Quantum Information Security

Andreas Winter
(ICREA & Universitat Autònoma de Barcelona)

Quantum Information Security

(kind of a tutorial)

Andreas Winter
(ICREA & Universitat Autònoma de Barcelona)

Outline

0. Quantum formalism

1. Motivation: quantum privacy amplification

2. Tools: (smoothed) min-entropy

3. Applications: QKD, quantum data hiding

0. Quantum formalism

We only need the "probabilistic core" of quantum theory, not the "mechanics".

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0. Quantum formalism

We only need the "probabilistic core" of quantum theory, not the "mechanics".

Non-commutative probability theory:

- States (densities)
- Transformations (channels)
- Observable probabilities (measurements & Born rule)

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0. Quantum formalism

Each quantum system characterized by a complex Hilbert space $\mathcal{H}$, A, B, C, ...
Here: dimensions $|\mathcal{H}|$, $|A|$, ... $< \infty$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0. Quantum formalism

Each quantum system characterized by a complex Hilbert space $\mathcal{H}$, A, B, C, ...
Here: dimensions $|\mathcal{H}|$, $|A|$, ... $< \infty$.

Dirac ("bra-ket") notation:

- Vectors $|\psi\rangle$
- Covectors $\langle\varphi|$
- Inner product $\langle\varphi|\psi\rangle$
- Outer product $|\psi\rangle\langle\varphi|$, in particular rank-one projector $|\psi\rangle\langle\psi|$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0. Quantum formalism

Dirac ("bra-ket") notation:

- Vectors $|\psi\rangle$
- Covectors $\langle\varphi|$
- Inner product $\langle\varphi|\psi\rangle$
- Outer product $|\psi\rangle\langle\varphi|$
- Hermitian conjugate $\dagger$:
  $|\psi\rangle^\dagger = \langle\psi|$, $\langle\varphi|^\dagger = |\varphi\rangle$
- Everything described in terms of operators $A \in L(\mathcal{H})$, $A^\dagger \in L(\mathcal{H})$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:

$\rho \geq 0$ (*positive semidefinite*), $\mathrm{Tr}\ \rho = 1$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:
$\rho \geq 0$ (*positive semidefinite*), $\mathrm{Tr}\ \rho = 1$.

States form a convex set $S(\mathcal{H})$ inside
the set $L(\mathcal{H})$ of all operators.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:
$\rho \geq 0$ (*positive semidefinite*), $\mathrm{Tr}\ \rho = 1$.

States form a convex set $S(\mathcal{H})$ inside
the set $L(\mathcal{H})$ of all operators.
(Well, it's really matrices...)

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:
$\rho \geq 0$ (positive semidefinite), $\mathrm{Tr}\ \rho = 1$.

States form a convex set $S(\mathcal{H})$ inside
the set $L(\mathcal{H})$ of all operators.

Spectral theorem: $\rho = \sum_j \lambda_j |e_j\rangle\langle e_j|$,
with ONB $|e_j\rangle$ and $\lambda_j \geq 0$ summing to 1.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:
$\rho \geq 0$ (*positive semidefinite*), $\mathrm{Tr}\ \rho = 1$.

States form a convex set $S(\mathcal{H})$ inside
the set $L(\mathcal{H})$ of all operators.

Spectral theorem: $\rho = \sum_j \lambda_j |e_j\rangle\langle e_j|$,
with ONB $|e_j\rangle$ and $\lambda_j \geq 0$ summing to 1.

Extremal points: rank-one projectors
$|\psi\rangle\langle\psi|$ – *pure states*.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-a. States

States on $\mathcal{H}$ are *density operators*:
$\rho \geq 0$ (positive semidefinite), $\mathrm{Tr}\ \rho = 1$.

States form a convex set $S(\mathcal{H})$ inside the set $L(\mathcal{H})$ of all operators.

With a distinguished ONB $|x\rangle$ ("computational basis"), have diagonal matrices $\rho = \sum_x p_x |x\rangle\langle x|$, isomorphic to the probability simplex.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-6. Measurement

Observations on quantum systems require an observable, which is a resolution of the identity (aka POVM):

$M_y \geq 0$, with $\sum_y M_y = 1$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-6. Measurement

Observations on quantum systems require an *observable*, which is a resolution of the identity (aka *POVM*):

$M_y \geq 0$, with $\sum_y M_y = 1$.

Born rule: $\Pr\{y|\rho\} = \mathrm{Tr}\, \rho M_y$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-6. Measurement

Observations on quantum systems require an *observable*, which is a resolution of the identity (aka *POVM*):

$M_y \geq 0$, with $\sum_y M_y = 1$.

Born rule: $\Pr\{y|\rho\} = \mathrm{Tr}\, \rho M_y$

State as the "catalog of expectations" (Schrödinger)

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-b. Measurement

Example: Discriminating equiprobable hypotheses ρ and σ. Need a binary POVM $(M, 1-M)$, with $0 \leq M \leq 1$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-b. Measurement

Example: Discriminating equiprobable hypotheses ρ and σ. Need a binary POVM $(M, 1-M)$, with $0 \le M \le 1$.

Want to maximize success probability

$$Pr\{succ\} = \frac{1}{2} Tr\, \rho M + \frac{1}{2} Tr\, \sigma(1-M)$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-b. Measurement

Example: Discriminating equiprobable hypotheses ρ and σ. Need a binary POVM $(M, 1-M)$, with $0 \le M \le 1$.

Want to maximize success probability

$$\Pr\{\text{succ}\} = \frac{1}{2} \operatorname{Tr} \rho M + \frac{1}{2} \operatorname{Tr} \sigma (1-M)$$

$$= \frac{1}{2} + \frac{1}{2} \operatorname{Tr} (\rho - \sigma) M$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-b. Measurement

Example: Discriminating equiprobable hypotheses ρ and σ. Need a binary POVM $(M, 1-M)$, with $0 \le M \le 1$.

Want to maximize success probability

$$\Pr\{\text{succ}\} = \frac{1}{2}\,\mathrm{Tr}\,\rho M + \frac{1}{2}\,\mathrm{Tr}\,\sigma(1-M)$$

$$= \frac{1}{2} + \frac{1}{4}\,\mathrm{Tr}\,(\rho-\sigma)(2M-1)$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-b. Measurement

Example: Discriminating equiprobable hypotheses ρ and σ. Need a binary POVM $(M, 1-M)$, with $0 \le M \le 1$.

Want to maximize success probability

$$\Pr\{\text{succ}\} = \frac{1}{2}\,\mathrm{Tr}\,\rho M + \frac{1}{2}\,\mathrm{Tr}\,\sigma(1-M)$$

$$= \frac{1}{2} + \frac{1}{4}\,\underbrace{\mathrm{Tr}\,(\rho-\sigma)(2M-1)}$$

$$\max = \|\rho-\sigma\|_1 \quad \text{(trace norm)}$$

$$= \mathrm{Tr}\,|\rho-\sigma|$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

$L(A \otimes B) = L(A) \otimes L(B)$ as vector spaces.

$L(A) \simeq L(A) \otimes I \subset L(A \otimes B)$, same for B.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

$L(A \otimes B) = L(A) \otimes L(B)$ as vector spaces.

$L(A) \simeq L(A) \otimes I \subset L(A \otimes B)$, same for B.

The latter allows us to identify a POVM (M_y) on A with $(M_y \otimes 1)$ on $A \otimes B$. And for (N_z) on B, joint POVM $(M_y \otimes N_z)$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

Where does that leave us with the states?

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

Where does that leave us with the states?

$S(A \otimes B)$ clearly contains all tensor product densities $\alpha \otimes \beta$ and their convex hull, but it has so much more...

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

Where does that leave us with the states?

$S(A \otimes B)$ clearly contains all tensor product densities $\alpha \otimes \beta$ and their convex hull, but it has so much more...

Entanglement! For instance all pure states $|\psi\rangle\langle\psi|$ with $|\psi\rangle \neq |\alpha\rangle \otimes |\beta\rangle$.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Composition of A and B (Hilbert spaces) is a system with tensor product Hilbert space $A \otimes B$.

Marginals: For a state $\rho^{AB} \in S(A \otimes B)$, the rule

$$\mathrm{Tr}\ \rho(X \otimes 1) = \mathrm{Tr}\ \rho^A X \qquad \text{(for all } X\text{)}$$

singles out uniquely the partial trace:

$$\rho^A = \mathrm{Tr}_B\, \rho^{AB}.$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-c. Composite systems

Purification: For every state $\rho \in S(A)$, there exists a unit vector $|\varphi\rangle \in A \otimes A'$, s.t. ρ is the marginal of the pure state:

$$\rho^A = Tr_{A'} |\varphi\rangle\langle\varphi|.$$

Any other pure state $|\psi\rangle\langle\psi|$ with this property is related to $|\varphi\rangle\langle\varphi|$ by a unitary conjugation on A':

$$|\psi\rangle = (1 \otimes U)|\varphi\rangle.$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Like classical channels, quantum channels map densities to densities, i.e.

$$N: S(A) \longrightarrow S(B).$$

As it must respect convex combinations, extends uniquely a *linear, positive, trace preserving* map $N: L(A) \longrightarrow L(B)$.

However, want *complete positivity*, i.e.

$$N \otimes id_C : S(A \otimes C) \longrightarrow S(B \otimes C)$$

should be positive for all auxiliary C.

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Quantum channel

$$\mathcal{N}: L(A) \longrightarrow L(B)$$

is a *linear, completely positive and trace preserving (cptp) map.*

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Quantum channel

$$\mathcal{N}: L(A) \longrightarrow L(B)$$

is a *linear, completely positive and trace preserving (cptp) map.*

Basic example: unitary conjugation on A

$$\mathcal{N}(\rho) = U \rho U^{\dagger}.$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Quantum channel

$$\mathcal{N}: L(A) \longrightarrow L(B)$$

is a *linear, completely positive and trace preserving (cptp) map.*

Basic example: unitary conjugation on A

$$\mathcal{N}(\rho) = U \rho U^{\dagger}.$$

Another one: partial trace from AB to A

$$\mathcal{N}(\rho) = Tr_B \rho.$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

More examples:

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 $\epsilon_q(\rho)=(1-q)\rho \oplus q|*\rangle\langle *|$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

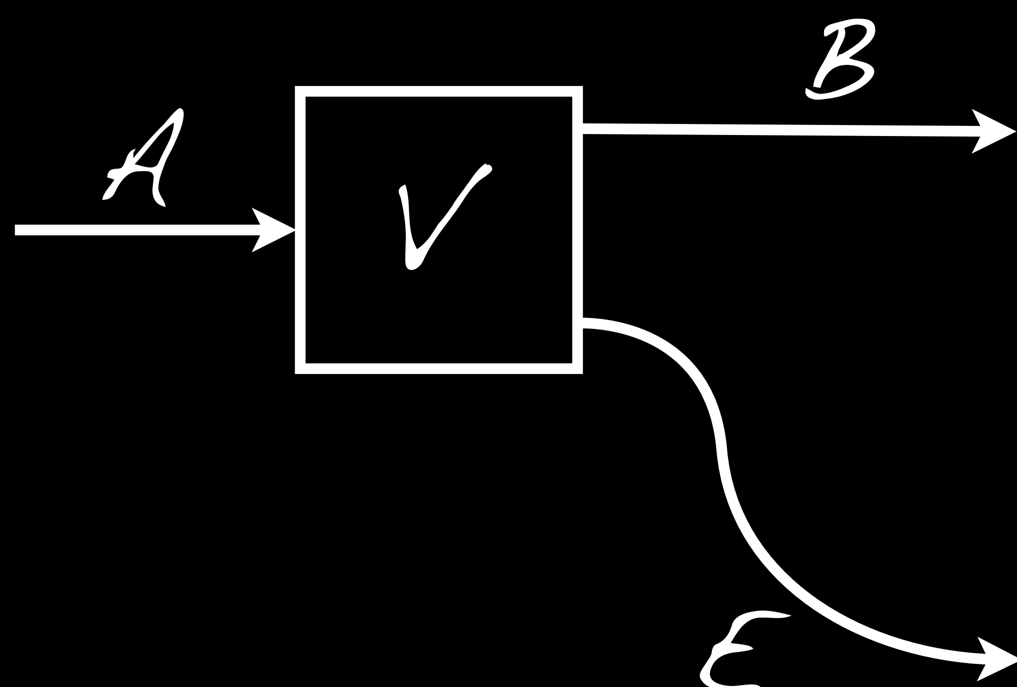
Stinespring: $\mathcal{N}(\rho) = \mathrm{Tr}_E\, V \rho V^\dagger$,

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

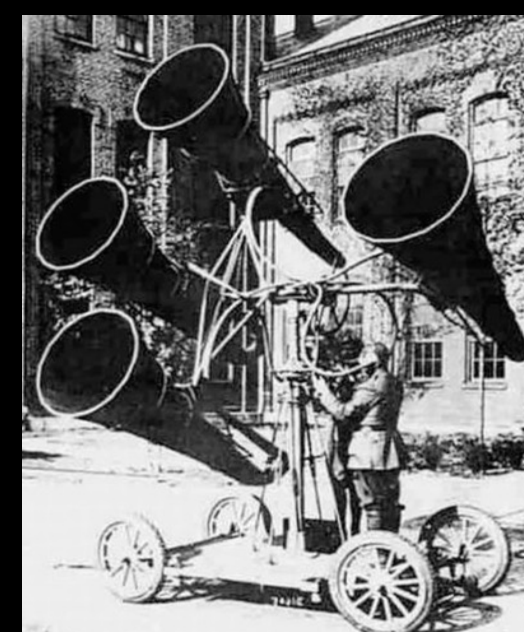
Complementary channel:

$$\widehat{\mathcal{N}}(\rho) = \mathrm{Tr}_B\, V \rho V^\dagger.$$

Alice



Bob

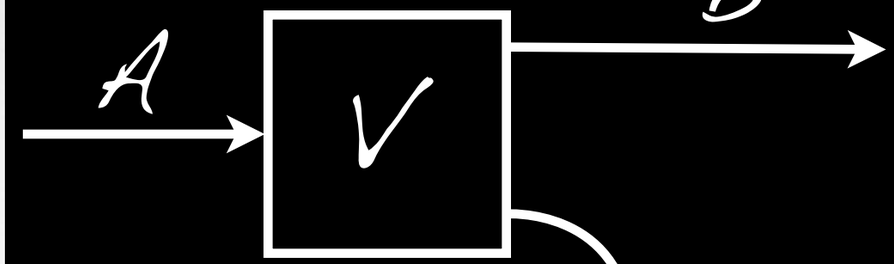


Eve

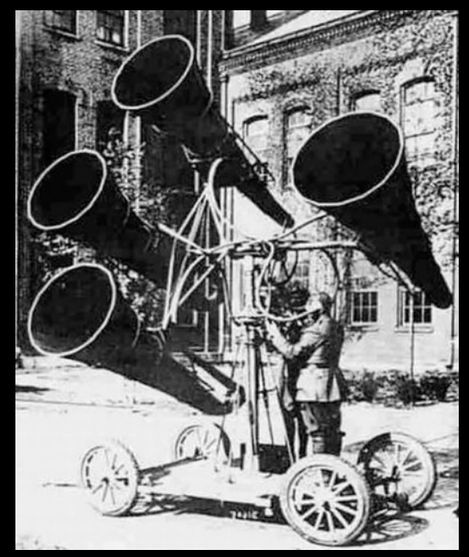
[M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Alice



Bob



Eve

It's a wiretap model! Note that automatically if Bob's channel is (nearly) noiseless, Eve's is (nearly) constant.

[Kretschmann et al., IEEE-IT 2008]

0-d. Quantum channels

Important property of cptp maps: trace norm is contractive. I.e., for any channel $\mathcal{N}$ and any operator ξ,

$$\|\mathcal{N}(\xi)\|_1 \leq \|\xi\|_1 .$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

0-d. Quantum channels

Important property of cptp maps: trace norm is contractive. I.e., for any channel $\mathcal{N}$ and any operator ξ,

$$\|\mathcal{N}(\xi)\|_1 \leq \|\xi\|_1 .$$

Other metrics with this property, e.g. the *purified distance*

$$P(\rho,\sigma) = \min \tfrac{1}{2} \|\varphi-\psi\|_1 \text{ s.t. purifications } \varphi, \psi \text{ of } \rho, \sigma$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

1. Privacy amplification

Alice has a "raw key" X (maybe shared with Bob), which is compromised: conditional on side information of Eve, the distribution of X is not uniform.

1. Privacy amplification

Alice has a "raw key" X (maybe shared with Bob), which is compromised: conditional on side information of Eve, the distribution of X is not uniform.

But if we know $-\log \Pr\{X=x\} \geq h$, then 2-universal hash-function F to k bits yields Y=F(X) with

$$\| P_{YF} - U \otimes P_F \|_1 \leq 2^{-(h-k)/2},$$

where U is the uniform distribution.

1. Privacy amplification

Including Eve explicitly, have Alice's X and Eve's Z jointly distributed. The optimal h is

$$H_{min}(X|Z) = -\log \max_{x,z} \Pr\{X=x|Z=z\}$$

I. Privacy amplification

Including Eve explicitly, have Alice's X and Eve's Z jointly distributed. The optimal h is

$$H_{min}(X|Z) = -\log \max_{x,z} Pr\{X=x|Z=z\}$$

What can we do if Eve has quantum information? What can that conditional probability mean?

[Cf. R. Renner, PhD thesis, arXiv:quant-ph/0512258]

I. Privacy amplification

Now Alice and Eve have a joint state:

$$\rho^{XE} = \sum_x p_x |x\rangle\langle x|^X \otimes \rho_x^E.$$

[Cf. R. Renner, PhD thesis, arXiv:quant-ph/0512258]

I. Privacy amplification

Now Alice and Eve have a joint state:

$$\rho^{XE} = \sum_x p_x |x\rangle\langle x|^X \otimes \rho_x^E.$$

It turns out the right definition is about comparing with operators $\lambda(1\otimes\sigma)$:

$$H_{min}(X|E) = -\log \min_{\lambda,\sigma} \lambda \text{ s.t. } \rho \le \lambda(1\otimes\sigma),$$

where σ is a state on E and λ is real.

[Cf. R. Renner, PhD thesis, arXiv:quant-ph/0512258]

1. Privacy amplification

Let $H_{min}(X|E) = -\log \min_{\lambda,\sigma} \lambda$ s.t. $\rho \le \lambda(1 \otimes \sigma) \ge h$.

Then 2-universal hash-function F to k bits yields $Y=F(X)$ with

$$\| \rho^{YFE} - U \otimes \rho_F \otimes \rho^E \|_1 \le 2^{-(h-k)/2},$$

where U is the uniform distribution (maximally mixed state).

[Cf. R. Renner, PhD thesis, arXiv:quant-ph/0512258]

1. Privacy amplification

Let $H_{min}(X|E) = -\log \min_{\lambda,\sigma} \lambda$ s.t. $\rho \le \lambda(1 \otimes \sigma) \ge h$.

Then 2-universal hash-function F to k bits yields $Y=F(X)$ with

$$\| \rho^{YFE} - U \otimes \rho_F \otimes \rho^E \|_1 \le 2^{-(h-k)/2},$$

where U is the uniform distribution (maximally mixed state).

...essentially optimal without knowing more about the joint state.

[Cf. R. Renner, PhD thesis, arXiv:quant-ph/0512258]

2. Min-entropy calculus

Renner found that one could develop a meaningful one-shot information calculus based on conditional min-entropy:

$$H_{min}(A|B)_\rho = -\log \min_{\lambda,\sigma} \lambda \text{ s.t. } \rho^{AB} \leq \lambda(1^A \otimes \sigma^B),$$

for an arbitrary state ρ on $A \otimes B$.

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

Renner found that one could develop a meaningful one-shot information calculus based on conditional min-entropy:

$$H_{min}(A|B)_\rho = -\log \min_{\lambda,\sigma} \lambda \text{ s.t. } \rho^{AB} \leq \lambda(1^A \otimes \sigma^B),$$

for an arbitrary state ρ on $A \otimes B$. Not only is this a semidefinite programme (SDP), as we shall see it shares many good properties with the von Neumann entropy.

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

[Entropy digression:

The von Neumann entropy of a state ρ is $S(\rho) = -Tr\ \rho \log \rho = H(\vec{\lambda})$, where $\vec{\lambda}$ is the eigenvalue vector of ρ.

We define information expressions by linear-combining entropies, à la Shannon:
E.g. $S(A|B)_\rho = S(\rho^{AB}) - S(\rho^{B})$, or conditional mutual information

$$I(A:B|C)_\rho = S(\rho^{AB}) + S(\rho^{BC}) - S(\rho^{ABC}) - S(\rho^{C}).$$

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

[Entropy digression:

While the quantum conditional entropy $S(A|B)_\rho = S(\rho^{AB}) - S(\rho^B)$ can be negative, the conditional mutual information

$$I(A:B|C)_\rho = S(\rho^{AB}) + S(\rho^{BC}) - S(\rho^{ABC}) - S(\rho^C)$$

is always ≥ 0; this is Lieb-Ruskai's strong subadditivity...

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

[Entropy digression:

While the quantum conditional entropy $S(A|B)_\rho = S(\rho^{AB}) - S(\rho^B)$ can be negative, the conditional mutual information

$$I(A:B|C)_\rho = S(\rho^{AB}) + S(\rho^{BC}) - S(\rho^{ABC}) - S(\rho^C)$$

is always ≥ 0; this is Lieb-Ruskai's strong subadditivity...]

[See (e.g.) M. M. Wilde, QIT, Cambridge University Press]

2. Min-entropy calculus

Conditional (smooth) min-entropy:

$$H_{min}(A|B)_\rho = -\log \min_{\lambda,\sigma} \mathrm{Tr}\, S \text{ s.t. } \rho^{AB} \leq 1^A \otimes S^B$$

In the applications (privacy amplification, ...) we can gain by "smoothing":

$$H^\varepsilon_{min}(A|B)_\rho = \max H_{min}(A|B)_\omega \text{ s.t. } P(\rho,\omega)\leq\varepsilon$$

Amazingly, also this is an SDP! Useful due to SDP duality (...)

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

Motivated by the von Neumann entropy identity $S(A|B) = -S(A|C)$ for a pure state on ABC, we define also a

conditional (smooth) max-entropy:

$$H_{max}^{\varepsilon}(A|B)_\rho = -H_{min}^{\varepsilon}(A|C)_\varphi \text{ w.r.t. purification } \varphi$$

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

Motivated by the von Neumann entropy identity $S(A|B) = -S(A|C)$ for a pure state on ABC, we define also a conditional (smooth) max-entropy:

$$H_{max}^{\varepsilon}(A|B)_\rho = -H_{min}^{\varepsilon}(A|C)_\varphi \quad \text{w.r.t. purification } \varphi$$

As in the classical case, "min" applies to extraction problems, while "max" to compression problems...

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

These quantities share many features with the von Neumann entropy, e.g. strong subadditivity reads $S(AIBC) \leq S(AIB)$:

$$H_{min}^{\varepsilon}(AIBC)_\rho \leq H_{min}^{\varepsilon}(AIB)_\rho ;$$

$$H_{max}^{\varepsilon}(AIBC)_\rho \leq H_{max}^{\varepsilon}(AIB)_\rho .$$

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

$$H_{min}^{\varepsilon}(A|BC)_\rho \leq H_{min}^{\varepsilon}(A|B)_\rho;$$

$$H_{max}^{\varepsilon}(A|BC)_\rho \leq H_{max}^{\varepsilon}(A|B)_\rho.$$

Furthermore, while H_{min}^{ε} increases and H_{max}^{ε} decreases with ε, we have for suff. small ε and δ,

$$H_{min}^{\varepsilon}(A|B)_\rho \leq H_{max}^{\delta}(A|B)_\rho + O(1).$$

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

2. Min-entropy calculus

Using properties of typical subspaces, one can also show the "quantum AEP": For n-tensor power states $\rho^{\otimes n}$ on A^nB^n, and $0<\varepsilon<1$,

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

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

[R. Renner, PhD thesis, arXiv:quant-ph/0512258;
M. Tomamichel, PhD thesis, arXiv:1203.2142]

3. Applications: QKD, ...

The min-entropy formalism was initially devised to give unified and optimized security proofs of QKD protocols.

[R. Renner, PhD thesis, arXiv:quant-ph/0512258]

3. Applications: QKD, ...

The min-entropy formalism was initially devised to give unified and optimized security proofs of QKD protocols.

[R. Renner, PhD thesis, arXiv:quant-ph/0512258]

Since then it was used in condensed matter physics [Area laws, Brandão/Horodecki] and for strong converses [talk by Ciara Morgan].

3'. LOCC hiding efficiency

Recall the state discrimination problem, but now let ρ and σ be states on a composite system: $\mathcal{H} = A \otimes B$, and let A (Alice) and B (Bob) be far apart.

Without a quantum channel between them, they can only perform *local operations and classical communication* (LOCC).

[Walgate et al., PRL85:4972-4975, 2000]
[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

[Walgate et al., PRL85:4972-4975, 2000]
[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

[Walgate et al., PRL85:4972-4975, 2000]
[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

ddm

[Walgate et al., PRL85:4972-4975, 2000]

[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

ddm

llap

[Walgate et al., PRL85:4972-4975, 2000]

[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

ddm

llap

guess

[Walgate et al., PRL85:4972-4975, 2000]

[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

ddm

llap

guess

$$\max P\{\text{guess}\} =: \frac{1}{2} + \frac{1}{4}\,\|\rho-\sigma\|_{LOCC}$$

[Walgate et al., PRL85:4972-4975, 2000]
[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

ρ or σ

abc

ddm

llap

guess

$$\max P\{\text{guess}\} =: \frac{1}{2} + \frac{1}{4}\,\|\rho-\sigma\|_{LOCC}$$

Can be much smaller than $\|\rho-\sigma\|_1$: data hiding!

[Terhal/DiVincenzo/Leung, PRL86:5807-5810, 2001]

3'. LOCC hiding efficiency

Let ρ_x be states on a composite system $\mathcal{H} = A \otimes B$, with the systems of Alice and Bob having dimensions $|A|=|B|=d$ ($x=1...M$), such that any pair of states is LOCC-hiding, but that there is a global POVM revealing x among all M.

3'. LOCC hiding efficiency

Let ρ_x be states on a composite system $\mathcal{H} = A \otimes B$, with the systems of Alice and Bob having dimensions $|A| = |B| = d$ ($x = 1 \ldots M$), such that any pair of states is LOCC-hiding, but that there is a global POVM revealing x among all M.

How large can M be in relation to d?

3'. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/AW, CMP 250:371-391, 2004]:

Random states in dxd of rank

$r = d\,\mathrm{polylog}(d)$ are hiding states.

Can distinguish $M = d/\mathrm{polylog}(d)$ many of them.

3'. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/AW, CMP 250:371-391, 2004]:

Random states in dxd of rank

$r = d\,\mathrm{polylog}(d)$ are hiding states.

Can distinguish $M = d/\mathrm{polylog}(d)$ many of them.

Information $\log M \sim \log d$ = local share.

3'. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/AW, CMP 250:371-391, 2004]:

Random states in dxd of rank

$r = d\,\mathrm{polylog}(d)$ are hiding states.

Can distinguish $M = d/\mathrm{polylog}(d)$ many of them.

Information $\log M \sim \log d$ = local share.

Can we have more?

3'. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/AW, CMP 250:371-391, 2004]:

Random states in dxd of rank

$r = d\,\mathrm{polylog}(d)$ are hiding states.

Can distinguish $M = d/\mathrm{polylog}(d)$ many of them.

Information $\log M \sim \log d$ = local share.

Can we have more? NO!

[AW, in preparation, 2014-2015]

3'. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 19791; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.

3'. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 19791; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret. Attained for (n,t) threshold schemes of t out of n parties.

3'. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 19791; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret. Attained for (n,t) threshold schemes of t out of n parties.
Here "(2,2)" - note that LOCC data hiding cannot be perfect (re secrecy).

Formal statement: If $\varepsilon, \delta > 0$ are small enough, s.t. $\|\rho_x - \rho_y\|_{LOCC} \leq \delta$ for all x, y, and $\mathrm{Tr}\rho_x D_x \geq 1-\varepsilon$ for a POVM (D_x).

Formal statement: If $\varepsilon,\delta>0$ are small enough, s.t. $\|\rho_x-\rho_y\|_{LOCC}\leq\delta$ for all x,y, and $\mathrm{Tr}\rho_x D_x\geq 1-\varepsilon$ for a POVM (D_x).

Then: μ, $C>0$ (dep. only on ε,δ) with

$$\log(M-1)\leq H_{max}^{\mu}(A|B)_\Omega+C\leq\log d+O(1),$$

w.r.t. uniform average state Ω of the ρ_x.

Formal statement: If $\varepsilon,\delta>0$ are small enough, s.t. $\|\rho_x-\rho_y\|_{LOCC}\leq\delta$ for all x,y, and $\mathrm{Tr}\rho_x D_x\geq 1-\varepsilon$ for a POVM (D_x).

Then: μ, $C>0$ (dep. only on ε,δ) with

$$\log(M-1)\leq H_{max}^{\mu}(A|B)_\Omega+C\leq\log d+O(1),$$

w.r.t. uniform average state Ω of the ρ_x.

Proof uses the full power of the min-/max-entropy calculus (...)

Proof uses the full power of the min-/max-entropy calculus: chain rules!

Recall entropy chain rule identity

$S(ABIC) = S(AIC) + S(BIAC)$.

Proof uses the full power of the min-/max-entropy calculus: chain rules!

Recall entropy chain rule identity $S(ABIC) = S(AIC)+S(BIAC)$. Turns into inequalities for min-/max-entropies:

$$H_{\min}^{\varepsilon+2\varepsilon'+\varepsilon''}(AB|C)_\rho \geq H_{\min}^{\varepsilon'}(A|BC)_\rho + H_{\min}^{\varepsilon''}(B|C)_\rho - \log\frac{2}{\varepsilon^2}, \quad (5.11)$$

$$H_{\max}^{\varepsilon+\varepsilon'+2\varepsilon''}(AB|C)_\rho \leq H_{\max}^{\varepsilon'}(A|BC)_\rho + H_{\max}^{\varepsilon''}(B|C)_\rho + \log\frac{2}{\varepsilon^2}, \quad (5.12)$$

$$H_{\min}^{\varepsilon+3\varepsilon'+2\varepsilon''}(A|BC)_\rho \geq H_{\min}^{\varepsilon'}(AB|C)_\rho - H_{\max}^{\varepsilon''}(B|C)_\rho - 2\log\frac{2}{\varepsilon^2}, \quad (5.13)$$

$$H_{\max}^{2\varepsilon+\varepsilon'+2\varepsilon''}(A|BC)_\rho \leq H_{\max}^{\varepsilon'}(AB|C)_\rho - H_{\min}^{\varepsilon''}(B|C)_\rho + 3\log\frac{2}{\varepsilon^2}, \quad (5.14)$$

$$H_{\min}^{2\varepsilon+\varepsilon'+2\varepsilon''}(B|C)_\rho \geq H_{\min}^{\varepsilon'}(AB|C)_\rho - H_{\max}^{\varepsilon''}(A|BC)_\rho - 3\log\frac{2}{\varepsilon^2}, \quad (5.15)$$

$$H_{\max}^{\varepsilon+3\varepsilon'+2\varepsilon''}(B|C)_\rho \leq H_{\max}^{\varepsilon'}(AB|C)_\rho - H_{\min}^{\varepsilon''}(A|BC)_\rho + 2\log\frac{2}{\varepsilon^2}. \quad (5.16)$$

[A. Vitanov, MSc thesis 2011, cf. 1203.21442]

Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x\rangle\langle x|^X \otimes \rho_x^{AB}$. Then:

$$\log(M-1) \leq H_{min}^{\sqrt{\delta}}(X|B)$$

{Local shares give little information}

Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x\rangle\langle x|^X \otimes \rho_x^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$

{Local shares give little information}

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{Y}(A|BX) + O(1)$$

{Otherwise "merging attack" breaks scheme}

Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x\rangle\langle x|^X \otimes \rho_x^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$ {Local shares give little information}

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1)$$ {Otherwise "merging attack" breaks scheme}

$$\leq H_{\max}^{\eta}(AX|B) + O(1)$$ {One of the chain rules}

Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x\rangle\langle x|^X \otimes \rho_x^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$

{Local shares give little information}

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1)$$

{Otherwise "merging attack" breaks scheme}

$$\leq H_{\max}^{\eta}(AX|B) + O(1)$$

{One of the chain rules}

$$\leq H_{\max}^{\mu}(A|B) + H_{\max}^{\lambda}(X|AB) + O(1)$$

{Another chain rule}

Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x\rangle\langle x|^X \otimes \rho_x^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$

{Local shares give little information}

{Otherwise "merging attack" breaks scheme}

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1)$$

$$\leq H_{\max}^{\eta}(AX|B) + O(1)$$ {One of the chain rules}

$$\leq H_{\max}^{\mu}(A|B) + H_{\max}^{\lambda}(X|AB) + O(1)$$ {Another chain rule}

$$\leq H_{\max}^{\mu}(A|B) + O(1)$$ {Decodability}

QED

Compare secret sharing [A. Shamir, 19791; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.

Corollary: In any tight LOCC data hiding scheme, each relevant share must be at least as large as the secret (plus a constant). Attained for "(n,t)" scheme.

[AW, in prep.; Hayden/Leung/Smith, PRA 71:062339, 2005]

Thank you for your attention