

CQC

Composing Quantum Channels

Start date: 1/7/2011

Michael M. Wolf ¹

Matthias Christandl ²

David Perez-Garcia ³

Presenter: David Perez-Garcia ³

¹Technical University of Munich (*TUM*)

²ETH Zurich (*ETH*) and University of Copenhagen

³Universidad Complutense de Madrid (*UCM*)

18.03.2015



Contents

Scientific background

Challenges and impact

Consortium

Workplan and project management

Main scientific achievements of 2014-2015

Valorization

CQC

**Composing Quantum
Channels**

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

Scientific background

Every process, every time evolution, every operation, can be abstracted as a quantum channel

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

Scientific background

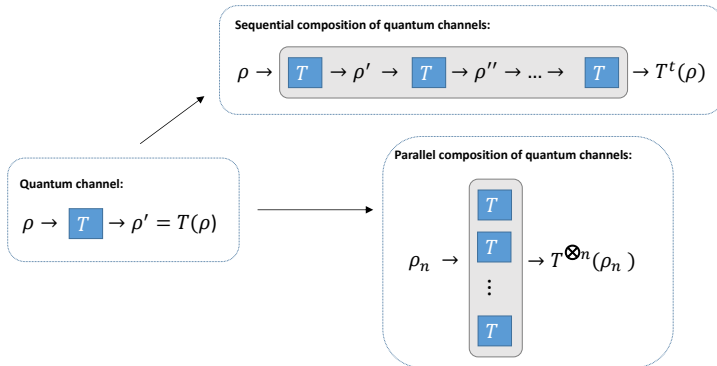
Every process, every time evolution, every operation, can be abstracted as a quantum channel

Quantum channel:

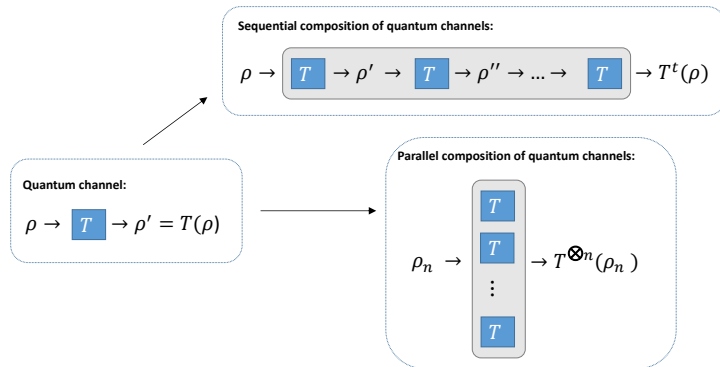
$$\rho \rightarrow T \rightarrow \rho' = T(\rho)$$

Scientific background

Every process, every time evolution, every operation, can be abstracted as a quantum channel



Every process, every time evolution, every operation, can be abstracted as a quantum channel



The CQC project has as purpose studying quantum channels with emphasis on the behavior under composition.

Key challenges and potential impact

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

Challenges (Mostly achieved)

- ▶ *Better convergence bounds for sequential compositions of QC.*
- ▶ *Better bounds on channel capacities (parallel composition of QC).*
- ▶ *Strong no-go results based on undecidability theory.*

Key challenges and potential impact

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

Challenges (Mostly achieved)

- ▶ *Better convergence bounds for sequential compositions of QC.*
- ▶ *Better bounds on channel capacities (parallel composition of QC).*
- ▶ *Strong no-go results based on undecidability theory.*

Impact

- ▶ *Quantum spin systems (analysis of noise and correlations)*
- ▶ *Computer science (quantum algorithms, interactive proof systems)*
- ▶ *Quantum cryptography (QKD, noisy storage model)*



Timeline

CQC

Composing Quantum Channels

Scientific background

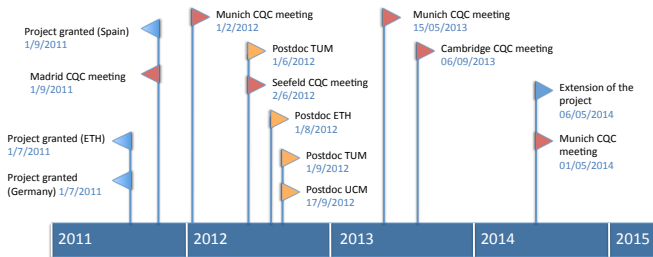
Challenges and impact

Consortium

Workplan and project management

Main scientific achievements of 2014-2015

Valorization



WP1: Basic properties



WP2: Sequential composition



WP3: Parallel composition



WP4: No-go results



WP5: Dissemination



Transnational collaboration

The collaboration between the three groups has been very fruitful so far:

CQC

**Composing Quantum
Channels**

Scientific background

Challenges and impact

Consortium

**Workplan and project
management**

Main scientific
achievements of
2014-2015

Valorization

Transnational collaboration

The collaboration between the three groups has been very fruitful so far:

- ▶ 7 papers involving more than one group.

The collaboration between the three groups has been very fruitful so far:

- ▶ 7 papers involving more than one group.
- ▶ D. Lercher and O. Szehr moved from ETH to TUM.
- ▶ A. Muller-Hermes will move from TUM to Copenhagen later this year.
- ▶ Several short visits and meetings.
- ▶ D. Perez-Garcia (UCM) awarded a John von Neumann guest professorship at TUM (May-July 2014).

The collaboration between the three groups has been very fruitful so far:

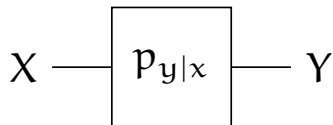
- ▶ 7 papers involving more than one group.
- ▶ D. Lercher and O. Szehr moved from ETH to TUM.
- ▶ A. Muller-Hermes will move from TUM to Copenhagen later this year.
- ▶ Several short visits and meetings.
- ▶ D. Perez-Garcia (UCM) awarded a John von Neumann guest professorship at TUM (May-July 2014).
- ▶ A follow-up project on *undecidability in quantum many body systems* led by D. Perez-Garcia (UCM), T. Cubitt and M.M. Wolf (TUM) has been funded by the Templeton Foundation. The key idea arose out of the work done in CQC.

Unbounded number uses required to detect quantum capacity.

Authors: Toby Cubitt, David Elkouss, William Matthews, Maris Ozols,
David Perez-Garcia, Sergii Strelchuk.

Ref: Nature Communications (to appear) and arXiv:1408.5115.

Classical Channel Capacity



CQC

**Composing Quantum
Channels**

Scientific background

Challenges and impact

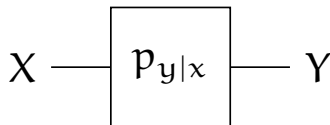
Consortium

Workplan and project
management

**Main scientific
achievements of
2014-2015**

Valorization

Classical Channel Capacity



The capacity is the optimal number of *bits* that can be **asymptotically** and reliably transmitted per use of the channel

Theorem (Shannon 1948)

The capacity of a channel is given by

$$C = \max_{P_X} I(X; Y)$$

Quantum Channel Capacity

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

- Coherent information: $I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

- ▶ Coherent information: $I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$
- ▶ $Q^{(n)}(\mathcal{N}) = \frac{1}{n} \max_{\rho} I_{coh}(\mathcal{N}^{\otimes n}, \rho)$

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

- ▶ Coherent information: $I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$
- ▶ $Q^{(n)}(\mathcal{N}) = \frac{1}{n} \max_{\rho} I_{coh}(\mathcal{N}^{\otimes n}, \rho)$
- ▶ $Q(\mathcal{N}) = \lim_{n \rightarrow \infty} Q^{(n)}(\mathcal{N})$

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

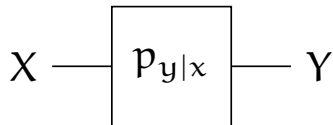
In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

- ▶ Coherent information: $I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$
- ▶ $Q^{(n)}(\mathcal{N}) = \frac{1}{n} \max_{\rho} I_{coh}(\mathcal{N}^{\otimes n}, \rho)$
- ▶ $Q(\mathcal{N}) = \lim_{n \rightarrow \infty} Q^{(n)}(\mathcal{N})$
- ▶ (dVSS'98): $Q(\mathcal{N}) > Q^{(1)}(\mathcal{N})$

The capacity is the optimal number of *qbits* that can be **asymptotically** and reliably transmitted per use of the channel.

In this case, the analogue coding theorem is indeed *asymptotic* (requires regularization).

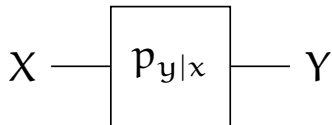
- ▶ Coherent information: $I_{coh}(\mathcal{N}, \rho) = H(\mathcal{N}(\rho)) - H(\mathcal{N}_c(\rho))$
- ▶ $Q^{(n)}(\mathcal{N}) = \frac{1}{n} \max_{\rho} I_{coh}(\mathcal{N}^{\otimes n}, \rho)$
- ▶ $Q(\mathcal{N}) = \lim_{n \rightarrow \infty} Q^{(n)}(\mathcal{N})$
- ▶ (dVSS'98): $Q(\mathcal{N}) > Q^{(1)}(\mathcal{N})$
- ▶ This makes the computation of Q very difficult.



Theorem (Shannon 1948)

The capacity of a channel is given by

$$C = \max_{p_X} I(X; Y)$$



Theorem (Shannon 1948)

The capacity of a channel is given by

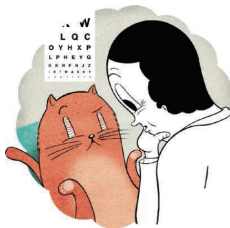
$$C = \max_{p_X} I(X; Y) = 0 \Leftrightarrow Y \text{ is indept from } X$$

CQC

Main scientific achievements of 2014-2015

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

In the quantum case, weird things may happen



‘You appear to be blind in your left eye and blind in your right eye. Why you can see with both eyes is beyond me...’ (Oppenheim, Science 2008)

Theorem (Smith-Yard 2008)

There exist two zero-capacity channels $\mathcal{E}, \mathcal{N}$ s.t. $Q(\mathcal{E} \otimes \mathcal{N}) > 0$.

'You appear to be blind in your left eye and blind in your right eye. Why you can see with both eyes is beyond me...' (Oppenheim, Science 2008)

There exist two zero-capacity channels $\mathcal{E}, \mathcal{N}$ s.t. $Q(\mathcal{E} \otimes \mathcal{N}) > 0$.

There exists a quantum channel $\mathcal{E}$ so that $Q^{(1)}(\mathcal{E}) = 0$ but $Q^{(2)}(\mathcal{E}) > 0$.

Theorem

For each $n \in \mathbb{N}$ there exists a channel $\mathcal{M}$ so that $Q^{(n)}(\mathcal{M}) = 0$ but $Q(\mathcal{M}) > 0$.

Theorem

For each $n \in \mathbb{N}$ there exists a channel $\mathcal{M}$ so that $Q^{(n)}(\mathcal{M}) = 0$ but $Q(\mathcal{M}) > 0$.

- ▶ An unbounded number of channel uses are required to see capacity.

Theorem

For each $n \in \mathbb{N}$ there exists a channel $\mathcal{M}$ so that $Q^{(n)}(\mathcal{M}) = 0$ but $Q(\mathcal{M}) > 0$.

- ▶ An unbounded number of channel uses are required to see capacity.
- ▶ First example of asymptotic regularization.

Theorem

For each $n \in \mathbb{N}$ there exists a channel $\mathcal{M}$ so that $Q^{(n)}(\mathcal{M}) = 0$ but $Q(\mathcal{M}) > 0$.

- ▶ An unbounded number of channel uses are required to see capacity.
- ▶ First example of asymptotic regularization.
- ▶ It suggests that having zero-capacity could be undecidable.

Positivity of linear maps under tensor powers.

Authors: Alexander Muller-Hermes, David Reeb, Michael M. Wolf.

Ref: arXiv:1502.05630

Definition (Tensor-stable positivity)

- (i) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **n-tensor-stable positive** for $n \in \mathbb{N}$ if the map $\mathcal{P}^{\otimes n} : \mathcal{M}_{d_1^n} \rightarrow \mathcal{M}_{d_2^n}$ is positive.
- (ii) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **tensor-stable positive** if it is *n-tensor-stable positive* for all $n \in \mathbb{N}$.

Definition (Tensor-stable positivity)

- (i) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **n-tensor-stable positive** for $n \in \mathbb{N}$ if the map $\mathcal{P}^{\otimes n} : \mathcal{M}_{d_1^n} \rightarrow \mathcal{M}_{d_2^n}$ is positive.
- (ii) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **tensor-stable positive** if it is *n-tensor-stable positive* for all $n \in \mathbb{N}$.

Trivial examples:

- ▶ Completely positive maps.
- ▶ Completely co-positive maps: $\tau \circ T$ where τ is transposition and T completely positive.

Definition (Tensor-stable positivity)

- (i) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **n-tensor-stable positive** for $n \in \mathbb{N}$ if the map $\mathcal{P}^{\otimes n} : \mathcal{M}_{d_1^n} \rightarrow \mathcal{M}_{d_2^n}$ is positive.
- (ii) A linear map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$ is called **tensor-stable positive** if it is *n-tensor-stable positive* for all $n \in \mathbb{N}$.

Trivial examples:

- ▶ Completely positive maps.
- ▶ Completely co-positive maps: $\tau \circ T$ where τ is transposition and T completely positive.

Questions

1. Is there a non-trivial example of tensor-stable positive map?
2. If so, would it have any implication in quantum information theory?

Tensor-stable positive maps

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

Main scientific
achievements of
2014-2015

Valorization

Theorem

For any $d_1, d_2 \geq 2$ and $n \in \mathbb{N}$, there exists a non trivial n -tensor-stable positive map

Theorem

For any $d_1, d_2 \geq 2$ and $n \in \mathbb{N}$, there exists a non trivial n -tensor-stable positive map

Theorem

For any d , there exist no non-trivial tensor-stable positive maps $\mathcal{P} : \mathcal{M}_d \rightarrow \mathcal{M}_2$ or $\mathcal{P} : \mathcal{M}_2 \rightarrow \mathcal{M}_d$.

Theorem

For any $d_1, d_2 \geq 2$ and $n \in \mathbb{N}$, there exists a non trivial n -tensor-stable positive map

Theorem

For any d , there exist no non-trivial tensor-stable positive maps $\mathcal{P} : \mathcal{M}_d \rightarrow \mathcal{M}_2$ or $\mathcal{P} : \mathcal{M}_2 \rightarrow \mathcal{M}_d$.

Theorem

If there exists a non trivial tensor-stable positive map $\mathcal{P} : \mathcal{M}_{d_1} \rightarrow \mathcal{M}_{d_2}$, then there exist NPT bound entangled states in $\mathcal{M}_{d_1} \otimes \mathcal{M}_{d_1}$ and in $\mathcal{M}_{d_2} \otimes \mathcal{M}_{d_2}$

NPT bound entangled states?

The existence of NPT bound entangled states is the oldest and more elusive open question in quantum information theory.

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

**Main scientific
achievements of
2014-2015**

Valorization

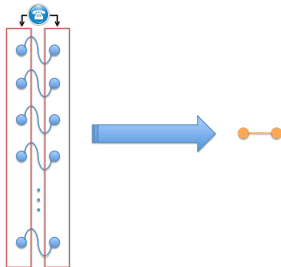
NPT bound entangled states?

The existence of NPT bound entangled states is the oldest and more elusive open question in quantum information theory.

Definition

A mixed bipartite state $\rho_{AB} \in \mathcal{M}_{d_A} \otimes \mathcal{M}_{d_B}$ is:

- ▶ PPT if $\tau_A \otimes \text{Id}_B(\rho_{AB})$ is positive.
- ▶ NPT if it is not PPT
- ▶ distillable if by taking $N \rightarrow \infty$ copies of ρ_{AB} one may distill by LOCC one copy of the maximally entangled state (EPR pair).
- ▶ bound entangled if it is entangled but not distillable.



NPT bound entangled states?

The existence of NPT bound entangled states is the oldest and more elusive open question in quantum information theory.

Definition

A mixed bipartite state $\rho_{AB} \in \mathcal{M}_{d_A} \otimes \mathcal{M}_{d_B}$ is:

- ▶ PPT if $\tau_A \otimes \text{Id}_B(\rho_{AB})$ is positive.
- ▶ NPT if it is not PPT
- ▶ distillable if by taking $N \rightarrow \infty$ copies of ρ_{AB} one may distill by LOCC one copy of the maximally entangled state (EPR pair).
- ▶ bound entangled if it is entangled but not distillable.

Let us assume that ρ_{AB} is entangled.
[HHH98] PPT $\Rightarrow$ bound entangled.

NPT bound entangled states?

The existence of NPT bound entangled states is the oldest and more elusive open question in quantum information theory.

Definition

A mixed bipartite state $\rho_{AB} \in \mathcal{M}_{d_A} \otimes \mathcal{M}_{d_B}$ is:

- ▶ PPT if $\tau_A \otimes \text{Id}_B(\rho_{AB})$ is positive.
- ▶ NPT if it is not PPT
- ▶ distillable if by taking $N \rightarrow \infty$ copies of ρ_{AB} one may distill by LOCC one copy of the maximally entangled state (EPR pair).
- ▶ bound entangled if it is entangled but not distillable.

Let us assume that ρ_{AB} is entangled.

[HHH98] PPT $\Rightarrow$ bound entangled.

The absence of NPT bound entangled states is just the reverse implication.

NPT bound entangled states?

The existence of NPT bound entangled states is the oldest and more elusive open question in quantum information theory.

Definition

A mixed bipartite state $\rho_{AB} \in \mathcal{M}_{d_A} \otimes \mathcal{M}_{d_B}$ is:

- ▶ PPT if $\tau_A \otimes \text{Id}_B(\rho_{AB})$ is positive.
- ▶ NPT if it is not PPT
- ▶ distillable if by taking $N \rightarrow \infty$ copies of ρ_{AB} one may distill by LOCC one copy of the maximally entangled state (EPR pair).
- ▶ bound entangled if it is entangled but not distillable.

Let us assume that ρ_{AB} is entangled.

[HHH98] PPT $\Rightarrow$ bound entangled.

The absence of NPT bound entangled states is just the reverse implication.

If true: a extremely simple (and efficiently computable) criterion for distillability

If not: extremely weird behaviors (super activation of distillability, non-convexity of distillable entanglement)

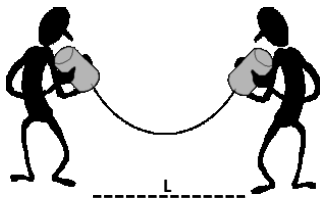
Limitations on Quantum Key Repeaters

Authors: Stefan Bauml, Matthias Christandl, Karol Horodecki, Andreas Winter.

Ref: arXiv:1402.5927

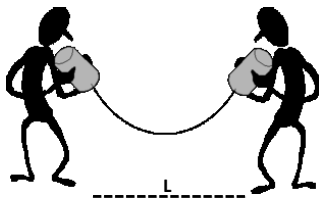
Quantum Repeaters

When a signal is passed through a receiver, it degrades exponentially in the distance L .



Quantum Repeaters

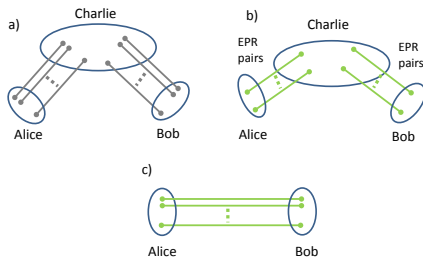
When a signal is passed through a receiver, it degrades exponentially in the distance L .



- ▶ Classical solution: amplification.
- ▶ Cannot work due to no-cloning if the signal is quantum mechanical.
- ▶ Sending a quantum signal crucial for QKD.
- ▶ Crucial limitation on distance to apply QKD.

Quantum Repeaters

A way around: Quantum Repeaters [BDC1998]



- (a)** Alice and Charlie (and similarly Charlie and Bob) distill EPR pairs from noisy states.
- (b)** Charlie uses the EPR pairs he shares with Bob to teleport his part of the state he shares with Alice
- (c)** Alice and Bob share EPR pairs that can be used to send key securely

Quantum Repeaters

It is well known [HHHO2005] that there are bound entangled states from which secret key can be extracted.

CQC

**Composing Quantum
Channels**

Scientific background

Challenges and impact

Consortium

Workplan and project
management

**Main scientific
achievements of
2014-2015**

Valorization

It is well known [HHHO2005] that there are bound entangled states from which secret key can be extracted.

Question

Can one come up with a repeater construction working directly with secret key instead of going via distillation of EPR pairs?

It is well known [HHHO2005] that there are bound entangled states from which secret key can be extracted.

Question

Can one come up with a repeater construction working directly with secret key instead of going via distillation of EPR pairs?

It would have the potential to:

- ▶ improve the secret key rate
- ▶ have an easier implementation
- ▶ tolerate larger amount of noise

It is well known [HHHO2005] that there are bound entangled states from which secret key can be extracted.

Question

Can one come up with a repeater construction working directly with secret key instead of going via distillation of EPR pairs?

It would have the potential to:

- ▶ improve the secret key rate
- ▶ have an easier implementation
- ▶ tolerate larger amount of noise

Main result: upper bounds on the *quantum key repeater rate* of a quantum state. As a consequence:

Theorem

Then answer to the question is NO. There exist states with a large key rate but with a negligible quantum key repeater rate.

Main scientific achievements of 2014-2015

CQC

Composing Quantum
Channels

Scientific background

Challenges and impact

Consortium

Workplan and project
management

**Main scientific
achievements of
2014-2015**

Valorization

Other important achievements:

- ▶ An optimal bound on the circuit complexity (number of CNOTS) needed to implement any quantum channel.
- ▶ An area law for the mutual information in the fixed point of any rapidly mixing quantum many body Markovian process.
- ▶ Strong bounds on the convergence of depolarizing channels via log-Sobolev inequalities.
- ▶

- ▶ The CQC project (now close to its end) has been a complete success.
- ▶ An important step forward in the theoretical study of quantum channels.
- ▶ Applications in quantum spin systems, quantum cryptography and computer science.
- ▶ Fruitful collaboration and scientific exchange between partners.
- ▶ New ideas arisen in CQC gave rise to follow-up projects (Templeton Foundation, 2 ERC grants).