfies $L = L^\dagger$.

Definition

A linear operator $A \in L(\mathcal{H})$ is called positive semi-definite if

$$A = A^\dagger \quad \text{and} \quad \forall\, |\psi\rangle \in \mathcal{H} : \quad \langle\psi|A|\psi\rangle \geq 0.$$

- We write $A \geq B$ if $A - B$ is positive semi-definite.
- Operators $|L| := \sqrt{L^\dagger L}$ are always positive semi-definite.
- The operator 1 is the identity operator on $\mathcal{H}$.

Tensor Spaces

- We distinguish mathematical objects corresponding to different physical systems using subscripts.
- The tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ is a vector space of linear combinations of elements $|\psi_A\rangle \otimes |\psi_B\rangle$, modulus

$$\begin{aligned} &\alpha\big(|\psi_A\rangle \otimes |\psi_B\rangle\big) \equiv \big(\alpha|\psi_A\rangle\big) \otimes |\psi_B\rangle \equiv |\psi_A\rangle \otimes \big(\alpha|\psi_B\rangle\big)\,, \\ &|\psi_A\rangle \otimes |\psi_B\rangle + |\psi_A\rangle \otimes |\phi_B\rangle \equiv |\psi_A\rangle \otimes \big(|\psi_B\rangle + |\phi_B\rangle\big) \qquad \text{and} \\ &|\psi_A\rangle \otimes |\psi_B\rangle + |\phi_A\rangle \otimes |\psi_B\rangle \equiv \big(|\psi_A\rangle + |\phi_A\rangle\big) \otimes |\psi_B\rangle\,, \end{aligned}$$

  where $|\psi_A\rangle, |\phi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle, |\phi_B\rangle \in \mathcal{H}_B$.
- Its inner product is a sesquilinear extension of

$$\langle |\psi_A\rangle \otimes |\psi_B\rangle, |\phi_A\rangle \otimes |\phi_B\rangle \rangle = \langle \psi_A|\phi_A\rangle \, \langle \psi_B|\phi_B\rangle\,.$$

Quantum States

Definition

A quantum state is an operator $\rho_A \geq 0$ with $\mathrm{tr}(\rho_A) = 1$.

- The set of quantum states on a Hilbert space $\mathcal{H}_A$ is $S(\mathcal{H}_A)$.
- We say a quantum state $\rho_{XB} \in \mathcal{H}_X \otimes \mathcal{H}_B$ is classical-quantum (CQ) if it is of the form

$$\rho_{XB} = \sum_x p_x |e_x\rangle\langle e_x| \otimes \rho_B^x \,,$$

  where $\{p_x\}_x$ is a probability distribution, $\{|e_x\rangle\}_x$ a fixed orthonormal basis of $\mathcal{H}_X$, and $\rho_B^x \in S(\mathcal{H}_B)$.
- A state is pure if it has rank 1, i.e., if it can be written as $\rho_A = |\psi\rangle\langle\psi|$, where $|\psi\rangle\langle\psi|$ is used to denote rank-1 projectors.

Distance between States

We use two metrics between quantum states:

Definition

The trace distance is defined as

$$\Delta(\rho,\sigma) := \frac{1}{2}\mathrm{tr}|\rho-\sigma|\,.$$

and the purified distance [TCR10] is defined as

$$P(\rho,\sigma) = \sqrt{1-F(\rho,\sigma)}.$$

- The fidelity is $F(\rho,\sigma) = \left(\mathrm{tr}|\sqrt{\rho}\sqrt{\sigma}|\right)^2$.
- Fuchs-van de Graaf Inequality [FvdG99]:

$$\Delta(\rho,\sigma) \leq P(\rho,\sigma) \leq \sqrt{2\Delta(\rho,\sigma)}.$$

Completely Positive Maps

Definition

A completely positive map (CPM), $\mathcal{E}$, is a linear map from $L(\mathcal{H}_A)$ to $L(\mathcal{H}_B)$ of the form

$$\mathcal{E} : X \mapsto \sum_k L_k X L_k^\dagger ,$$

where L_k are linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$.

- CPMs map positive semi-definite operators onto positive semi-definite operators.
- They are trace-preserving (TP) if $\mathrm{tr}(\mathcal{E}(K)) = \mathrm{tr}(K)$ for all $K \in L(\mathcal{H}_A)$.
- They are unital if $\mathcal{E}(1_A) = 1_B$.
- The adjoint map $\mathcal{E}^\dagger$ of $\mathcal{E}$ is defined through the relation $\langle L, \mathcal{E}(K)\rangle = \langle \mathcal{E}^\dagger(L), K\rangle$ for all $L \in L(\mathcal{H}')$, $K \in L(\mathcal{H})$.
- The partial trace, tr_B, is the adjoint map to $\rho_A \mapsto \rho_A \otimes 1_B$.

Choi-Jamiolkowski Isomorphism

- The adjoint maps of trace-preserving maps are unital, and the adjoint maps of unital maps are trace-preserving.

The Choi-Jamiolkowski isomorphism establishes a one-to-one correspondence between CPMs from $L(\mathcal{H}_A)$ to $L(\mathcal{H}_B)$ and positive semi-definite operators in $L(\mathcal{H}_A \otimes \mathcal{H}_B)$.

$$\text{cj} : \mathcal{E} \mapsto \omega_{AB}^{\mathcal{E}} = \mathcal{E}_{A' \to B}\left(|\gamma_{AA'}\rangle\langle\gamma_{AA'}|\right), \quad \text{where } |\gamma_{AA'}\rangle = \sum_x |e_x\rangle \otimes |e_x\rangle$$

for some orthonormal basis $\{|e_x\rangle\}_x$ of $\mathcal{H}_A$.

- Choi-Jamiolkowski states of TP CPMs satisfy $\text{tr}_B\left(\omega_{AB}^{\mathcal{E}}\right) = 1_A$.
- Choi-Jamiolkowski states of unital CPMs satisfy $\text{tr}_A\left(\omega_{AB}^{\mathcal{E}}\right) = 1_B$.

Measurements

Definition

A positive operator-valued measure (POVM) on $\mathcal{H}_A$ is a set $\{M_x\}_x$ of operators $M_x \geq 0$ such that $\sum_x M_x = 1_A$.

- The associated measurement is the unital TP CPM

$$\mathcal{M}_X : \rho_{AB} \mapsto \rho_{XB} = \sum_x |e_x\rangle\langle e_x| \otimes \mathrm{tr}_A\big(\sqrt{M_x}\rho_{AB}\sqrt{M_x}\big),$$

  where we omit 1_B to shorten notation.
- The resulting state $\rho_{XB} = \sum_x p_x |e_x\rangle\langle e_x| \otimes \rho_B^x$ is CQ with $p_x = \mathrm{tr}\big(\sqrt{M_x}\rho_{AB}\sqrt{M_x}\big)$ and $\rho_B^x = 1/p_x \cdot \sqrt{M_x}\rho_{AB}\sqrt{M_x}$.
- If all M_x satisfy $(M_x)^2 = M_x$, the measurement is projective. Moreover, if all M_x have rank 1, it is a rank-1 measurement.

The most important rule!

Lemma

For any CPM $\mathcal{E}$, the following implication holds

$$A \geq B \implies \mathcal{E}(A) \geq \mathcal{E}(B).$$

Proof.

$$A \geq B \implies A - B \geq 0 \implies \mathcal{E}(A - B) \geq 0 \implies \mathcal{E}(A) \geq \mathcal{E}(B). \quad \square$$

- Example: $A \geq B \implies LAL^\dagger \geq LBL^\dagger$ for any L.

Semi-Definite Programming

- We use the notation of Watrous [Wat08] and restrict to positive operators.

Definition

A semi-definite program (SDP) is a triple $\{A, B, \Psi\}$, where $A \geq 0$, $B \geq 0$ and Ψ a CPM. The following two optimization problems are associated with the semi-definite program.

primal problem		dual problem	
`minimize :`	$\langle A, X \rangle$	`maximize :`	$\langle B, Y \rangle$
`subject to :`	$\Psi(X) \geq B$	`subject to :`	$\Psi^\dagger(Y) \leq A$
	$X \geq 0$		$Y \geq 0$

- Under certain weak conditions, both optimizations evaluate to the same value. (This is called strong duality.)

The Min-Entropy and Guessing

Now it gets more interesting.

Min-Entropy: Definition

Definition (Min-Entropy)

Let $\rho_{AB} \in S(\mathcal{H}_{AB})$ be a quantum state. The min-entropy of A conditioned on B of the state ρ_{AB} is

$$H_{\min}(A|B)_\rho := \sup\left\{\lambda \in \mathbb{R} \,\middle|\, \exists \sigma_B \in S(\mathcal{H}_B) : \rho_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B\right\}.$$

- The supremum is bounded from above by $\log \dim\{\mathcal{H}_A\}$.
  ($\rho_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B \implies 1 \leq 2^{-\lambda} \dim\{\mathcal{H}_A\}$.)
- Choosing $\sigma_B = 1_B / \dim\{\mathcal{H}_B\}$, we see that $2^{-\lambda} = \dim\{\mathcal{H}_B\}$ is a lower bound.
- This implies $-\log \dim\{\mathcal{H}_B\} \leq H_{\min}(A|B)_\rho \leq \log \dim\{\mathcal{H}_A\}$.
- The set is also closed, thus compact, and we can replace the supremum by a maximum.

Question:

Nice, but how can I calculate this messy thing for a given state?

Min-Entropy: SDP I

Recall: $H_{\min}(A|B)_\rho = \max\left\{\lambda \in \mathbb{R} \,\middle|\, \exists \sigma_B \in S(\mathcal{H}_B) : \rho_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B\right\}$

We can rewrite this as

$$2^{-H_{\min}(A|B)_\rho} = \min\left\{\mu \in \mathbb{R}^+ \,\middle|\, \exists \sigma_B \in S(\mathcal{H}_B) : \rho_{AB} \leq \mu 1_A \otimes \sigma_B\right\}.$$

Absorbing μ into σ_B, we can express $2^{-H_{\min}(A|B)_\rho}$ as the primal problem of an SDP.

The primal problem for the min-entropy.

$$\underline{\text{primal problem}}$$

$$\begin{aligned} \texttt{minimize}: \quad & \langle 1_B, \sigma_B \rangle \\ \texttt{subject to}: \quad & 1_A \otimes \sigma_B \geq \rho_{AB} \\ & \sigma_B \geq 0 \end{aligned}$$

Min-Entropy: SDP II

Recall the primal problem for the min-entropy:

$$\begin{aligned} \texttt{minimize}: \quad & \langle 1_B, \sigma_B \rangle \\ \texttt{subject to}: \quad & 1_A \otimes \sigma_B \geq \rho_{AB} \\ & \sigma_B \geq 0 \end{aligned}$$

To find the dual program

- We introduce a dual variable $X_{AB} \geq 0$.
- We use $\Psi : \sigma_B \mapsto 1_A \otimes \sigma_B$. Then, $\Psi^\dagger : X_{AB} \mapsto \mathrm{tr}_A(X_{AB})$.

The SDP for the min-entropy.

primal problem	dual problem
$\texttt{minimize}: \langle 1_B, \sigma_B \rangle$	$\texttt{maximize}: \langle \rho_{AB}, X_{AB} \rangle$
$\texttt{subject to}: 1_A \otimes \sigma_B \geq \rho_{AB}$	$\texttt{subject to}: X_B \leq 1_B$
$\sigma_B \geq 0$	$X_{AB} \geq 0$

This SDP is strongly dual (without proof).

Min-Entropy: SDP III

Recall the SDP for the min-entropy:

$$\begin{array}{rl} \texttt{minimize}: & \langle 1_B, \sigma_B \rangle \\ \texttt{subject to}: & 1_A \otimes \sigma_B \geq \rho_{AB} \\ & \sigma_B \geq 0 \end{array} \qquad \begin{array}{rl} \texttt{maximize}: & \langle \rho_{AB}, X_{AB} \rangle \\ \texttt{subject to}: & X_B \leq 1_B \\ & X_{AB} \geq 0 \end{array}$$

- The dual optimal states will always satisfy $X_B = 1_B$.
- They correspond to Choi-Jamiolkowski states of unital CPMs from A to B.
- Their adjoint maps are TP CPMs from B to A.
- We thus find the following expression for the min-entropy:

$$\begin{aligned} 2^{-H_{\min}(A|B)_\rho} &= \max_{\mathcal{E}^\dagger} \langle \rho_{AB}, \mathcal{E}^\dagger_{A' \to B}(|\gamma\rangle\langle\gamma|) \rangle \\ &= \max_{\mathcal{E}} \langle \gamma_{AA'} | \mathcal{E}_{B \to A'}(\rho_{AB}) | \gamma_{AA'} \rangle \,, \end{aligned}$$

  where we optimize over all TP CPMs $\mathcal{E}_{B \to A'}$ from B to A', and fix $|\gamma_{AA'}\rangle = \sum_k |e_k\rangle \otimes |e_k\rangle$.

Guessing Probability

Recall: $2^{-H_{\min}(A|B)_\rho} = \max_{\mathcal{E}} \langle \gamma_{AA'} | \mathcal{E}_{B\to A'}(\rho_{AB}) | \gamma_{AA'} \rangle$.

- We consider a CQ state ρ_{XB}. Then, the expression simplifies

$$2^{-H_{\min}(X|B)_\rho} = \max_{\mathcal{E}} \sum_{x,y,z} \big(\langle e_y| \otimes \langle e_y|\big) p_x |e_x\rangle\langle e_x| \otimes \mathcal{E}(\rho_B^x)\big(|e_z\rangle \otimes |e_z\rangle\big)$$
$$= \max_{\mathcal{E}} \sum_x p_x \langle e_x | \mathcal{E}(\rho_B^x) | e_x \rangle .$$

- The maximum is taken for maps of the form $\mathcal{E} : \rho_B \mapsto \sum_x |e_x\rangle\langle e_x| \operatorname{tr}\big(M_x \rho_B\big)$, where $\{M_x\}_x$ is a POVM. Thus

$$2^{-H_{\min}(X|B)_\rho} = \max_{\{M_x\}_x} \sum_x p_x \operatorname{tr}(M_x \rho_B^x)$$

- This is the maximum probability of guessing X correctly for an observer with access to the quantum system B [KRS09].

The Max-Entropy

Recall: $2^{-H_{\min}(A|B)_\rho} = \max_{\mathcal{E}} \langle\gamma|\mathcal{E}_{B\to A'}(\rho_{AB})|\gamma\rangle = \max_{\mathcal{E}} F\big(|\gamma\rangle\langle\gamma|, \mathcal{E}_{B\to A'}(\rho_{AB})\big)$.

- We assume ρ_{ABC} is a purification of ρ_{AB}.
- For every TP CPM $\mathcal{E}_{B\to A'}$, there exists an isometry U from $\mathcal{H}_B$ to $\mathcal{H}'_A \otimes \mathcal{H}'_B$ such that $\mathcal{E}(\rho) = \mathrm{tr}_{B'}(U\rho U^\dagger)$.
- Using Uhlmann's theorem, we can thus write

$$2^{-H_{\min}(A|B)_\rho} = \max_{U_{B\to A'B'}} \max_{\theta_{B'C}} F\big(|\gamma\rangle\langle\gamma| \otimes |\theta\rangle\langle\theta|, U\rho_{ABC}U^\dagger\big).$$

- Again applying Uhlmann's theorem, this time to $\mathrm{tr}_{B'C'}$, yields

$$2^{-H_{\min}(A|B)_\rho} = \max_{\sigma_C} F\big(1_A \otimes \sigma_C, \rho_{AC}\big) =: 2^{H_{\max}(A|C)_\rho}.$$

Definition (Max-Entropy)

The max-entropy of A given B of a state $\rho_{AB} \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$ is

$$H_{\max}(A|B)_\rho := \max_{\sigma_B} \log F\big(1_A \otimes \sigma_B, \rho_{AB}\big).$$

Examples I

- For a pure state $\rho_{AB} = |\psi\rangle\langle\psi|$ in Schmidt decomposition $|\psi_{AB}\rangle = \sum_i \sqrt{\mu_i}|e_i\rangle \otimes |e_i\rangle$, we get $\rho_A = \sum_i \mu_i |e_i\rangle\langle e_i|$ and

$$\begin{aligned} H_{\min}(A|B)_\rho = -H_{\max}(A)_\psi &= -\log F(1_A, \rho_A) \\ &= -\log \Big(\sum_i \sqrt{\mu_i} \Big)^2 . \end{aligned}$$

- For a maximally entangled state, $\mu_i = \frac{1}{d}$, and

$$H_{\min}(A|B)_\rho = -\log d \, .$$

- This is also evident from the expression

$$H_{\min}(A|B)_\rho = -\log \max_{\mathcal{E}} F\big(|\gamma\rangle\langle\gamma|, \mathcal{E}_{B\to A'}(\rho_{AB})\big)$$

as $|\psi\rangle = \frac{1}{\sqrt{d}}|\gamma\rangle$ is already of the required form.

Examples II

Recall the SDP for the min-entropy:

$$\begin{array}{rl} \texttt{minimize}: & \langle 1_B, \sigma_B \rangle \\ \texttt{subject to}: & 1_A \otimes \sigma_B \geq \rho_{AB} \\ & \sigma_B \geq 0 \end{array} \qquad \begin{array}{rl} \texttt{maximize}: & \langle \rho_{AB}, X_{AB} \rangle \\ \texttt{subject to}: & X_B \leq 1_B \\ & X_{AB} \geq 0 \end{array}$$

- Take product states $\rho_{AB} = \rho_A \otimes \rho_B$ with $\rho_A = \sum_x \mu_x |e_x\rangle\langle e_x|$, and $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_k$.
- We choose $\sigma_B = \mu_1 \rho_B$ and $X_{AB} = |e_1\rangle\langle e_1| \otimes 1_B$.
- Clearly, $1_A \otimes \sigma_B \geq \rho_A \otimes \rho_B$ since $\mu_1 1_A \geq \rho_A$. Hence, σ_B and X_{AB} are feasible.
- This gives us lower and upper bounds on the min-entropy

$$\mu_1 = \langle \rho_{AB}, X_{AB} \rangle \leq 2^{-H_{\min}(A|B)_\rho} \leq \langle 1_B, \sigma_B \rangle = \mu_1 \,.$$

- Finally, note that $H_{\min}(A|B)_\rho = -\log \mu_1 = H_{\min}(A)_\rho$.

Is the Min-Entropy a Rényi-Entropy?

- Yes (ongoing work with Oleg Szehr and Frédéric Dupuis), the Rényi-Entropies

$$H_\alpha(A)_\rho := \frac{\alpha}{1-\alpha} \log \|\rho_A\|_\alpha$$

can be generalized to

$$H_\alpha(A|B)_{\rho,\sigma} := \frac{\alpha}{1-\alpha} \log \left\| \frac{\rho_{AB}}{\sigma_B} \right\|_{\alpha, 1_A \otimes \sigma_B},$$

where $\frac{\rho_{AB}}{\sigma_B} = (1_A \otimes \sigma_B)^{-\frac{1}{2}} \rho_{AB} (1_A \otimes \sigma_B)^{-\frac{1}{2}}$ and we use the weighted norms

$$\|\rho\|_{\alpha,\tau} := \left(\mathrm{tr}\left(\tau^{\frac{1}{2\alpha}} \rho \, \tau^{\frac{1}{2\alpha}} \right)^\alpha \right)^{\frac{1}{\alpha}}.$$

- Now, $H_{\min}(A|B)_\rho = \max_{\sigma_B} \lim_{n\to\infty} H_\alpha(A|B)_{\rho,\sigma}$
- And $H_{\max}(A|B)_\rho = \max_{\sigma_B} H_{\frac{1}{2}}(A|B)_{\rho,\sigma}$.

Smooth Min- and Max-Entropies

And their operational interpretation.

Why Smoothing?

1. Most properties of the min- and max-entropy generalize to smooth entropies.
2. On top of that, the smooth entropies have additional properties. Most prominently, they satisfy an entropic equipartition law which relates them to the conditional von Neumann entropy.
3. The smoothing parameter has operational meaning in some applications, for example, the ε-smooth min-entropy characterizes how much ε-close to uniform randomness can be extracted from a random variable.
4. The smooth entropies allow us to exclude improbable events. A statistical analysis performed on a random sample of states may thus allow us to bound a smooth entropy, but not (directly) the actual min- or max-entropy.

A Ball of ε-Close States

Recall: $P(\rho,\tau) := \sqrt{1 - F(\rho,\tau)}$, where F is the fidelity.

- We write $\rho \approx^{\varepsilon} \tau$ if $P(\rho,\tau) \leq \varepsilon$.
- The purified distance has a triangle inequality $P(\rho,\sigma) \leq P(\rho,\tau) + P(\tau,\sigma)$.
- The purified distance is contractive under TP CPMs $\mathcal{E}$ and projections Π, $\Pi^2 = \Pi$:

$$\rho \approx^{\varepsilon} \tau \implies \mathcal{E}(\rho) \approx^{\varepsilon} \mathcal{E}(\tau) \quad \wedge \quad \Pi\rho\Pi \approx^{\varepsilon} \Pi\tau\Pi\,.$$

- For two states $\rho_A \approx^{\varepsilon} \tau_A$ a state ρ_{AB} with $\mathrm{tr}_B(\rho_{AB}) = \rho_A$, there exists a state τ_{AB} with $\mathrm{tr}_B(\tau_{AB}) = \tau_A$ and $\tau_{AB} \approx^{\varepsilon} \rho_{AB}$.
- We define a ball of ε-close states around ρ as

$$B^{\varepsilon}(\rho) := \left\{ \tilde{\rho} \geq 0 \,\middle|\, \tilde{\rho} \approx^{\varepsilon} \rho \ \wedge \ \mathrm{tr}(\tilde{\rho}) \leq 1 \right\}.$$

Smooth Entropies

Definition (Smooth Entropies [TCR10])

Let $0 \leq \varepsilon < 1$ and $\rho_{AB} \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$. The ε-smooth min-entropy of A given B is defined as

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \max_{\tilde{\rho}_{AB} \in B^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}\,.$$

The ε-smooth max-entropy of A given B is defined as

$$H_{\max}^{\varepsilon}(A|B)_{\rho} := \min_{\tilde{\rho}_{AB} \in B^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}\,.$$

- They satisfy a duality relation: $H_{\max}^{\varepsilon}(A|B)_{\rho} = -H_{\min}^{\varepsilon}(A|C)_{\rho}$ for any pure state ρ_{ABC}.

Operational Interpretation: Smooth Min-Entropy I

- Investigate the maximum number of random and independent bits that can be extracted from a CQ random source ρ_{XE}.
- A protocol $\mathcal{P}$ extracts a random number Z from X.

$$\ell^{\varepsilon}(X|E)_{\rho} := \max\left\{\ell \in \mathbb{N} \,\middle|\, \exists\, \mathcal{P}, \sigma_E : |Z| = 2^{\ell} \wedge \rho_{ZE} \approx^{\varepsilon} 2^{-\ell} 1_Z \otimes \sigma_E\right\}.$$

- Renner [Ren05] showed that $H_{\min}^{\varepsilon}(A|B)$ can be extracted, up to terms logarithmic in ε, and a converse was shown for $\varepsilon = 0$.
- We recently showed a stronger result [TH12]

$$H_{\min}^{\varepsilon}(X|E)_{\rho} \geq \ell^{\varepsilon}(X|E)_{\rho} \geq H_{\min}^{\varepsilon-\eta}(X|E)_{\rho} - 4\log\frac{1}{\eta} - 3\,.$$

- The smoothing parameter, ε, thus has operational meaning as the allowed distance from perfectly secret randomness.

Operational Interpretation: Smooth Min-Entropy II

Recall: $\ell^0(X|E)_\rho = \max\left\{\ell \in \mathbb{N} \,\middle|\, \exists \mathcal{P}, \sigma_E : |Z| = 2^\ell \wedge \rho_{ZE} = 2^{-\ell} 1_Z \otimes \sigma_E\right\}$.

- To get some intuition, we can consider the case $\varepsilon = 0$.
- We now show that $H_{\min}(X|E)_\rho \geq \ell^0(X|E)_\rho$, i.e. that the number of perfectly secret bits that can be extracted from X is bounded by the conditional min-entropy of X given E.

Proof.

- By definition, the protocol must output a state of the form $\rho_{ZE} = 2^{-\ell} 1_Z \otimes \sigma_E$. Hence, $p_{\text{guess}}(Z|E)_\rho = 2^{-\ell} \leq 2^{-\ell^0(X|E)_\rho}$.
- Since $Z = f(X)$ is the output of a function, and since it is harder to guess the input of a function than its output, we get $p_{\text{guess}}(Z|E)_\rho \geq p_{\text{guess}}(X|E)_\rho$.
- Thus,

$$\begin{aligned} H_{\min}(X|E)_\rho &= -\log p_{\text{guess}}(X|E)_\rho \\ &\geq -\log p_{\text{guess}}(Z|E)_\rho \geq \ell^0(X|E)_\rho \,. \end{aligned}$$

□

Operational Interpretation: Smooth Max-Entropy

- Find the minimum encoding length for data reconciliation of X if quantum side information B is available.
- A protocol $\mathcal{P}$ encodes X into M and then produces an estimate X' of X from B and M.

$$m^{\varepsilon}(X|E)_{\rho} := \min\left\{m \in \mathbb{N} \,\middle|\, \exists \mathcal{P} : |M| = 2^m \wedge P[X \neq X'] \leq \varepsilon\right\}.$$

- Renes and Renner [RR12] showed that

$$H_{\max}^{\sqrt{2\varepsilon}}(X|B)_{\rho} \leq m^{\varepsilon}(X|B)_{\rho} \leq H_{\max}^{\varepsilon-\eta}(X|B)_{\rho} + 2\log\frac{1}{\eta} + 4\,.$$

- The smoothing parameter, ε, is related to the allowed decoding error probability.

Basic Properties of Smooth Entropies

Asymptotic Equipartition

- Classically, for n independent and identical (i.i.d.) repetitions of a task, we consider a random variable $X^n = (X_1, \ldots, X_n)$ and a probability distribution $P[X^n = x^n] = \prod_i P[X_i = x_i]$.
- Then, $-\log P(x^n) \to H(X)$ in probability for $n \to \infty$.
- This means that the distribution is essentially flat, and since smoothing removes "untypical" events, all entropies converge to the Shannon entropy.

Theorem (Entropic Asymptotic Equipartition [TCR09])

Let $0 < \varepsilon < 1$ and $\rho_{AB} \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$. Then, the sequence of states $\{\rho_{AB}^n\}_n$, with $\rho_{AB}^n = \rho_{AB}^{\otimes n}$, satisfies

$$\lim_{n\to\infty} \frac{1}{n} H_{\min}^{\varepsilon}(A|B)_{\rho^n} = \lim_{n\to\infty} \frac{1}{n} H_{\max}^{\varepsilon}(A|B)_{\rho^n} = H(A|B)_{\rho}\,.$$

Data-Processing Inequalities

- Operations on the observers (quantum) memory cannot decrease the uncertainty about the system.
- We consider a TP CPM $\mathcal{E}$ from B to B'. This maps the state ρ_{AB} to $\tau_{AB'} = \mathcal{E}(\rho_{AB})$ and

$$H_{\min}^{\varepsilon}(A|B')_{\tau} \geq H_{\min}^{\varepsilon}(A|B)_{\rho}\,, \quad H_{\max}^{\varepsilon}(A|B')_{\tau} \geq H_{\max}^{\varepsilon}(A|B)_{\rho}\,.$$

- An additional register K with k bits of classical information cannot decrease the uncertainty by more than k. Thus,

$$H_{\min}^{\varepsilon}(A|BK) \geq H_{\min}^{\varepsilon}(A|B) - k\,,$$
$$H_{\max}^{\varepsilon}(A|BK) \geq H_{\max}^{\varepsilon}(A|B) - k\,.$$

Data-Processing Inequalities II

Theorem (Data-Processing for Min-Entropy)

Let $0 \leq \varepsilon < 1$, $\rho_{AB} \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$, *and* $\mathcal{E}$ *a TP CPM from* B *to* B' *with* $\tau_{AB'} = \mathcal{E}(\rho_{AB})$. *Then,*

$$H_{\min}^{\varepsilon}(A|B')_{\tau} \geq H_{\min}^{\varepsilon}(A|B)_{\rho}.$$

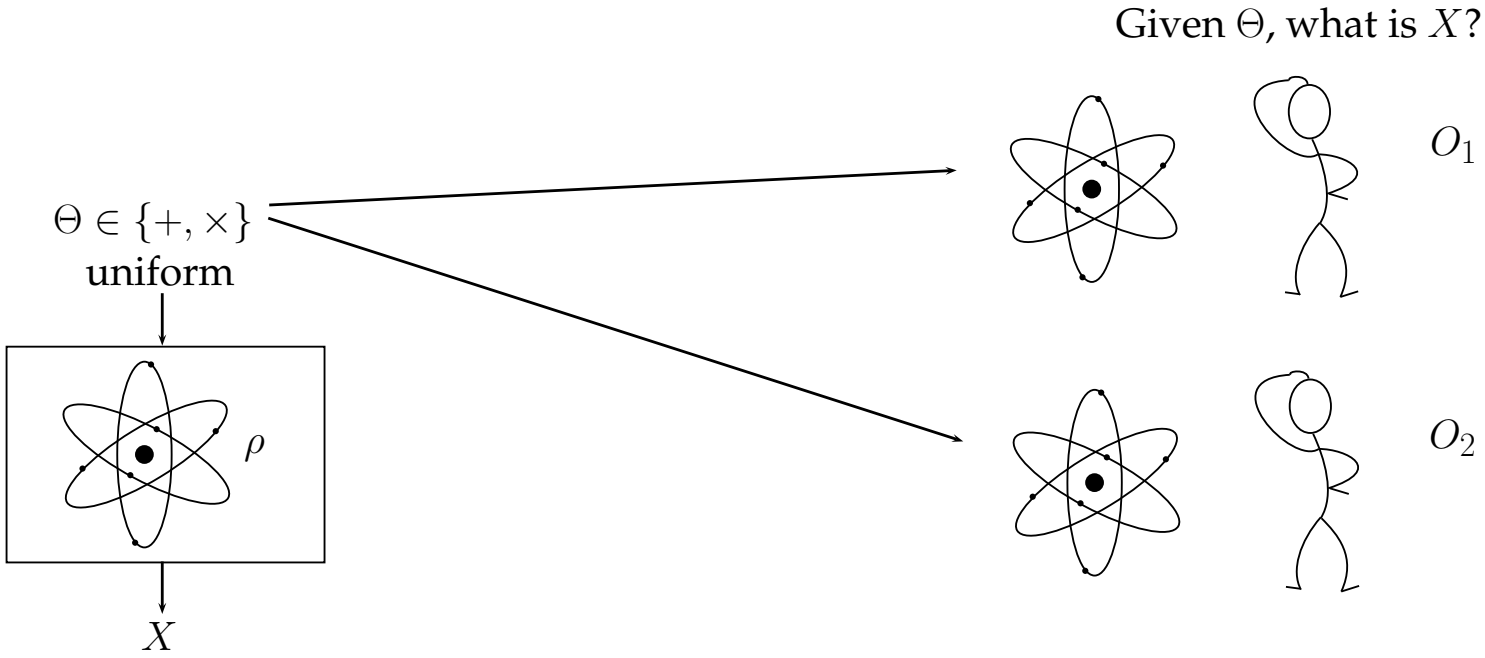
Recall: $H_{\min}^{\varepsilon}(A|B)_{\rho} = \max\left\{\lambda \,\middle|\, \exists \sigma_B, \tilde{\rho}_{AB} : \tilde{\rho}_{AB} \approx^{\varepsilon} \rho_{AB} \wedge \tilde{\rho}_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B\right\}$.

- Set $\lambda = H_{\min}^{\varepsilon}(A|B)_{\rho}$. Then, by definition there exists a state $\tilde{\rho}_{AB} \approx^{\varepsilon} \rho_{AB}$ and a state $\sigma_B \in S(\mathcal{H}_B)$ such that

$$\tilde{\rho}_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B \implies \mathcal{E}(\tilde{\rho}_{AB}) \leq 2^{-\lambda} 1_A \otimes \mathcal{E}(\sigma_B)\,.$$

- Contractivity: $\mathcal{E}(\tilde{\rho}_{AB}) \approx^{\varepsilon} \tau_{AB'}$. Also, $\mathcal{E}(\sigma_B) \in S(\mathcal{H}_{B'})$.
- Thus, $H_{\min}^{\varepsilon}(A|B')_{\tau} \geq \lambda$. □

Entropic Uncertainty I



- The observers, Bob (O_1) and Charlie (O_2), prepare a tripartite quantum state, shared with Alice. (This can be an arbitrary state ρ_{ABC}.)
- Alice measures her system in a basis determined by Θ.
- What is the entropy the observers have about the outcome X, after they are given Θ?

Entropic Uncertainty II

Apply measurement in a basis determined by a uniform $\theta \in \{0,1\}$.

Theorem (Entropic Uncertainty Relation [TR11, Tom12])

For any state ρ_{ABC}, $\varepsilon \geq 0$ and POVMs $\{M_x^\theta\}$ on A, Θ uniform:

$$H_{\min}^{\varepsilon}(X|B\Theta) + H_{\max}^{\varepsilon}(X|C\Theta) \geq \log \frac{1}{c},$$

$$c = \max_{x,y} \left\| \sqrt{M_x^0}\sqrt{M_x^1} \right\|_\infty^2,$$

$$\rho_{XBC\Theta} = \sum_{x,\theta} |e_x\rangle\langle e_x| \otimes |e_\theta\rangle\langle e_\theta| \otimes \mathrm{tr}_A\big((M_x^\theta \otimes 1_{BC})\rho_{ABC}\big).$$

- Overlap is $c = \max_{x,y} \left|\langle x^0|y^1\rangle\right|^2$ for projective measurements, where $|x^0\rangle$ is an eigenvector of M_x^0 and $|y^1\rangle$ is an eigenvector of M_x^1.
- For example, for qubit measurements in the computational and Hadamard basis: $c = \frac{1}{2}$.

Entropic Uncertainty III

- This can be lifted to n independent measurements, each chosen at random.

$$H_{\min}^{\varepsilon}(X^n|B\Theta^n) + H_{\max}^{\varepsilon}(X^n|C\Theta^n) \geq n \log \frac{1}{c}.$$

- This implies previous uncertainty relations for the von Neumann entropy [BCC$^+$10] via asymptotic equipartition.
  - For this, we apply the above relation to product states $\rho_{ABC}^n = \rho_{ABC}^{\otimes n}$.
  - Then, we divide by n and use

$$\frac{1}{n} H_{\min/\max}^{\varepsilon}(X^n|B^n\Theta^n) \xrightarrow{n\to\infty} H(X|B\Theta)\,.$$

This yields $H(X|B\Theta) + H(X|C\Theta) \geq \log \frac{1}{c}$ in the limit.

Quantum Key Distribution

An attempt to prove security on 4 slides.

(Asymptotically, and trusting our devices to some degree...)

Protocol

- We consider the entanglement-based Bennett-Brassard 1984 protocol [BBM92].
- We only do an asymptotic analysis here, a finite-key analysis based on this method can be found in [TLGR12].
- Alice produces n pairs of entangled qubits, and sends one qubit of each pair to Bob. This results in a state $\rho_{A^n B^n E}$.
- Then, Alice randomly chooses a measurement basis for each qubit, either $+$ or $\times$, and records her measurement outcomes in X^n. She sends the string of choices, Θ^n, to Bob.
- Bob, after learning Θ^n, produces an estimate $\hat{X}^n$ of X^n by measuring the n systems he received.
- Alice and Bob calculate the error rate δ on a random sample.
- Then, classical information reconciliation and privacy amplification protocols are employed to extract a shared secret key Z from the raw keys, X^n and $\hat{X}^n$.
- We are interested in the secret key rate.

Security Analysis I

- Consider the situation before Bob measures

$$\rho_{X^n B^n E} = \sum_{x^n} |x^n\rangle\langle x^n| \otimes \mathrm{tr}_{A^n}\Big(\big(\bigotimes P_{x_i}^{\theta_i} \otimes 1_{B^n E} \big) \rho_{A^n B^n E} \Big),$$

  where $P_x^\theta = H^\theta |e_x\rangle\langle e_x| H^\theta$ and H the Hadamard matrix.

- The uncertainty relation applies here,

$$H_{\min}^\varepsilon(X^n|E\Theta^n) + H_{\max}^\varepsilon(X^n|B^n\Theta^n) \geq n \log \frac{1}{c} = n.$$

- Data-Processing of the smooth max-entropy then implies

$$H_{\min}^\varepsilon(X^n|E\Theta^n) \geq n - H_{\max}^\varepsilon(X^n|\hat{X}^n),$$

  since $\hat{X}^n$ is the result of a TP CPM applied to B^n and Θ^n.

Security Analysis II

Recall: $H_{\min}^{\varepsilon}(X^n|E\Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.

- Let ε be a small constant.
- The extractable ε-secure key length is give by $\ell^{\varepsilon}(X^n|E\Theta SP)$, where S is the syndrom Alice sends to Bob for error correction and P is the information leaked due to parameter estimation.
- We ignore P for this analysis, and just note that $\log|P| = o(n)$.
- If we want information reconciliation up to probability ε, we can bound $\log|S| \leq H_{\max}^{\varepsilon}(X^n|\hat{X}^n) + O(1)$ using the operational interpretation of the smooth max-entropy.
- This ensures that

$$\begin{aligned}\ell^{\varepsilon}(X^n|E\Theta SP) &\geq H_{\min}^{\varepsilon}(X^n|E\Theta SP) + O(1)\\ &\geq H_{\min}^{\varepsilon}(X^n|E\Theta) - H_{\max}^{\varepsilon}(X^n|\hat{X}^n) + o(n)\\ &\geq n - 2H_{\max}^{\varepsilon}(X^n|\hat{X}^n) + o(n).\end{aligned}$$

Security Analysis III

Recall: $\ell^{\varepsilon}(X^n|E\Theta SP) \geq n - 2H_{\max}^{\varepsilon}(X^n|\hat{X}^n) + o(n)$.

- We have now reduced the problem of bounding Eve's information about the key to bounding the correlations between Alice and Bob.
- From the observed error rate δ, we can estimate the smooth max-entropy: $H_{\max}^{\varepsilon}(X^n|\hat{X}^n) \leq nh(\delta)$, where h is the binary entropy. (This one you just have to believe me.)
- The secret key rate thus asymptotically approaches

$$r = \lim_{n\to\infty} \frac{1}{n}\ell^{\varepsilon}(X^n|E\Theta SP) \geq n\big(1 - 2h(\delta)\big) .$$

- This recovers the results due to Mayers [May96, May02], and Shor and Preskill [SP00].

Conclusion

- The entropic approach to quantum information is very powerful, especially in cryptography.
- The smooth entropies are universal, they have many useful properties (I discussed only a small fraction of them here) and clear operational meaning.
- The smooth entropy formalism leads to an intuitive security proof for QKD, which also naturally yields finite key bounds.

Thank you for your attention.

Bibliography I

[BBM92] Charles H. Bennett, Gilles Brassard, and N. D. Mermin, *Quantum cryptography without Bells theorem*, Phys. Rev. Lett. **68** (1992), no. 5, 557–559.

[BCC+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner, *The Uncertainty Principle in the Presence of Quantum Memory*, Nat. Phys. **6** (2010), no. 9, 659–662.

[BD10] Francesco Buscemi and Nilanjana Datta, *The Quantum Capacity of Channels With Arbitrarily Correlated Noise*, IEEE Trans. on Inf. Theory **56** (2010), no. 3, 1447–1460.

[Ber08] Mario Berta, *Single-Shot Quantum State Merging*, Master's thesis, ETH Zurich, 2008.

[Col12] Patrick J. Coles, *Collapse of the quantum correlation hierarchy links entropic uncertainty to entanglement creation*.

[Dat09] Nilanjana Datta, *Min- and Max- Relative Entropies and a New Entanglement Monotone*, IEEE Trans. on Inf. Theory **55** (2009), no. 6, 2816–2826.

[DBWR10] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner, *The Decoupling Theorem*.

[dRAR+11] Lídia del Rio, Johan Aberg, Renato Renner, Oscar Dahlsten, and Vlatko Vedral, *The Thermodynamic Meaning of Negative Entropy.*, Nature **474** (2011), no. 7349, 61–3.

[DrFSS08] Ivan B. Damgå rd, Serge Fehr, Louis Salvail, and Christian Schaffner, *Cryptography in the Bounded-Quantum-Storage Model*, SIAM J. Comput. **37** (2008), no. 6, 1865.

[DRRV11] Oscar C O Dahlsten, Renato Renner, Elisabeth Rieper, and Vlatko Vedral, *Inadequacy of von Neumann Entropy for Characterizing Extractable Work*, New J. Phys. **13** (2011), no. 5, 053015.

[Dup09] Frédéric Dupuis, *The Decoupling Approach to Quantum Information Theory*, Ph.D. thesis, Université de Montréal, April 2009.

[FvdG99] C.A. Fuchs and J. van de Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Trans. on Inf. Theory **45** (1999), no. 4, 1216–1227.

Bibliography II

[KRS09] Robert König, Renato Renner, and Christian Schaffner, *The Operational Meaning of Min- and Max-Entropy*, IEEE Trans. on Inf. Theory **55** (2009), no. 9, 4337–4347.

[KWW12] Robert Konig, Stephanie Wehner, and Jürg Wullschleger, *Unconditional Security From Noisy Quantum Storage*, IEEE Trans. on Inf. Theory **58** (2012), no. 3, 1962–1984.

[May96] Dominic Mayers, *Quantum Key Distribution and String Oblivious Transfer in Noisy Channels*, Proc. CRYPTO, LNCS, vol. 1109, Springer, 1996, pp. 343–357.

[May02] ———, *Shor and Preskill's and Mayers's security proof for the BB84 quantum key distribution protocol*, Eur. Phys. J. D **18** (2002), no. 2, 161–170.

[Rén61] A. Rényi, *On Measures of Information and Entropy*, Proc. Symp. on Math., Stat. and Probability (Berkeley), University of California Press, 1961, pp. 547–561.

[Ren05] Renato Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich, December 2005.

[RK05] Renato Renner and Robert König, *Universally Composable Privacy Amplification Against Quantum Adversaries*, Proc. TCC (Cambridge, USA), LNCS, vol. 3378, 2005, pp. 407–425.

[RR12] Joseph M. Renes and Renato Renner, *One-Shot Classical Data Compression With Quantum Side Information and the Distillation of Common Randomness or Secret Keys*, IEEE Trans. on Inf. Theory **58** (2012), no. 3, 1985–1991.

[Sha48] C. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. **27** (1948), 379–423.

[SP00] Peter Shor and John Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85** (2000), no. 2, 441–444.

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner, *A Fully Quantum Asymptotic Equipartition Property*, IEEE Trans. on Inf. Theory **55** (2009), no. 12, 5840–5847.

Bibliography III

[TCR10] ———, *Duality Between Smooth Min- and Max-Entropies*, IEEE Trans. on Inf. Theory **56** (2010), no. 9, 4674–4681.

[TH12] Marco Tomamichel and Masahito Hayashi, *A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks*.

[TLGR12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner, *Tight Finite-Key Analysis for Quantum Cryptography*, Nat. Commun. **3** (2012), 634.

[Tom12] Marco Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, Ph.D. thesis, ETH Zurich, March 2012.

[TR11] Marco Tomamichel and Renato Renner, *Uncertainty Relation for Smooth Entropies*, Phys. Rev. Lett. **106** (2011), no. 11.

[Wat08] John Watrous, *Theory of Quantum Information, Lecture Notes*, 2008.

[WTHR11] Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner, *Impossibility of Growing Quantum Bit Commitments*, Phys. Rev. Lett. **107** (2011), no. 9.

[WW08] Stephanie Wehner and Jürg Wullschleger, *Composable Security in the Bounded-Quantum-Storage Model*, Proc. ICALP, LNCS, vol. 5126, Springer, July 2008, pp. 604–615.

[WW12] Severin Winkler and Jürg Wullschleger, *On the Efficiency of Classical and Quantum Secure Function Evaluation*.