Two-way assisted capacities for quantum and private communication

Riccardo Laurenza
University of York

Based on the **PLOB** paper:

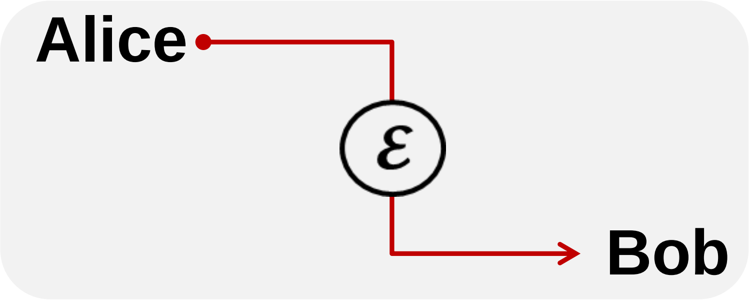
Pirandola, **L**aurenza, **O**ttaviani, **B**anchi
"Fundamental limits of repeaterless quantum communications"
arXiv:1510.08863 (2015) – *Hopefully* soon on Nature Comms

QIP2017 - Westin, Seattle, Washington, USA (January 14-20, 2017)

Basic Problem

Consider the following tasks over a quantum channel:

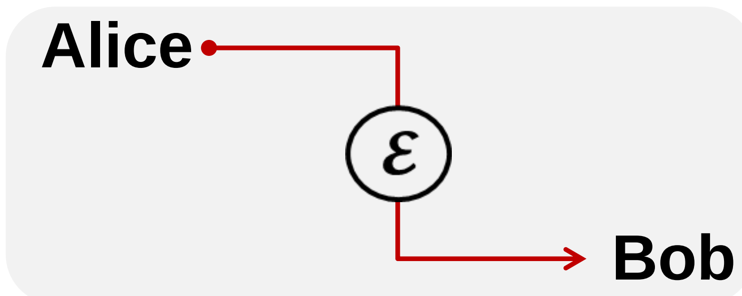
QC = **Q**uantum **C**ommunication – *transmission of qubits*
ED = **E**ntanglement **D**istribution – *sharing of ebits*
QKD = **Q**uantum **K**ey **D**istribution – *generation of secret bits*



Basic Problem

Consider the following tasks over a quantum channel:

QC = **Q**uantum **C**ommunication – *transmission of qubits*
ED = **E**ntanglement **D**istribution – *sharing of ebits*
QKD = **Q**uantum **K**ey **D**istribution – *generation of secret bits*

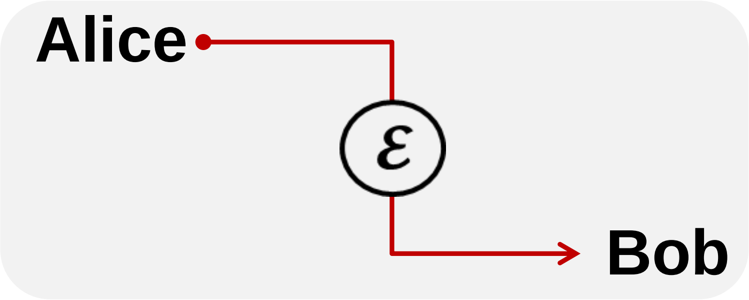


What are the maximum rates achievable by point-to-point protocols?

Basic Problem

Consider the following tasks over a quantum channel:

QC = **Q**uantum **C**ommunication – *transmission of qubits*
ED = **E**ntanglement **D**istribution – *sharing of ebits*
QKD = **Q**uantum **K**ey **D**istribution – *generation of secret bits*



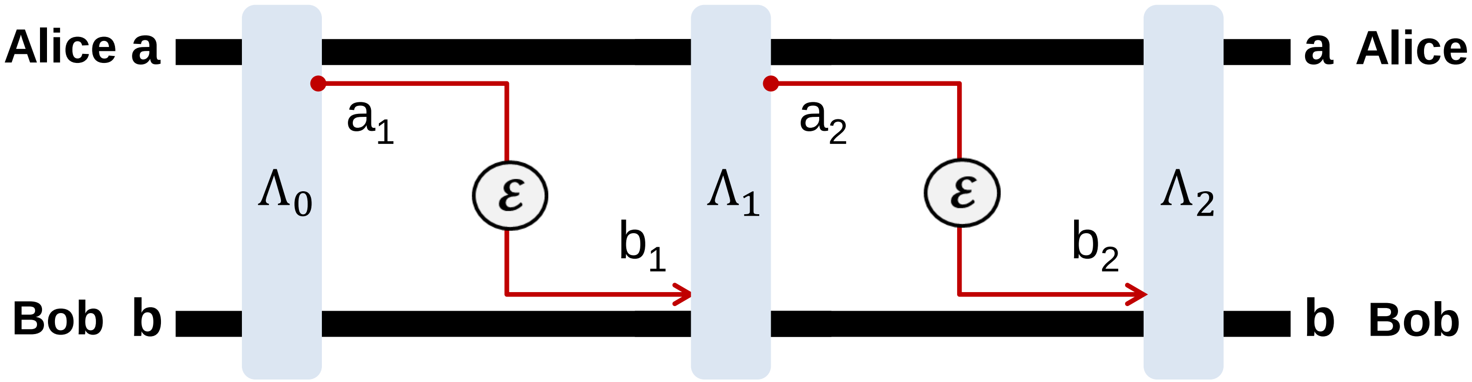
What are the maximum rates achievable by point-to-point protocols?

2-way capacities of the channel

Defined by optimizing the rates over **adaptive LOCCs** (LOs assisted by unlimited 2-way CCs)

Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



- Arbitrary task (can be QC, ED, QKD…)
- Arbitrary dimension (qubits, qudits, bosonic)

Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs

Alice a

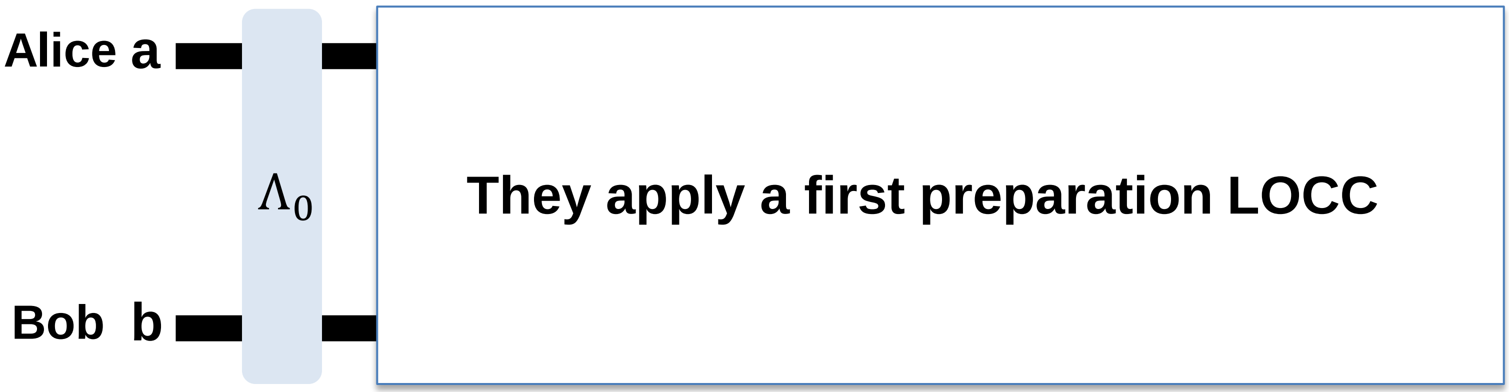
Alice and Bob have local registers “a” and “b”

(ensembles of quantum systems)

Bob b

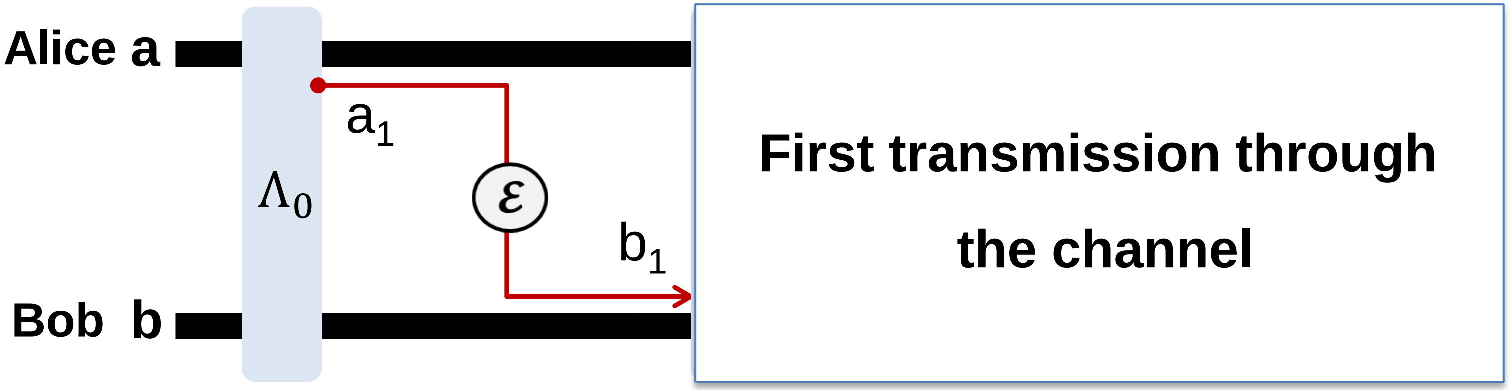
Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



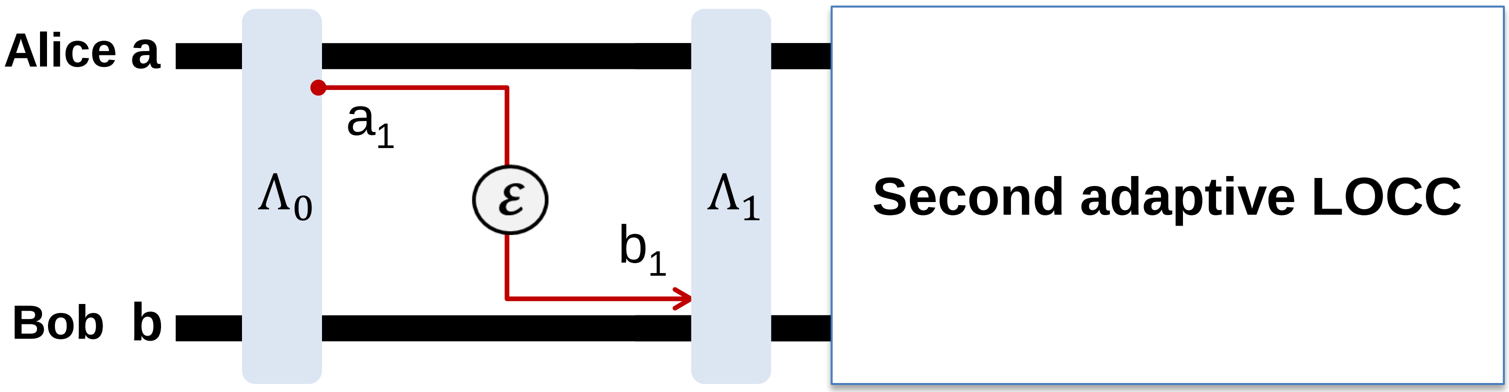
Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



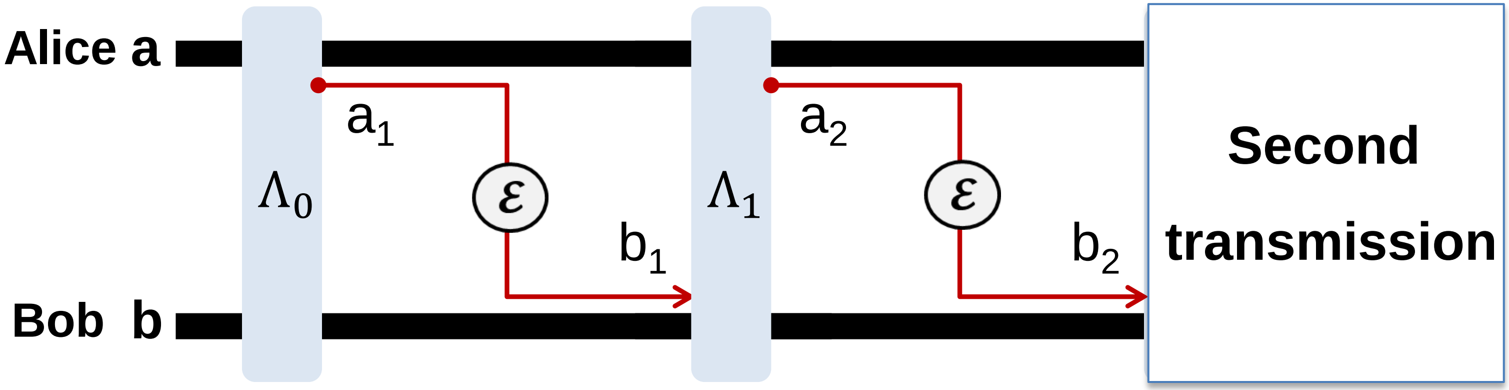
Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



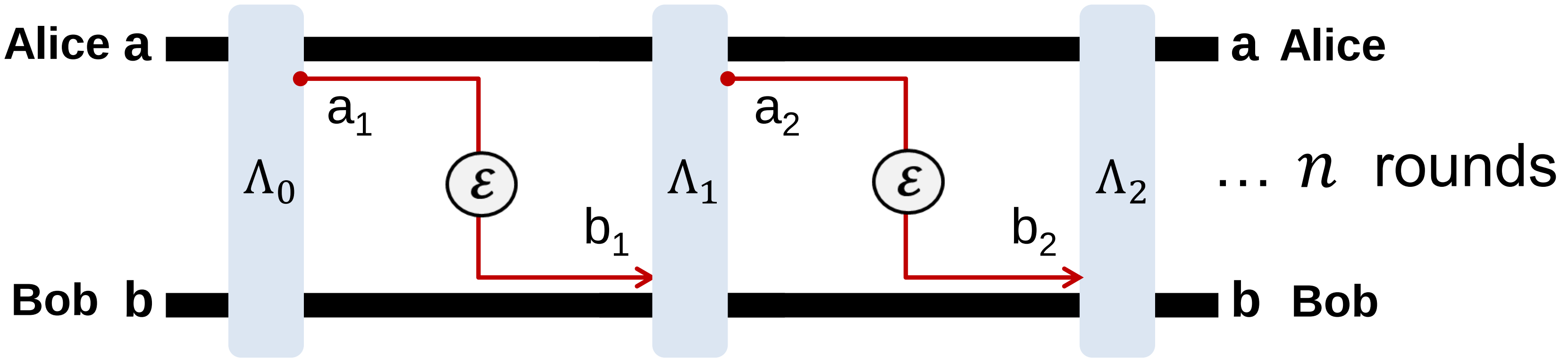
Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



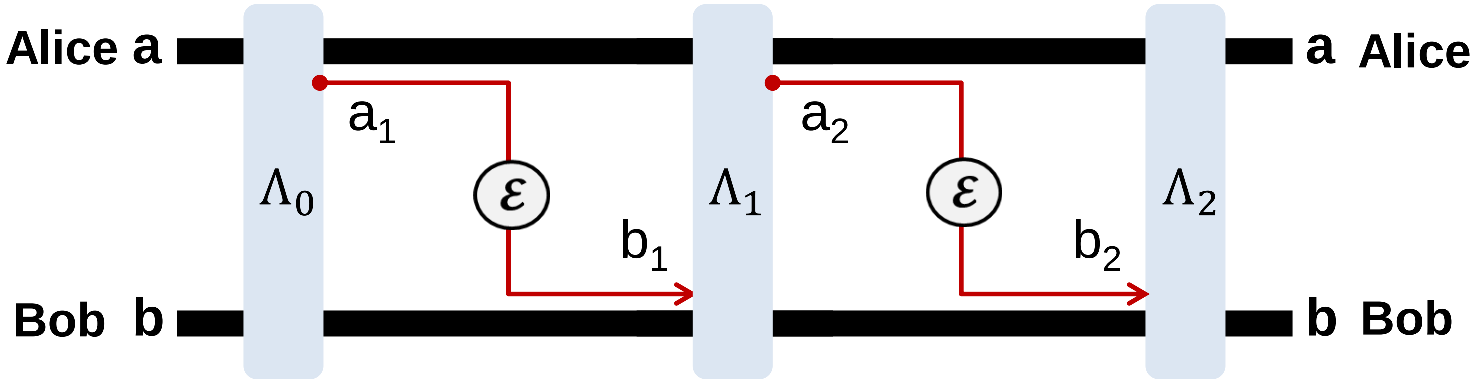
Adaptive protocols over a quantum channel

Quantum protocol
assisted by adaptive LOCCs



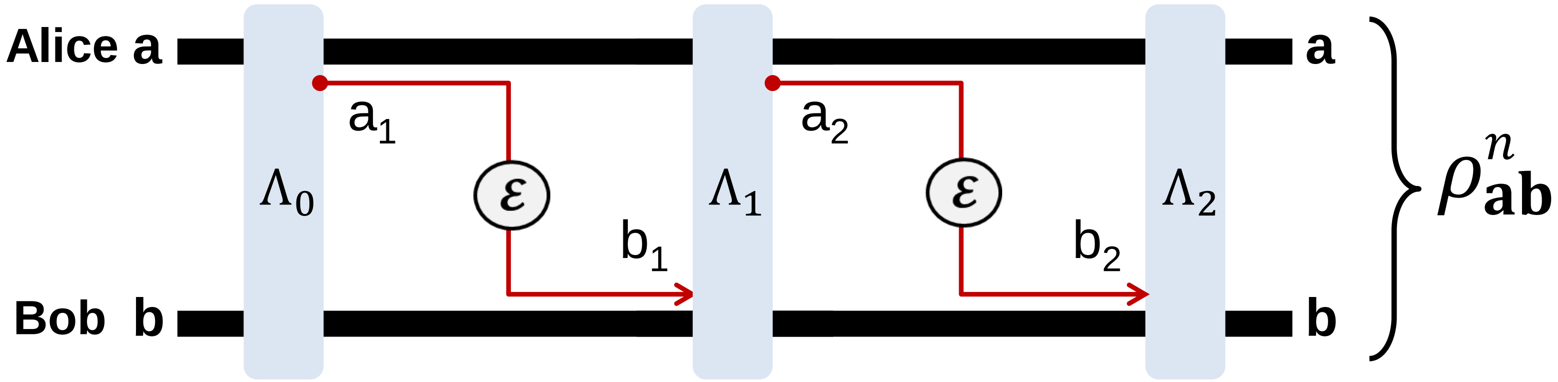
Another adaptive LOCC and so on…

Adaptive protocols over a quantum channel



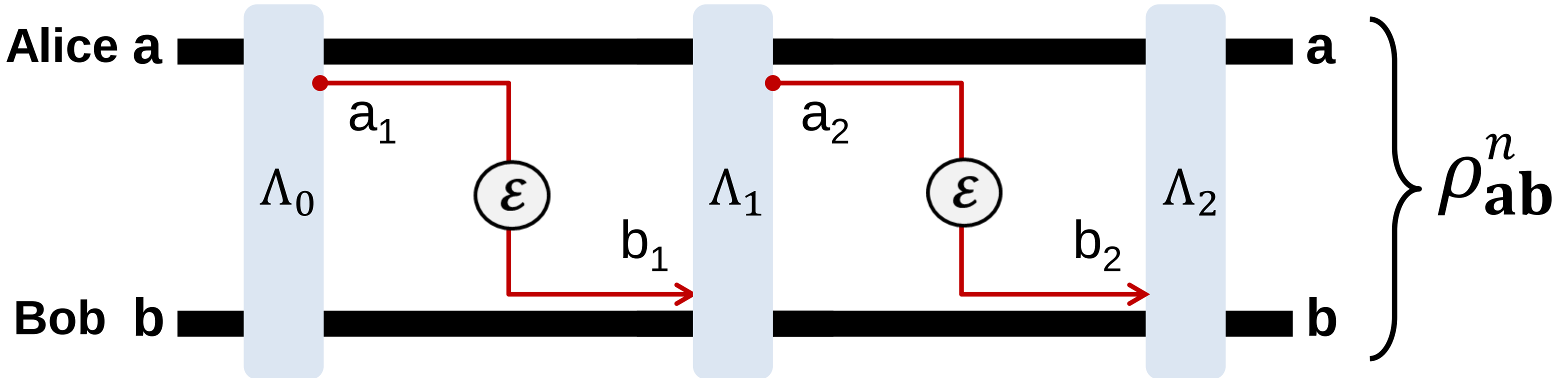
- LOCC-sequence defining the protocol $\mathcal{L} = \{\Lambda_0, \Lambda_1, \cdots, \Lambda_n\}$

Adaptive protocols over a quantum channel



- LOCC-sequence defining the protocol $\mathcal{L} = \{\Lambda_0, \Lambda_1, \cdots, \Lambda_n\}$
- Output $\rho^n_{\mathbf{ab}} \approx \phi_n$ target state defining the rate R_n (bits/use)

Adaptive protocols over a quantum channel



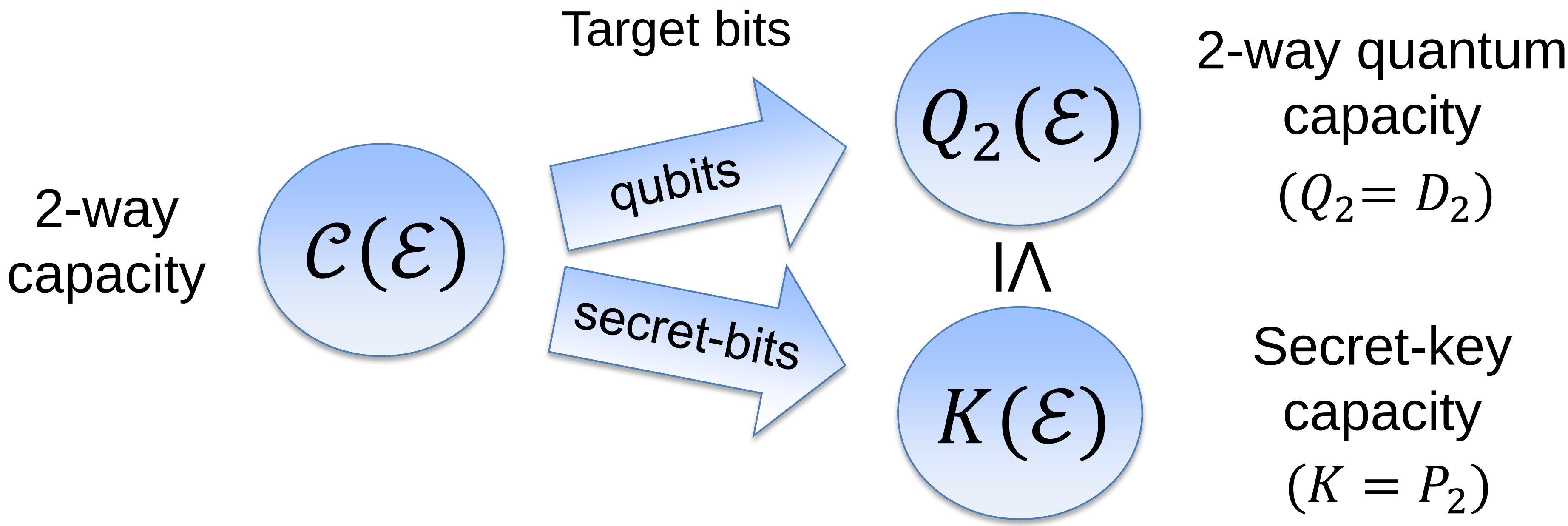
- LOCC-sequence defining the protocol $\mathcal{L} = \{\Lambda_0, \Lambda_1, \cdots, \Lambda_n\}$
- Output $\rho^n_{\mathbf{ab}} \approx \phi_n$ target state defining the rate R_n (bits/use)
- Generic 2-way capacity of the channel

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} R_n$$

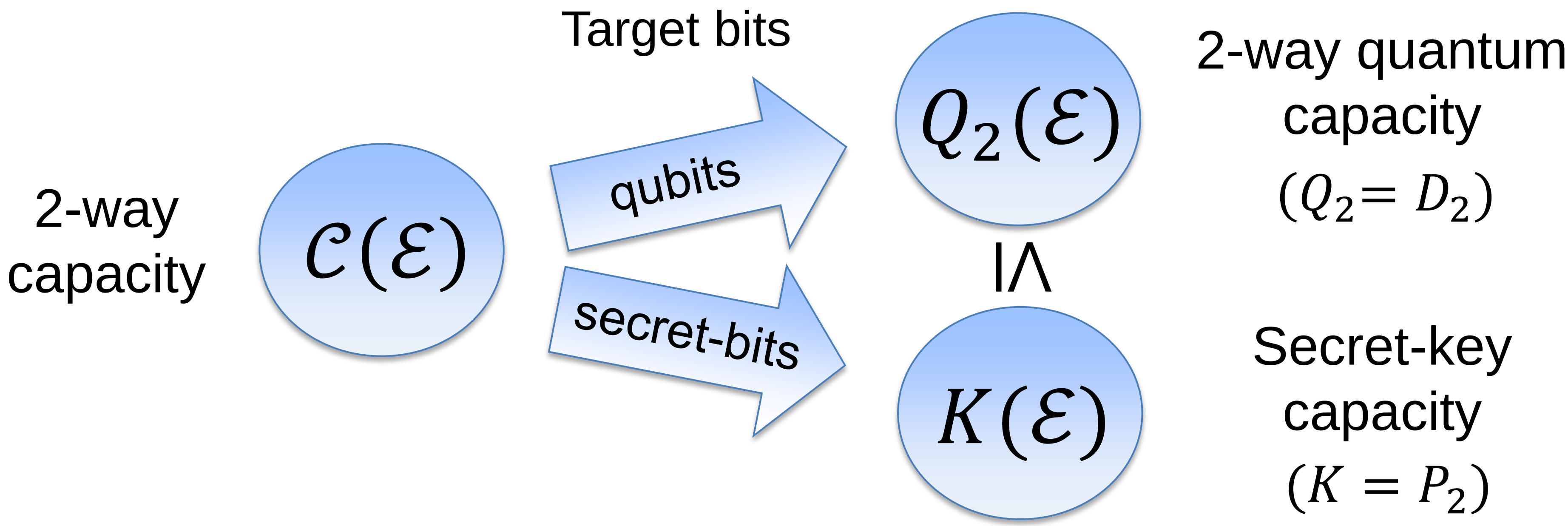
Optimization over adaptive protocols

Asymptotic rate

Two-way capacities and benchmarks



Two-way capacities and benchmarks



2-way capacities are **optimal point-to-point rates**

No constraints on:

- ❑ LOCCs
- ❑ Number of channel uses
- ❑ Input energy

Therefore, **general benchmarks** for quantum repeaters

Bounding two-way capacities

$$\underbrace{Q_2(\mathcal{E}) \leq K(\mathcal{E})}_{\mathcal{C}(\mathcal{E})} \leq \textbf{?}$$

General Reduction Method

1) Relative Entropy of Entanglement (REE)
2) LOCC-simulation of quantum channels
3) Teleportation Stretching of adaptive protocols

*Formulations are asymptotic for bosonic channels

$$\Rightarrow \mathcal{C}(\mathcal{E}) \leq \textbf{Single-Letter Bound}$$

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq \mathbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{ab}})}{n}}$$

[PLOB, Theorem 1]

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq \mathbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho_{\mathbf{ab}}^n)}{}}$$

[PLOB, Theorem 1]

REE computed on the output state

$$E_R(\rho_{\mathbf{ab}}^n) := \min_{\sigma \in \mathrm{SEP}} S(\rho_{\mathbf{ab}}^n || \sigma)$$

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \ \leq \textbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{ab}})}{n}}$$

[PLOB, Theorem 1]

PLOB gives <u>alternative</u> but equivalent proofs:

$$\rho^n_{\mathbf{ab}} \approx \underbrace{\phi_n}_{\text{private state}} \begin{cases} \text{Key system} \\ \boxed{\text{Shield system}} \end{cases}$$

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq ?$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_n \frac{E_R(\rho^n_{\mathbf{ab}})}{n}}$$

[PLOB, Theorem 1]

PLOB gives <u>alternative</u> but equivalent proofs:

$$\rho^n_{\mathbf{ab}} \approx \phi_n \begin{cases} \text{Key system} \\ \boxed{\text{Shield system}} \end{cases}$$

private state

Proof 1: Size grows (at most) exponentially*

$$nR \leq E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) + 4\varepsilon \log_2 d_{\mathbf{ab}} + 2H_2(\varepsilon)$$

$$d_{\mathbf{ab}} \leq c^n$$

*For **both DVs and CVs** justified by known arguments [Christiandl et al., CMP 311, 397 (2012)]

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq \mathbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho_{\mathbf{ab}}^n)}{n}}$$

[PLOB, Theorem 1]

PLOB gives <u>alternative</u> but equivalent proofs:

$$\rho_{\mathbf{ab}}^n \approx \underbrace{\phi_n}_{\text{private state}} \begin{cases} \text{Key system} \\ \boxed{\text{Shield system}} \end{cases}$$

Proof 1: Size grows (at most) exponentially*
Proof 2: Energy grows (at most) exponentially

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq \mathbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^\star(\mathcal{E}) := \sup_{\mathcal{L}} \lim_n \frac{E_R(\rho_{\mathbf{ab}}^n)}{n}}$$

[PLOB, Theorem 1]

PLOB gives alternative but equivalent proofs:

$$\rho_{\mathbf{ab}}^n \approx \underbrace{\phi_n}_{\text{private state}} \begin{cases} \text{Key system} \\ \boxed{\text{Shield system}} \end{cases}$$

Proof 1: Size grows (at most) exponentially*
Proof 2: Energy grows (at most) exponentially
Proof 3: No assumptions on the shield

$$nR \leq E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n) + 8\varepsilon \log_2 d_{\mathrm{K}} + 2H_2(\varepsilon)$$

Dimension of key system only

General Reduction Method (1)

$$Q_2(\mathcal{E}) \leq K(\mathcal{E}) \leq \mathbf{?}$$

REE bound for the channel

$$\boxed{K(\mathcal{E}) \leq E_R^{\star}(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho_{\mathbf{ab}}^n)}{n}}$$

[PLOB, Theorem 1]

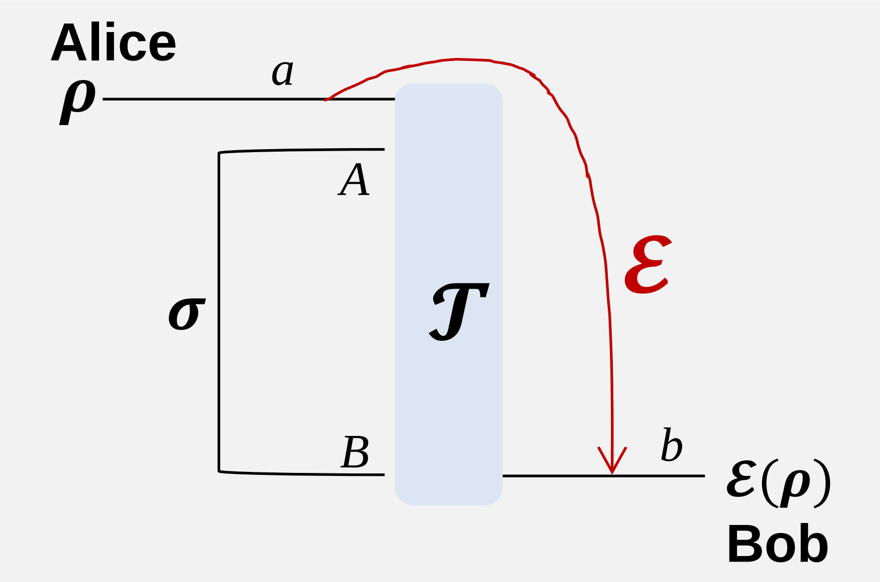
Difficult bound

We need to simplify the output state

(2) LOCC-simulation & (3) Teleportation stretching

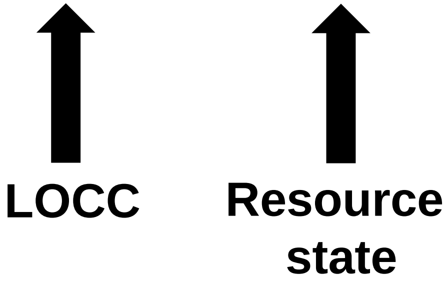
General Reduction Method (2)

LOCC-simulation of (any) quantum channel



σ –stretchable channel

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma)$$



*Asymptotic formulation for bosonic channels (LOCC may include parts of the channel)

- Precursory teleportation-based tool in BDSW, restricted to Pauli channels

BDSW = [Bennett et al., PRA 54, 3824 (1996)]

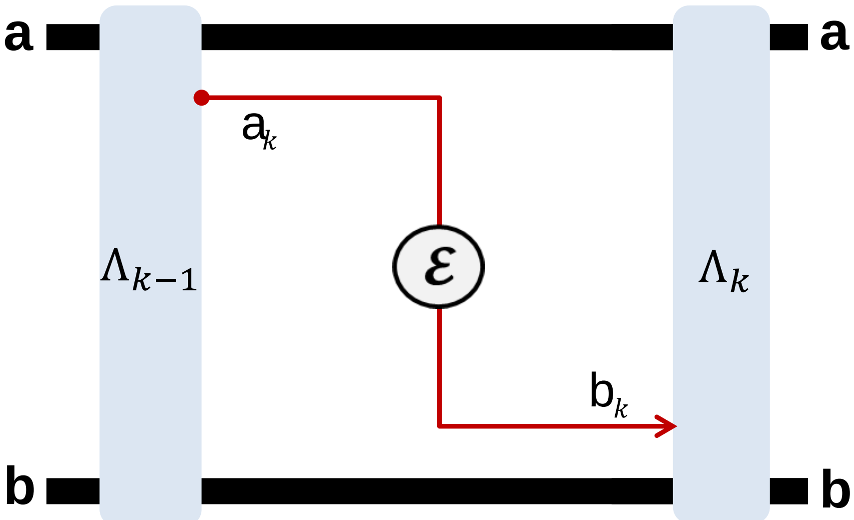
- Different non-local tool in NC, restricted to programmable channels

NC = [Nielsen & Chuang, PRL 79, 321 (1997)]

General Reduction Method (3)

<u>Teleportation-stretching</u>:

Reduction of an adaptive protocol to a block one

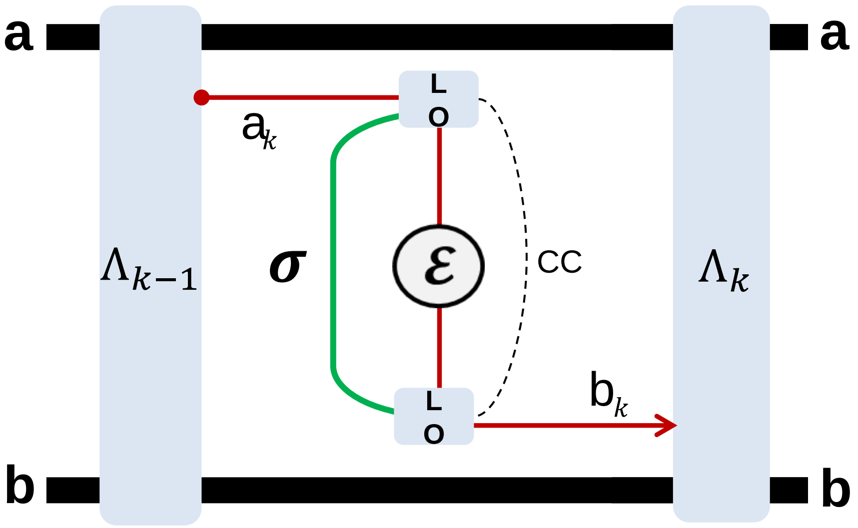


Transmission between adaptive LOCCs

General Reduction Method (3)

<u>Teleportation-stretching</u>:

Reduction of an adaptive protocol to a block one

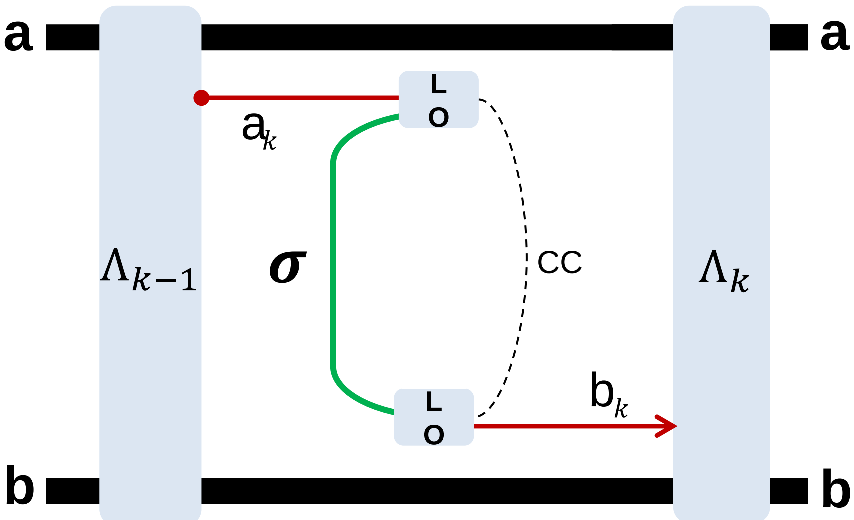


LOCC-simulation
of the channel

General Reduction Method (3)

Teleportation-stretching:

Reduction of an adaptive protocol to a block one

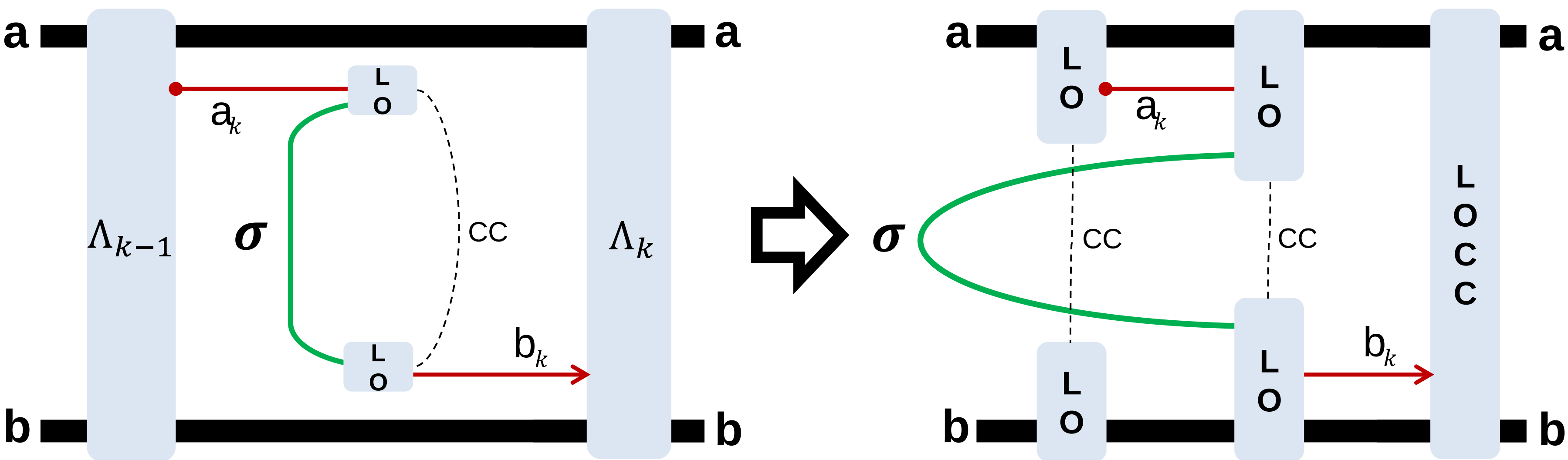


LOCC-simulation
of the channel

General Reduction Method (3)

Teleportation-stretching:

Reduction of an adaptive protocol to a block one

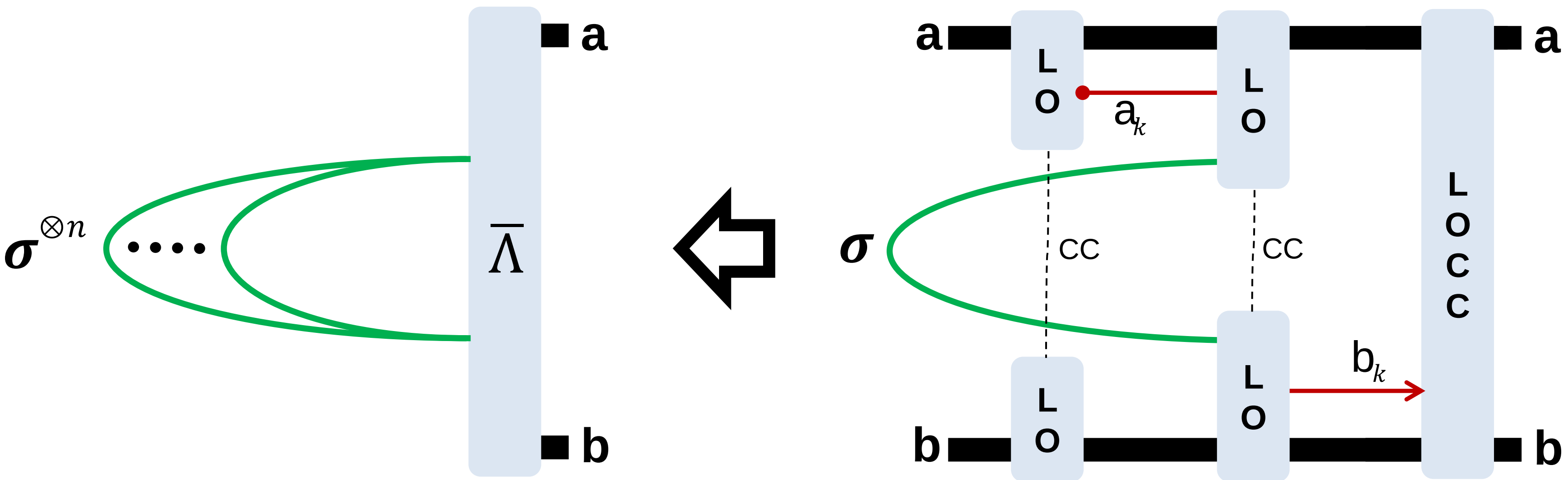


Stretching of the resource state

General Reduction Method (3)

Teleportation-stretching:

Reduction of an adaptive protocol to a block one

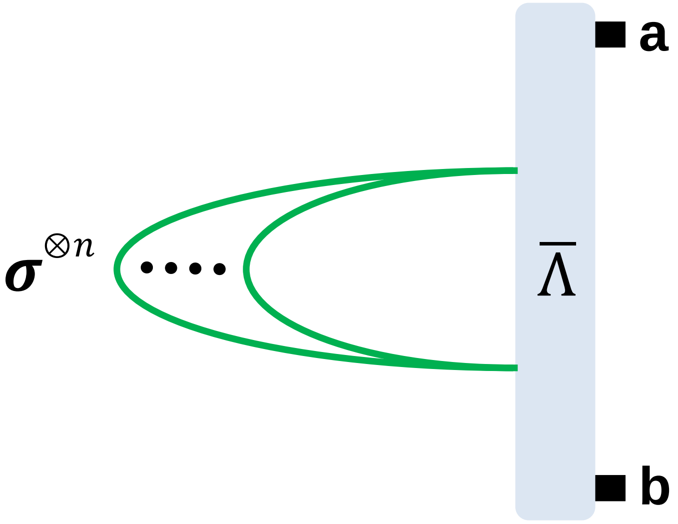


Iteration and collapse of the LOCCs

General Reduction Method (3)

Teleportation-stretching:

Reduction of an adaptive protocol to a block one

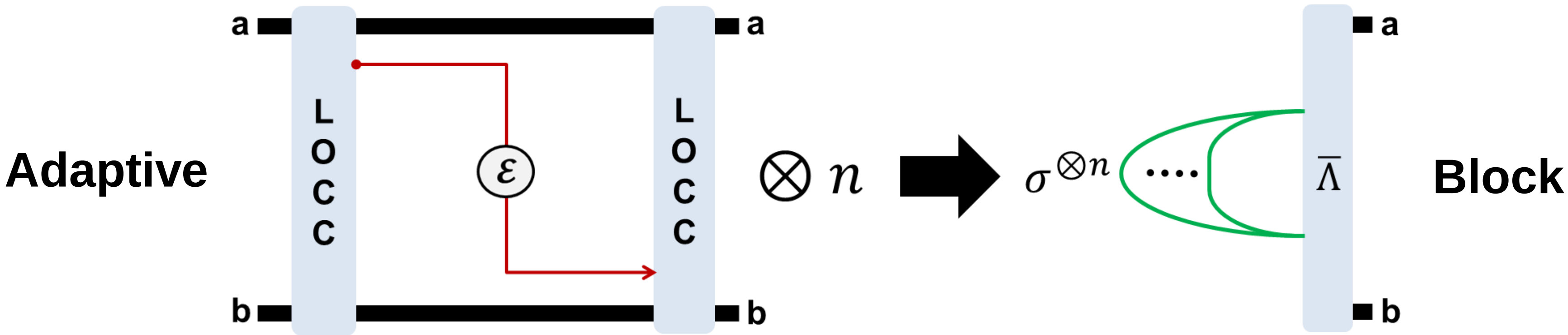


$$\rho^{n}_{\mathbf{ab}} = \bar{\Lambda}(\sigma^{\otimes n})$$

Decomposition of the output

[PLOB, Lemma 3]

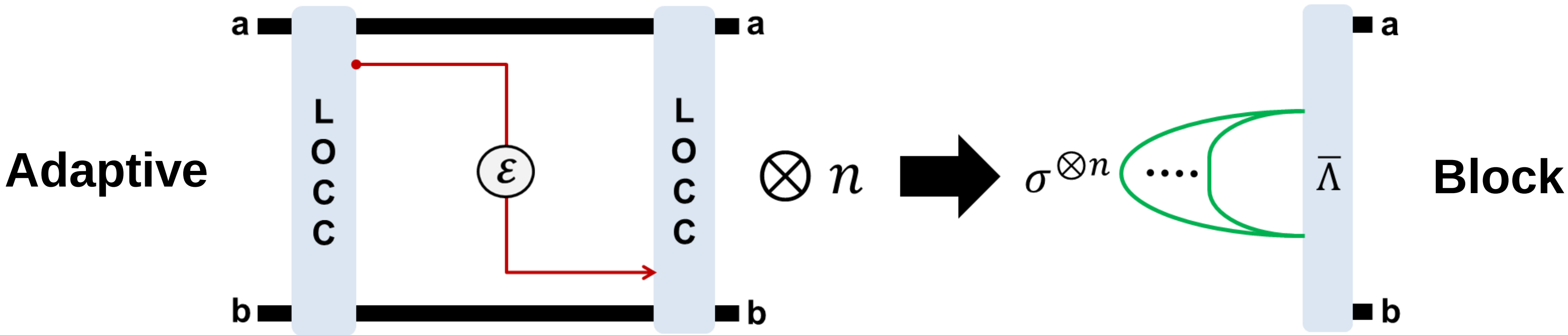
General Reduction Method (3)



Teleportation-stretching:

- Maintain the task (QC, ED, QKD, any task!)
- Any channel
- Any dimension (finite or infinite)

General Reduction Method (3)



<u>Teleportation-stretching</u>:

- Maintain the task (QC, ED, QKD, any task!)
- Any channel
- Any dimension (finite or infinite)

> ➢ Precursory but restricted argument in BDSW:
> - From QC to ED (task changing)
> - Restricted to Pauli channels in finite dimension

BDSW = [Bennett et al., PRA 54, 3824 (1996)]

General Reduction Method (3)

Combining the ingredients: REE + teleportation stretching

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) \coloneqq \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho_{\mathbf{ab}}^n)}{n}$$ REE bound

General Reduction Method (3)

Combining the ingredients: REE + teleportation stretching

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho_{\mathbf{ab}}^n)}{n}$$

REE bound

Stretching

$$\rho_{\mathbf{ab}}^n = \bar{\Lambda}(\sigma^{\otimes n})$$

$$E_R(\rho_{\mathbf{ab}}^n) \leq n E_R(\sigma)$$

Monotonicity & subadditivity of the REE

General Reduction Method (3)

Combining the ingredients: REE + teleportation stretching

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) := \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{ab}})}{n}$$ REE bound

Stretching $$\boxed{\rho^n_{\mathbf{ab}} = \bar{\Lambda}(\sigma^{\otimes n})}$$

$$E_R(\rho^n_{\mathbf{ab}}) \leq n E_R(\sigma)$$

Monotonicity & subadditivity of the REE

$$\mathcal{C}(\mathcal{E}) \leq E_R(\mathcal{E}) \leq \cancel{\sup_{\mathcal{L}}} \cancel{\lim_{n}} \frac{\cancel{n} E_R(\sigma)}{\cancel{n}}$$ **Single-Letter Bound**

Single-letter bounds for 2-way capacities

Combining the ingredients: REE + teleportation stretching

$$\boxed{\mathcal{C}(\mathcal{E}) \leq E_R(\sigma)}$$ [PLOB, Theorem 5]

Single-letter bounds for 2-way capacities

Combining the ingredients: REE + teleportation stretching

$$\boxed{\mathcal{C}(\mathcal{E}) \leq E_R(\sigma)}$$ [PLOB, Theorem 5]

Tele-covariance [PLOB, Proposition 2]

If $\mathcal{E}$ is teleportation-covariant $\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger$

then $\sigma = \rho_{\mathcal{E}}$ (Choi-stretchable channel)

Single-letter bounds for 2-way capacities

Combining the ingredients: REE + teleportation stretching

$$\boxed{\mathcal{C}(\mathcal{E}) \leq E_R(\sigma)}$$ [PLOB, Theorem 5]

Tele-covariance [PLOB, Proposition 2]

If $\mathcal{E}$ is teleportation-covariant $\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger$

then $\sigma = \rho_{\mathcal{E}}$ (Choi-stretchable channel)

For a Choi-stretchable channel $\mathcal{E}$ we have

$$\boxed{\mathcal{C}(\mathcal{E}) \leq E_R(\rho_{\mathcal{E}})}$$

*Asymptotic formulation for bosonic channels

Stretchable and Distillable Channels

Choi-stretchable channels

- Bosonic Gaussian channels
- Pauli channels

$$\mathcal{C}(\mathcal{E}) \leq E_R(\rho_{\mathcal{E}})$$

Stretchable and Distillable Channels

Choi-stretchable channels

- Bosonic Gaussian channels
- Pauli channels

$$\mathcal{C}(\mathcal{E}) \leq E_R(\rho_{\mathcal{E}})$$

Distillable channels

- Bosonic lossy channels
- Quantum-limited amplifiers
- Dephasing channels
- Erasure channels

$$D_1(\rho_{\mathcal{E}}) = \mathcal{C}(\mathcal{E}) = E_R(\rho_{\mathcal{E}})$$

2-way capacities all established

Two-way capacities of distillable channels

- Lossy channel (transmissivity η) $\boxed{Q_2 = K = -\log_2(1-\eta)}$
- Quantum-limited amplifier (gain g) $\boxed{Q_2 = K = -\log_2(1-g^{-1})}$
- Dephasing channel (probability p) $\boxed{Q_2 = K = 1 - H_2(p)}$ *
- Erasure channel (probability p) $\boxed{Q_2 = K = 1 - p}$ *

Only result previously known!
[Bennett et al. PRL 78, 3217 (1997)]

See also the independent proof in
[Goodenough et al. arXiv:1511.08710]

*Similar results for arbitrary dim $d \geq 2$

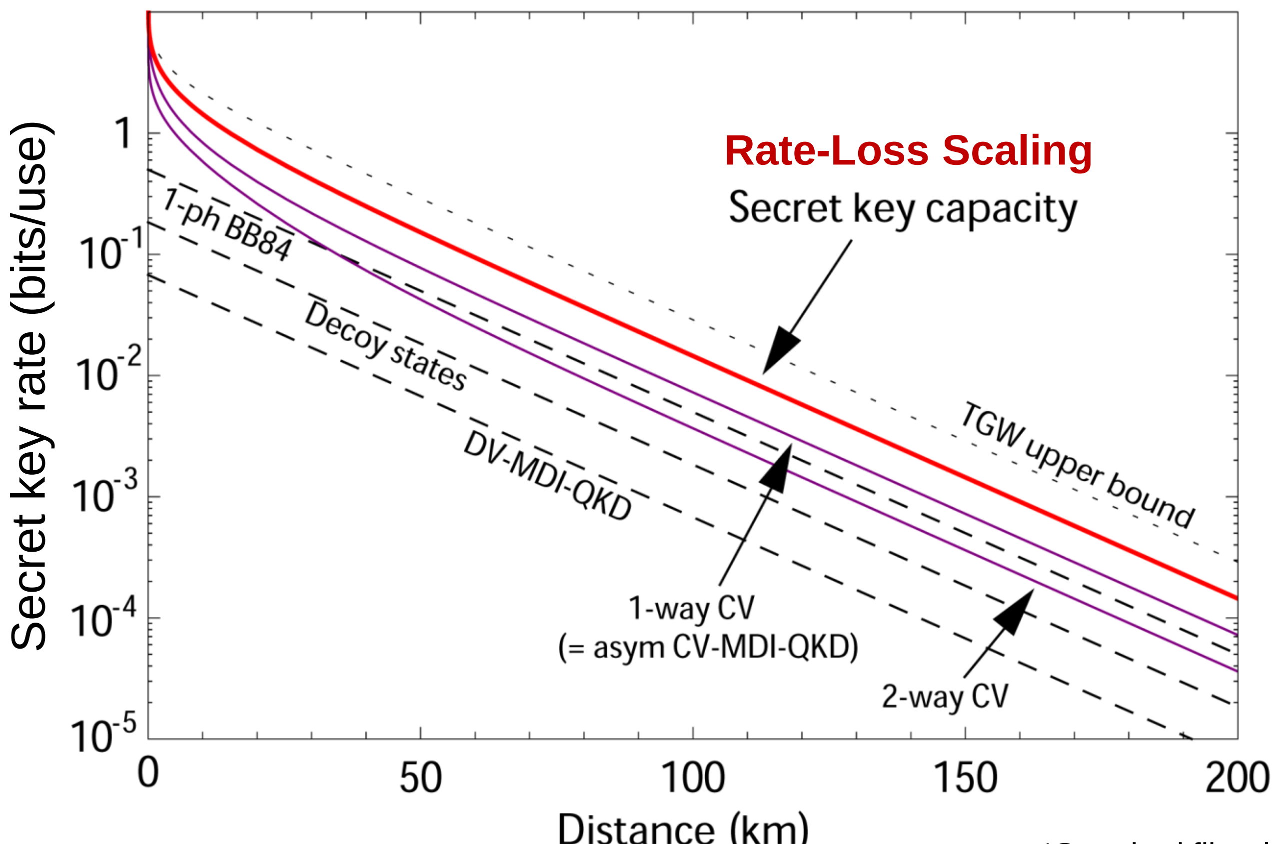
Two-way capacities of distillable channels

- ❑ Lossy channel (transmissivity η)

$$\boxed{\mathrm{Q}_2 = K = -\log_2(1-\eta)}$$

At long distances $(\eta \simeq 0)$ rate-loss scaling for repeaterless quantum communications (QKD)

$$\boxed{K \simeq 1.44\,\eta \ \text{ bits/use}}$$



*Standard fibre loss-rate (0.2dB/km)

Conclusions

New methodology

Channel's REE + Teleportation Stretching

Reduction of adaptive protocols to single-letter bounds

Our main results

- 2-way capacities of many channels (lossy, amplifiers, dephasing, erasure)
- Fundamental rate-loss scaling for optical quantum comms (1.44 bits/use)
- Benchmarks for quantum repeaters

Some recent developments and follow-up works

- Theory extended to repeaters and networks [Pirandola, arXiv:1601.00966]
- Single-hop multiuser networks (broadcast, multiple-access, interference channel) [Laurenza & Pirandola, arXiv:1603.07262]
- Quantum metrology and channel discrimination [Pirandola & Lupo, arXiv:1609.02160]
- Strong converse rates [Wilde, Tomamichel, Berta, arXiv:1602.08898] **– NEXT TALK**