Private Quantum Decoupling

Francesco Buscemi[1]

3rd Intl. Conference on Quantum Foundations (ICQF-17)
Hotel Panache, Patna, 7 December 2017

[1]Dept. of Mathematical Informatics, Nagoya University, buscemi@i.nagoya-u.ac.jp

worried about data remanence?

go on shoot your hard-drive!

What the Principles Tell Us

- the input is a quantum system Q
- the hiding process is a CPTP map $\mathcal{E} : Q \to Q'$
- the output is also a quantum system Q'
- the eavesdropper holds the environment E purifying ($\to$ Appendix) the hiding process $\mathcal{E}$

Perfect Hiding

Ideal objective: the initial information, after the erasure process, is neither in Q' nor in E.

Question: is this possible?

No, It's Not Possible

No-Hiding Theorem (Braunstein, Pati, 2007)

- input: an unknown quantum state $|\psi\rangle \in \mathcal{H}_Q$
- assumption: perfect erasure, i.e., the output $\mathcal{E}(|\psi\rangle\langle\psi|)$ does not depend on $|\psi\rangle$
- conclusion: no-hiding, i.e., the initial state $|\psi\rangle$ can be found intact in the environment E

Interpretation. Perfect hiding of quantum information is impossible, that is, quantum information is preserved: it can only be moved to the environment (i.e., handed over to the eavesdropper)

Yes, It Is Possible

- **input**: an unknown state $|\psi^i\rangle$ chosen from a set of orthogonal states
- **hiding process**: measurement on the Fourier transform basis $|\tilde{\psi}^j\rangle$, i.e., $|\langle\tilde{\psi}^j|\psi^i\rangle|^2 = \frac{1}{d}$
- the corresponding **Stinespring-Kraus dilation** is given by

$$|\psi^i_Q\rangle \longmapsto \underbrace{\sum_j |\tilde{\psi}^j_{Q'}\rangle|\tilde{\psi}^j_E\rangle\langle\tilde{\psi}^j_Q|}_{\text{isometry } V_{Q\to Q'E}}|\psi^i_Q\rangle = \underbrace{|\mathcal{B}^i_{Q'E}\rangle}_{\text{max. ent.}},$$

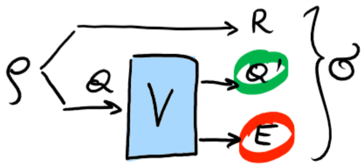
- perfect hiding has been achieved in this case

Motivation of This Talk

- whether perfect hiding can be achieved or not, depends on the "form" of the set of input states used to encode information
- tantalizing idea: quantum information (the first example) cannot be hidden, while classical information (the second example) can; to what extent is this true?
- problem: to find a framework able to handle general families of input states

Private Quantum Decoupling

The Extended Setting



- **input**: instead of a family of states of Q, one bipartite state ρ_{RQ}, shared with a reference R
- **hiding process**: an isometry V splitting the input system Q into **output** Q' and **junk** E
- **ideal goal (perfect hiding)**: $\sigma_{RQ'} = \sigma_R \otimes \sigma_{Q'}$ (perfect decoupling) and $\sigma_{RE} = \sigma_R \otimes \sigma_E$ (perfect privacy)

The Quantum Mutual Information

- define $I(X;Y) \triangleq H(X) + H(Y) - H(XY)$
- $0 \leq I(X;Y) \leq 2H(X)$
- $I(X;Y) \geq \frac{1}{2\ln 2} \|\rho_{XY} - \rho_X \otimes \rho_Y\|_1^2$

Ideal Hiding (Reformulation)

Given an input bipartite state ρ_{RQ}, find an isometry V, taking Q into $Q'E$, such that

$$\underbrace{I(R;Q') = 0}_{\text{decoupling}} \quad \text{and} \quad \underbrace{I(R;E) = 0}_{\text{privacy}} .$$

Optimal Hiding of Correlations

Since ideal hiding is in general impossible, we consider a relaxation of the problem:

Optimal Hiding

Given an input bipartite state ρ_{RQ}, its **non-hidable or "intrinsic" correlations** are defined by

$$\xi(\rho_{RQ}) \triangleq \inf_{V:Q\to Q'E} \Big\{ I(R;Q') + I(R;E) \Big\}$$

Remark. Perfect hiding for ρ_{RQ} is possible if and only if $\xi(\rho_{RQ}) = 0$.

No-Hiding Theorem and QMI

The No-Hiding Theorem can be reformulated in terms of QMI.

- consider an initial bipartite pure state $|\Psi_{RQ}\rangle$
- *any* isometry on Q will output a tripartite pure state $|\tilde{\Psi}_{RQ'E}\rangle$
- in this case, the balance relation identically holds

$$\xi(\rho_{RQ}) \triangleq I(R;Q') + I(R;E) = I(R;Q)$$

No-Hiding (reform.): in the pure state case, all correlations are intrinsic, i.e., decoupling and privacy are mutually excluding requirements.

General Bound

Theorem

For any ρ_{RQ}, we have

$$\xi(\rho_{RQ}) \geq 2I_c(Q\rangle R) \ ,$$

where $I_c(Q\rangle R) \triangleq H(R) - H(RQ)$ is the *coherent information*.

Proof.

- purify: $\rho_{RQ} \to |\Phi_{R'RQ}\rangle$
- apply isometric splitting: $|\Phi_{R'RQ}\rangle \to |\tilde{\Phi}_{R'RQ'E}\rangle$
- by entropic calculus, we have $I(R;Q') \geq I_c(Q\rangle R) + H(Q') - H(E)$ and $I(R;E) \geq I_c(Q\rangle R) + H(E) - H(Q')$
- hence, for any splitting, $I(R;Q') + I(R;E) \geq 2I_c(Q\rangle R)$

Some Comments

- for pure states, $I(R;Q) = I_c(Q\rangle R) = H(Q)$, hence $\frac{1}{2}\xi(\rho_{RQ})$ equals the entropy of entanglement; in general, however, it is not an entanglement measure
- it is nonetheless a good entanglement parameter, in the sense that

$$\frac{1}{2}\xi(\rho_{RQ}) \to H(Q) \iff I_c(Q\rangle R) \to H(Q)$$

- it satisfies monogamy, that is, for any tripartite pure state $|\Psi_{RAB}\rangle$, $\frac{1}{2}\xi(\rho_{RA}) + \frac{1}{2}\xi(\rho_{RB}) \leq H(R)$

The Asymptotic Scenario

As it is customary in information theory, we consider

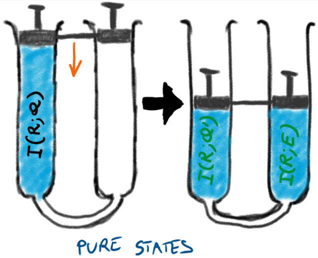
$$\xi^{\infty}(\rho_{RQ}) \triangleq \lim_{n\to\infty} \frac{1}{n}\xi(\rho_{RQ}^{\otimes n}) .$$

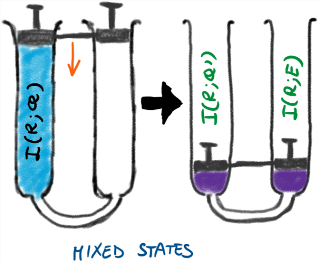
Remark. The splitting isometry is in general entangled, that is, $Q^{\otimes n} \to Q'_n E_n \neq (Q'E)^{\otimes n}$.

Theorem (Asymptotic Erasure)

For any initial state ρ_{RQ}, $\xi^{\infty}(\rho_{RQ}) = 2I_c(Q\rangle R)$.

An Attempt at Visualizing





$$I(R;Q') + I(R;E) = I(R;Q)$$

$$I(R;Q') + I(R;E) = 2I_c(Q\rangle R)$$

Hence:

- **intrinsic (non-hidable) correlations**: $2I_c(Q\rangle R) \ll I(R;Q)$
- **pure-state correlations are all intrinsic**: $2I_c(Q\rangle R) = I(R;Q)$
- **separable-state correlations are all extrinsic**: $2I_c(Q\rangle R) = 0$

The Role of Randomness

With free private randomness, private quantum decoupling becomes trivial.

- **private randomness**: a max. mixed state $\omega_P = \frac{1}{d_P} I_P$ that we can trust to be independent of Eve
- **hiding process**: an isometry $V : QP \to Q'E$
- **output state**: $\sigma_{RQ'E} = (I_R \otimes V_{QP})(\rho_{RQ} \otimes \omega_P)(I_R \otimes V_{QP}^\dagger)$

Example

Since $\frac{1}{4} \sum_i \sigma_i \rho \sigma_i = \frac{1}{2} I_2$ for any initial qubit state ρ, the state $\omega_P = \frac{1}{4} I_4$ and the isometry $V : QP \to Q'E$, given by $V = \sum_i \sigma_i^{Q \to Q'} \otimes |i_E\rangle\langle i_P|$, are enough to perfectly hide any two-qubit correlation.

Summary

- pure-state correlations cannot be hidden:

$$I(R;Q') + I(R;E) = I(R;Q)$$

- however, in general:

$$I(R;Q') + I(R;E) = 2I_c(Q\rangle R) \ll I(R;Q)$$

- **private randomness** enables perfect hiding
- connections with other protocols in QIT? e.g., randomness extraction, private key distribution, etc.
- connections with foundations? e.g., Landauer's principle, uncertainty relations, quantumness of correlations, etc.

Thank you

Appendix: The Stinespring-Kraus Dilation

- consider an input/output quantum process (CPTP map) $\mathcal{E}$, mapping density matrices on $\mathcal{H}_Q$ to density matrices on $\mathcal{H}_{Q'}$
- **Kraus operator-sum representation**: $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$
- **Kraus-Stinespring dilation**: each CPTP map $\mathcal{E}$ can be written as $\mathcal{E}(\rho) = \mathrm{Tr}_E[V \rho V^\dagger]$ (Stinespring) or $\mathcal{E}(\rho) = \mathrm{Tr}_E[U(\rho_Q \otimes |0\rangle\langle 0|_{E_0})U^\dagger]$ (Kraus)
- in quantum crypto-analyses, the subsystem E is the eavesdropper's