Trade-off Capacities for Quantum Channels II:

Completing the Analogy between the Classical and Quantum Worlds

Mark M. Wilde

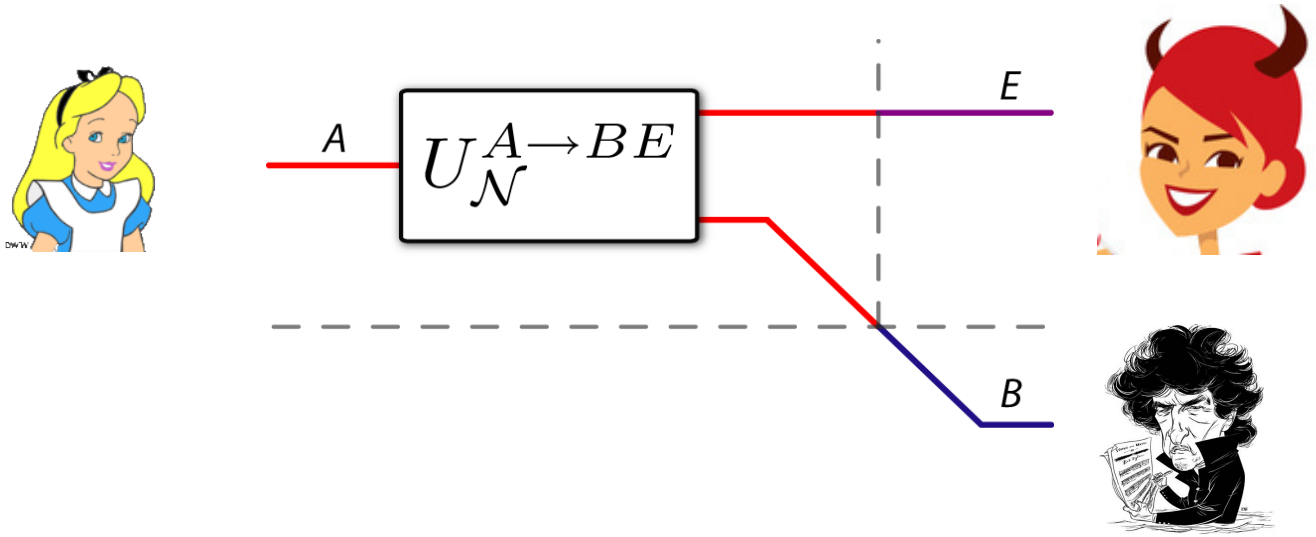
School of Computer Science
McGill University

2010 Spring Biannual meeting of INTRIQ,
Saint-Sauveur, Quebec, Canada,
Tuesday, June 8, 2010

Overview

- The **Many Uses** of a Quantum Channel
- The **full trade-off** between classical communication, quantum communication, and entanglement for a quantum channel
- The **Collins-Popescu Analogy**
- The **full trade-off** between
  public classical communication,
  private classical communication, and secret key
  for a quantum channel

The Many Uses of a Quantum Channel



Classical Data – Alice wishes to send “I love you” or “I don't love you”

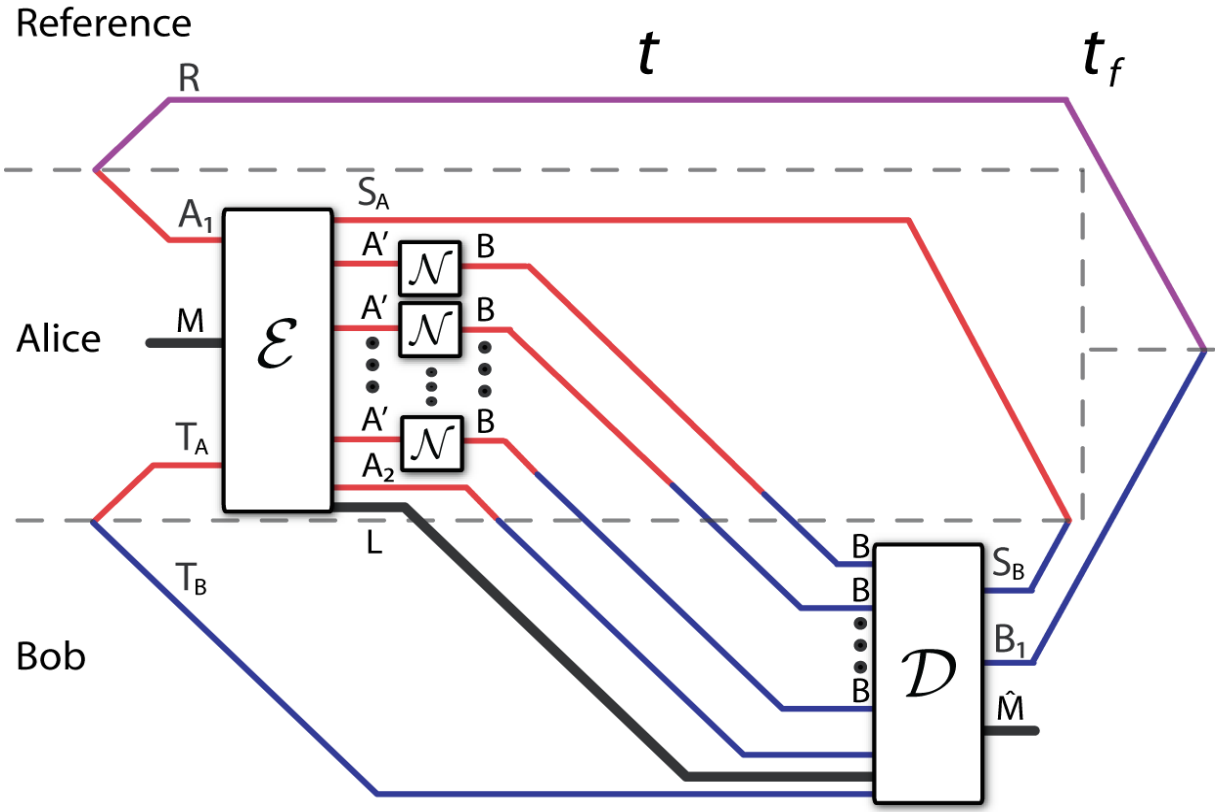
Quantum Data – Alice sends $\frac{1}{\sqrt{2}}(|\text{“I love you”}\rangle + |\text{“I don't love you”}\rangle)$

Private Classical Data – A concerned Alice sends “I love you” or “I don't love you” and doesn't want Eve to know

Assisting Resources – If Alice and Bob share any assisting resources such as entanglement or secret key, this can help

Can also **consume** or **generate** these resources in addition to using a quantum channel

First Setting: The CQE Setting



$$nC = \log|M| - \log|L|$$

$$nQ = \log|A_1| - \log|A_2|$$

$$nE = \log|S_A| - \log|T_A|$$

[1] Hsieh and Wilde. arXiv:0901.3038. Accepted in *IEEE Transactions on Information Theory*, 2010.
[2] Wilde and Hsieh. arXiv:1004.0458. The quantum dynamic capacity formula of a quantum channel.

Quantum Dynamic Capacity Theorem

The dynamic capacity region $\mathcal{C}_{CQE}(\mathcal{N})$ is

$$\mathcal{C}_{CQE}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{C}^{(1)}_{CQE}(\mathcal{N}^{\otimes k})}. \tag{1}$$

The "one-shot" region $\mathcal{C}^{(1)}_{CQE}(\mathcal{N})$ is

$$\mathcal{C}^{(1)}_{CQE}(\mathcal{N}) \equiv \bigcup_{\sigma} \mathcal{C}^{(1)}_{CQE,\sigma}(\mathcal{N}).$$

The "one-shot, one-state" region $\mathcal{C}^{(1)}_{CQE,\sigma}(\mathcal{N})$ is the set of all rates C, Q, and E, such that

$$C + 2Q \leq I(AX;B)_{\sigma}, \tag{2}$$

$$Q + E \leq I(A\rangle BX)_{\sigma}, \tag{3}$$

$$C + Q + E \leq I(X;B)_{\sigma} + I(A\rangle BX)_{\sigma}. \tag{4}$$

The above entropic quantities are with respect to a classical-quantum state σ^{XAB} where

$$\sigma^{XAB} \equiv \sum_{x} p(x) \left|x\right\rangle \left\langle x\right|^{X} \otimes \mathcal{N}^{A' \to B}(\phi_x^{AA'}). \tag{5}$$

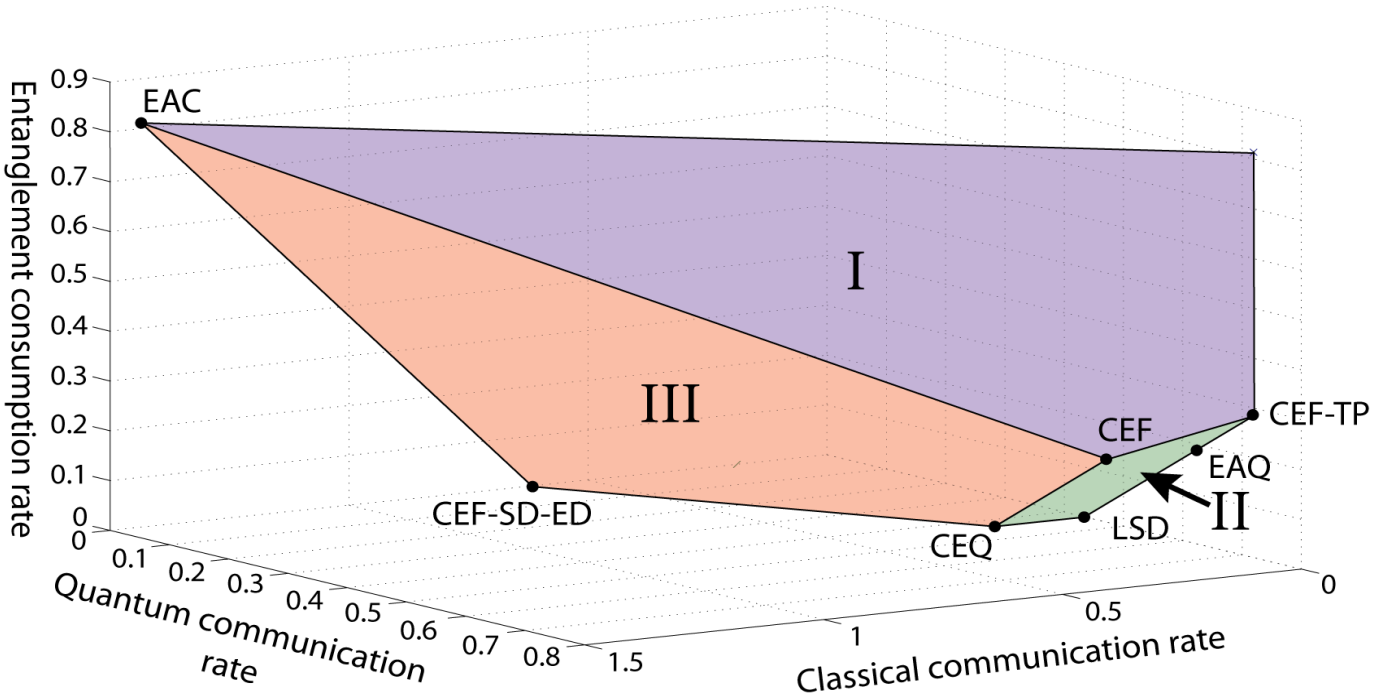
One should consider states on A'^k instead of A' when taking the regularization.

Achievability Proof

There exists a protocol for
entanglement-assisted classical and quantum communication
that achieves the following rates:

$$\langle \mathcal{N}^{A' \to B} \rangle + \frac{1}{2} I(A;E|X)_\sigma [qq] \geq \frac{1}{2} I(A;B|X)_\sigma [q \to q] + I(X;B)_\sigma [c \to c]$$

Combine this with teleportation, dense coding, and entanglement distribution...



Hsieh and Wilde. arXiv:0811.4227. Accepted in *IEEE Transactions on Information Theory*, 2010.

Converse Proof

Can prove using just the simplest tools:

Assume the existence of a good catalytic protocol

(The actual state is close to the ideal state)

Alicki-Fannes' inequality for continuity of entropic terms

(Entropies are close if states are close)

Quantum data processing inequality

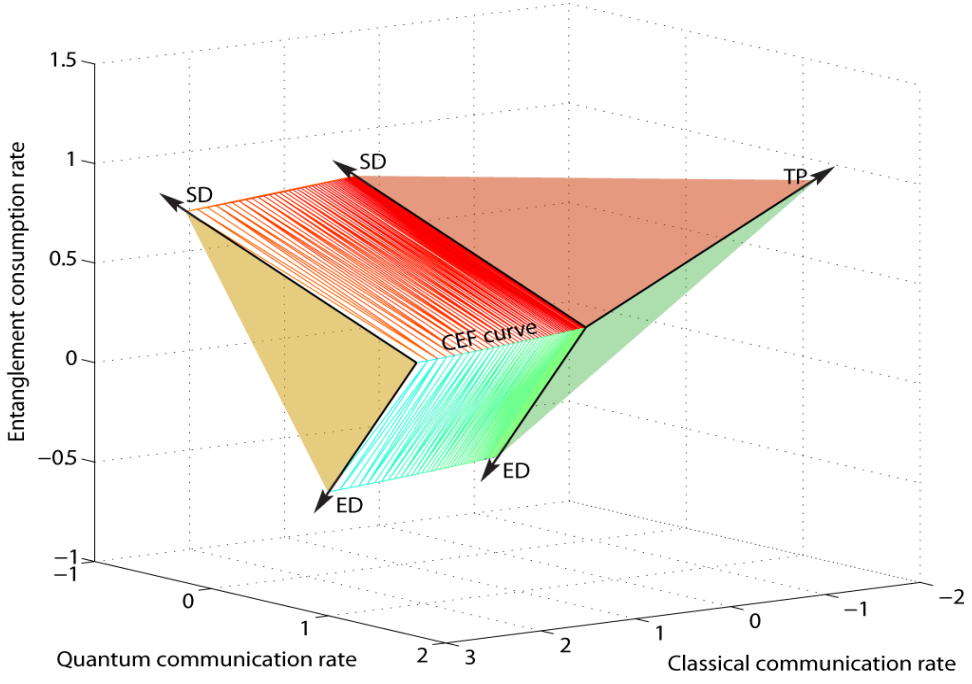
(Data processing cannot increase classical or quantum correlations)

Chain rule for quantum mutual information

Wilde and Hsieh. The quantum dynamic capacity formula of a quantum channel. arXiv:1004.0458.

Example CQE Regions

Dephasing Channel

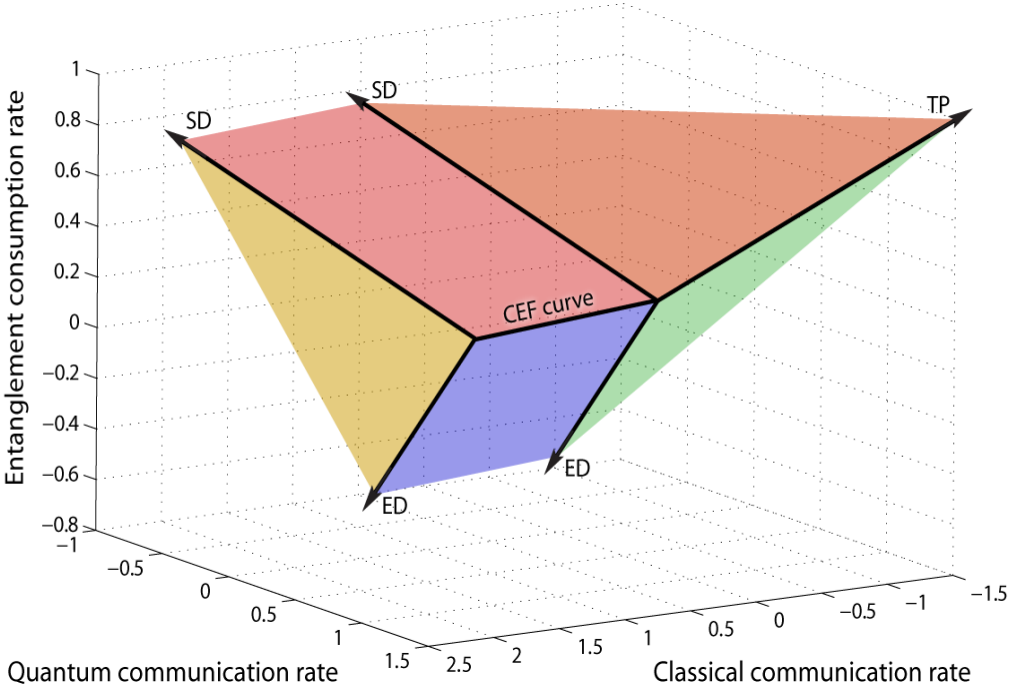


$$
\begin{aligned}
C + 2Q &\leq 1 + H_2(v) - H_2(\gamma(v,p)), \\
Q + E &\leq H_2(v) - H_2(\gamma(v,p)), \\
C + Q + E &\leq 1 - H_2(\gamma(v,p))
\end{aligned}
$$

$$
\gamma(v,p) \equiv \frac{1}{2} + \frac{1}{2}\sqrt{1 - 16 \cdot \frac{p}{2}\left(1 - \frac{p}{2}\right) v(1-v)}
$$

$$
v \in [0, 1/2]
$$

Erasure Channel



$$
\begin{aligned}
C + 2Q &\leq (1-\epsilon)(1 + H_2(p)), \\
Q + E &\leq (1-2\epsilon) H_2(p), \\
C + Q + E &\leq 1 - \epsilon - \epsilon H_2(p)
\end{aligned}
$$

$$
p \in [0, 1/2]
$$

The Collins-Popescu Analogy between the Classical and Quantum Worlds

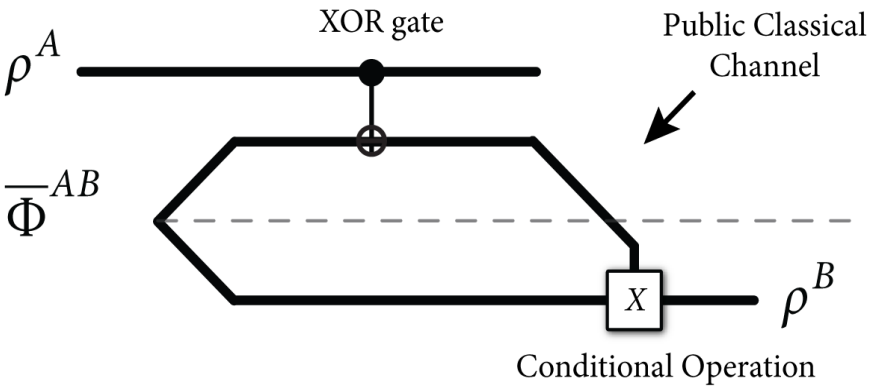
The way that certain **classical noiseless resources** interact is similar to the way that certain **quantum resources** interact

Classical Resources	Quantum Resources
Public classical communication	Classical communication
Secret Key	Entanglement
Private classical communication	Quantum communication

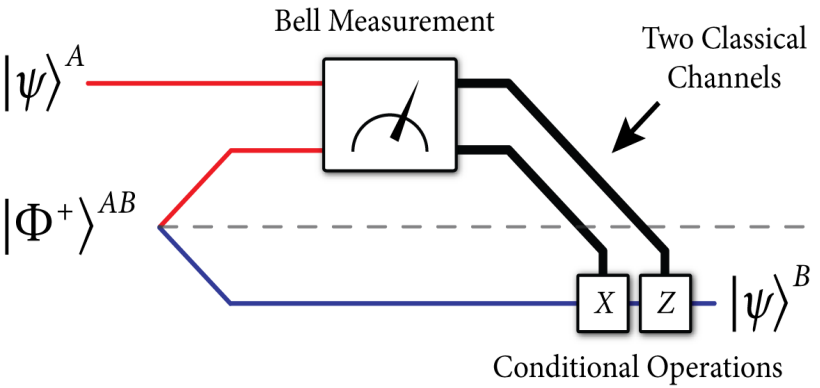
Collins and Popescu. Classical analog of entanglement. *Physical Review A,* 65(3):032321, February 2002.

Collins-Popescu Analogy (ctd.)

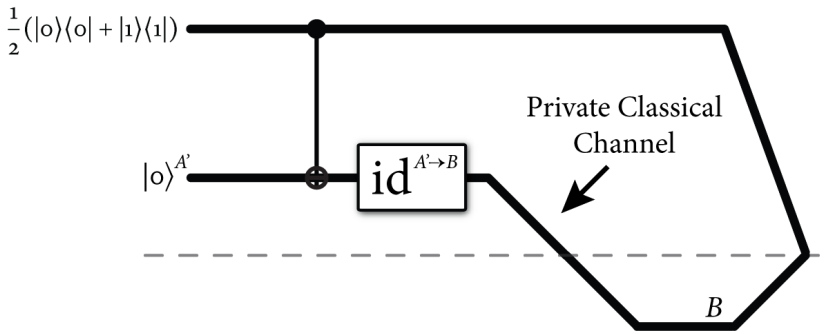
One-Time Pad



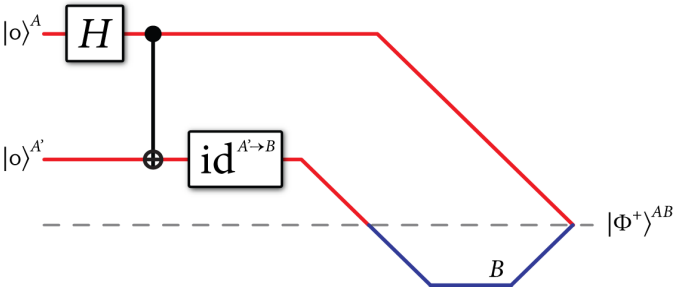
Teleportation



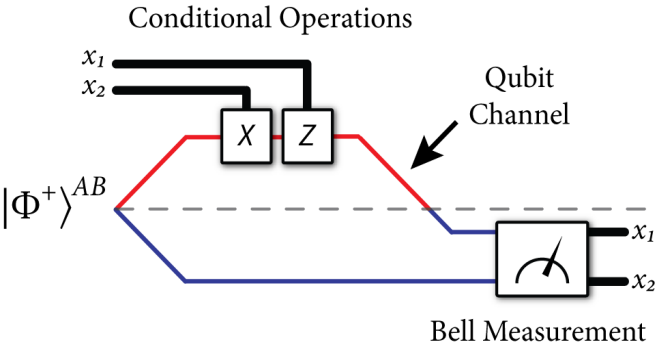
Secret Key Distribution



Entanglement Distribution



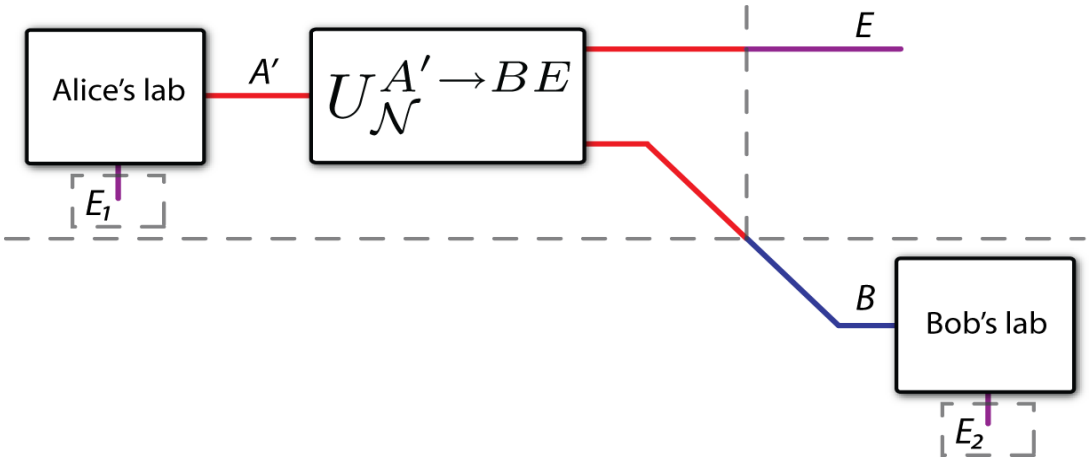
Super-dense Coding



?????????

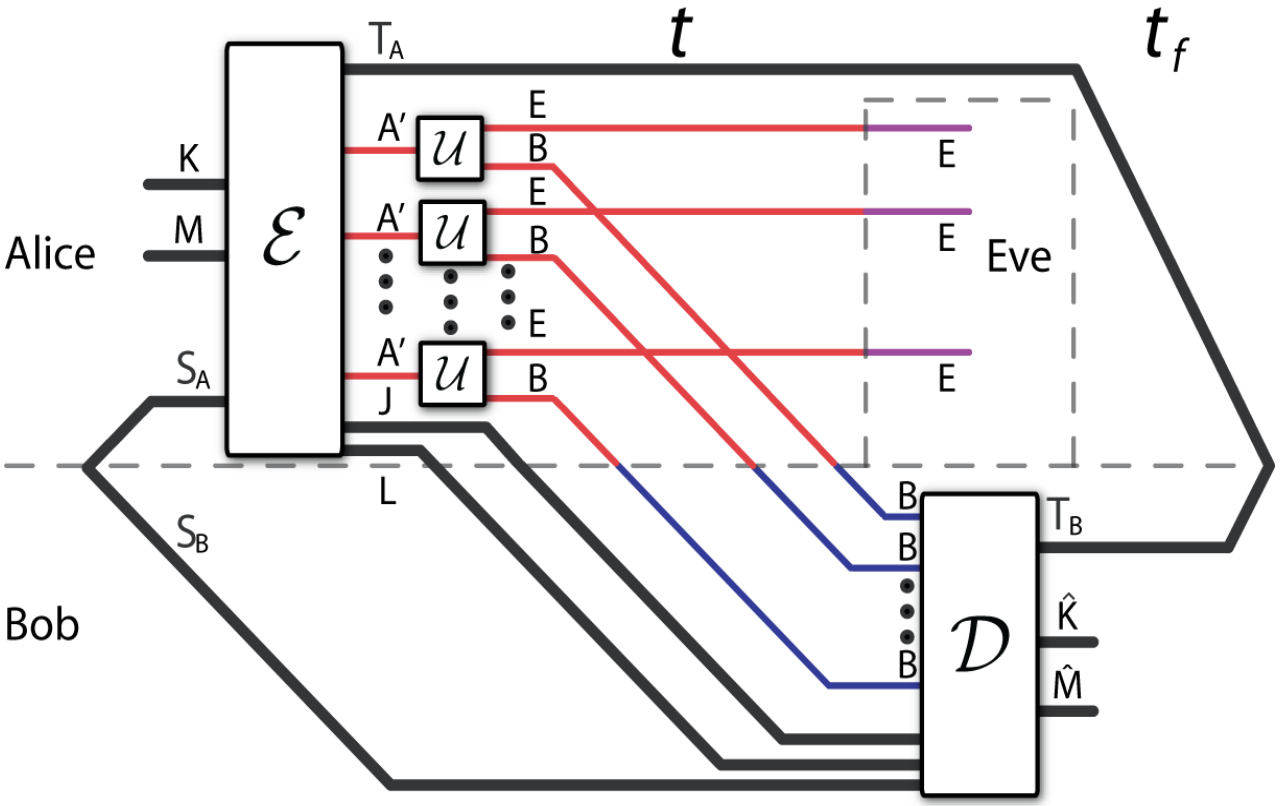
Collins-Popescu Analogy for Channels

We would expect a trade-off between
public classical communication,
private classical communication, and
secret key
to be similar to the CQE trade-off we just described



This holds for the above communication model,
but there are differences, and we will explicitly
see how the analogy breaks down....

Second Setting: The RPS Setting



$$nR = \log|K| - \log|L|$$
$$nP = \log|M| - \log|J|$$
$$nS = \log|T_A| - \log|S_A|$$

Wilde and Hsieh. Public and private resource trade-offs for a quantum channel. arXiv:1005.3818.

Private Dynamic Capacity Theorem

The private dynamic capacity region $\mathcal{C}_{RPS}(\mathcal{N})$ is equal

$$\mathcal{C}_{RPS}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{C}^{(1)}_{RPS}(\mathcal{N}^{\otimes k})}, \tag{1}$$

The "one-shot" region $\mathcal{C}^{(1)}_{RPS}(\mathcal{N})$ is

$$\mathcal{C}^{(1)}_{RPS}(\mathcal{N}) \equiv \bigcup_{\sigma} \mathcal{C}^{(1)}_{RPS,\sigma}(\mathcal{N}).$$

The "one-shot, one-state" region $\mathcal{C}^{(1)}_{RPS,\sigma}(\mathcal{N})$ is the set of all rates R, P, and S such that

$$R + P \leq I(YX;B)_{\sigma}, \tag{2}$$

$$P + S \leq I(Y;B|X)_{\sigma} - I(Y;E|X)_{\sigma}, \tag{3}$$

$$R + P + S \leq I(YX;B)_{\sigma} - I(Y;E|X)_{\sigma}. \tag{4}$$

The above entropic quantities are with respect to a classical-quantum state σ^{XYBE} where

$$\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x,y) |x\rangle\langle x|^{X} \otimes |y\rangle\langle y|^{Y} \otimes U_{\mathcal{N}}^{A' \to BE}(\rho^{A'}_{x,y}), \tag{5}$$

One should consider states on A'^{k} instead of A' when taking the regularization.

Achievability Proof

There exists a protocol for
secret-key-assisted public and private classical communication
that achieves the following rates:

$$\langle \mathcal{N} \rangle + I(Y;E|X)_\sigma [cc]_{\text{priv}} \geq I(Y;B|X)_\sigma [c \to c]_{\text{priv}} + I(X;B)_\sigma [c \to c]_{\text{pub}}$$

Combine this with the
one-time pad,
private-to-public transmission,
and **secret key distribution**...

Hsieh and Wilde. Public and private communication with a quantum channel and a secret key. *Physical Review A* 80, 022306 (2009)

Converse Proof

Can **again** prove using just the simplest tools:

Assume the existence of a good catalytic protocol

(The actual state is close to the ideal state)

Alicki-Fannes' inequality for continuity of entropic terms

(Entropies are close if states are close)

Quantum data processing inequality

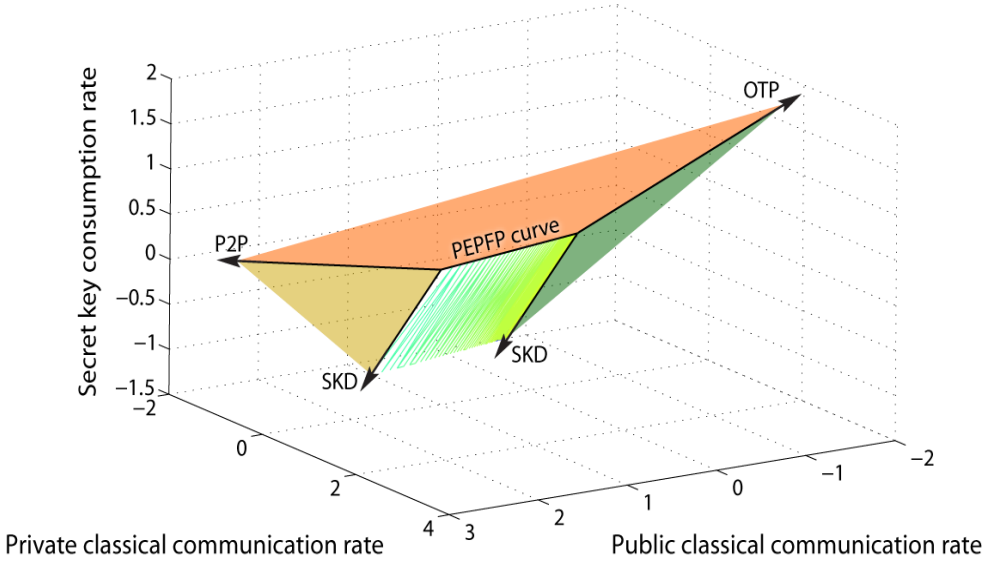
(Data processing cannot increase classical or quantum correlations)

Chain rule for quantum mutual information

Wilde and Hsieh. Public and private resource trade-offs for a quantum channel. arXiv:1005.3818.

Example RPS Regions

Dephasing Channel

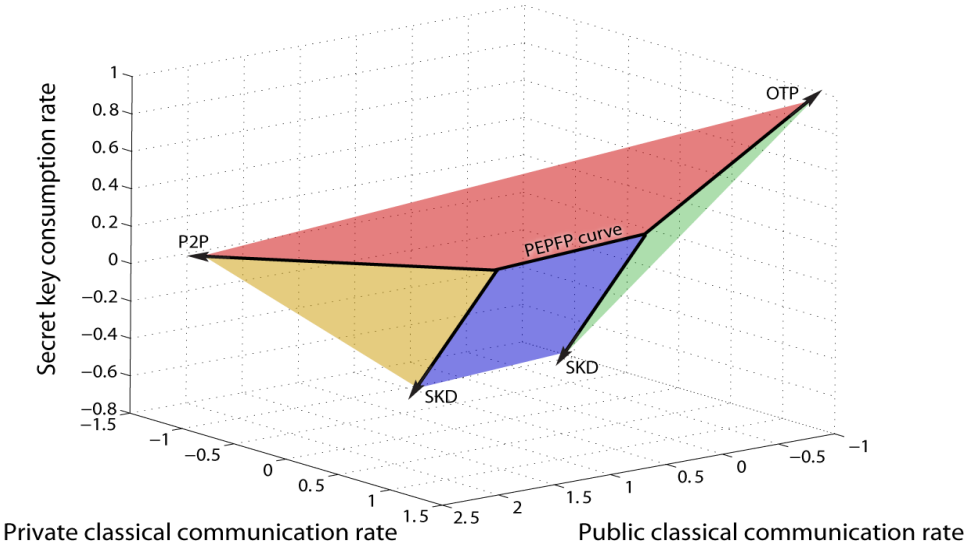


$$
\begin{aligned}
R+P &\leq 1, \\
P+S &\leq H_2(v) - H_2(\gamma(v,p)), \\
R+P+S &\leq 1 - H_2(\gamma(v,p))
\end{aligned}
$$

$$
\gamma(v,p) \equiv \frac{1}{2} + \frac{1}{2}\sqrt{1 - 16 \cdot \frac{p}{2}\left(1 - \frac{p}{2}\right) v(1-v)}
$$

$$
v \in [0, 1/2]
$$

Erasure Channel



$$
\begin{aligned}
R+P &\leq (1-\epsilon), \\
P+S &\leq (1-2\epsilon) H_2(p), \\
R+P+S &\leq 1 - \epsilon - \epsilon H_2(p)
\end{aligned}
$$

$$
p \in [0, 1/2]
$$

Conclusion and Open Questions

Open question: Other examples of channels for which we can compute the capacity regions?

Open question: Complete the Collins-Popescu analogy for the case of a shared state?

Open question: Other interesting trade-offs?

Open question: Trade-offs in network quantum Shannon theory?

Open question: Could the inequalities here correspond to some fundamental physical law?