Trading Resources in Quantum Communication

Mark M. Wilde

School of Computer Science
McGill University

Joint work with **Min-Hsiu Hsieh**
in arXiv:0811.4227, 0901.3038, 0903.3920, 1004.0458, 1005.3818

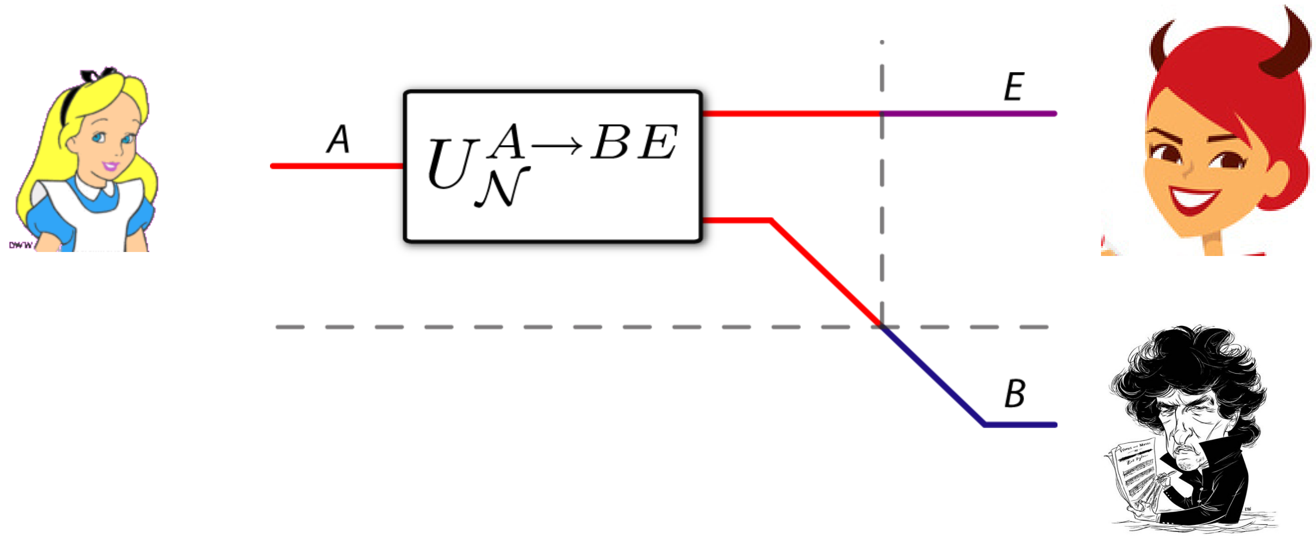
Joint work with **Kamil Bradler, Dave Touchette** and **Patrick Hayden**
1001.1732

Seminar for the Institute for Quantum Information
Caltech, Pasadena, California
Friday, August 6, 2010

Overview

- The **Many Uses** of a Quantum Channel (a review)
- 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”

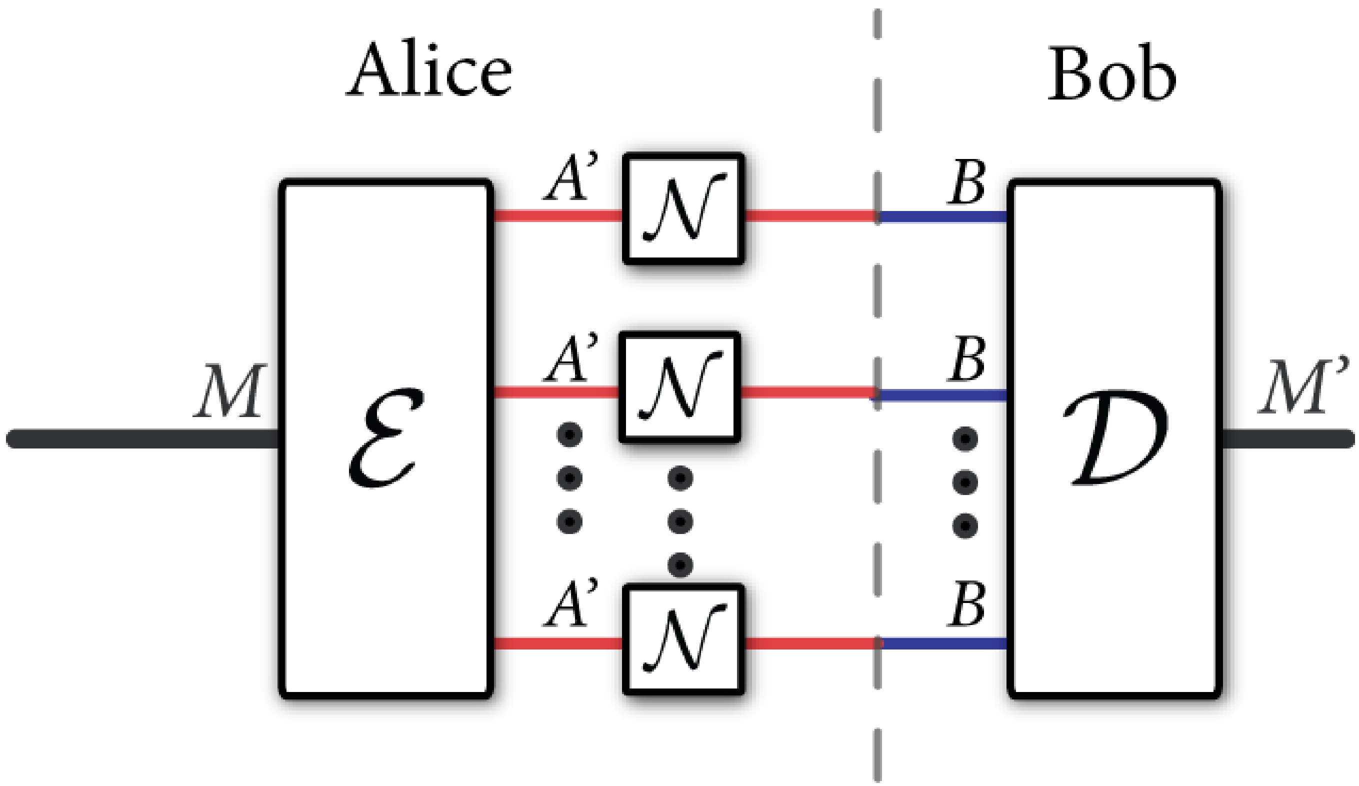
Quantum Data – Alice sends $\frac{1}{\sqrt{2}}(|\text{“I love you”}\rangle + |\text{“I don't love you”}\rangle)$

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

Sending Classical Information over a Quantum Channel (ctd.)



Encoder just maps classical signal to a **tensor product state**

Decoder performs a measurement over all the output states to determine transmitted classical signal

Sending Classical Information over a Quantum Channel

Coding Strategy

(similar to that for classical case)

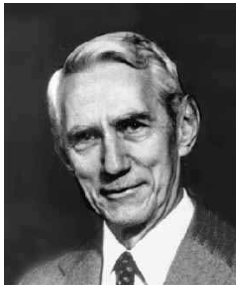
Use a quantum channel many times so that law of large numbers comes into play

Code randomly with an ensemble of the following form:

$$\{p(x), \rho_x^{A'}\}_{x \in \mathcal{X}}$$

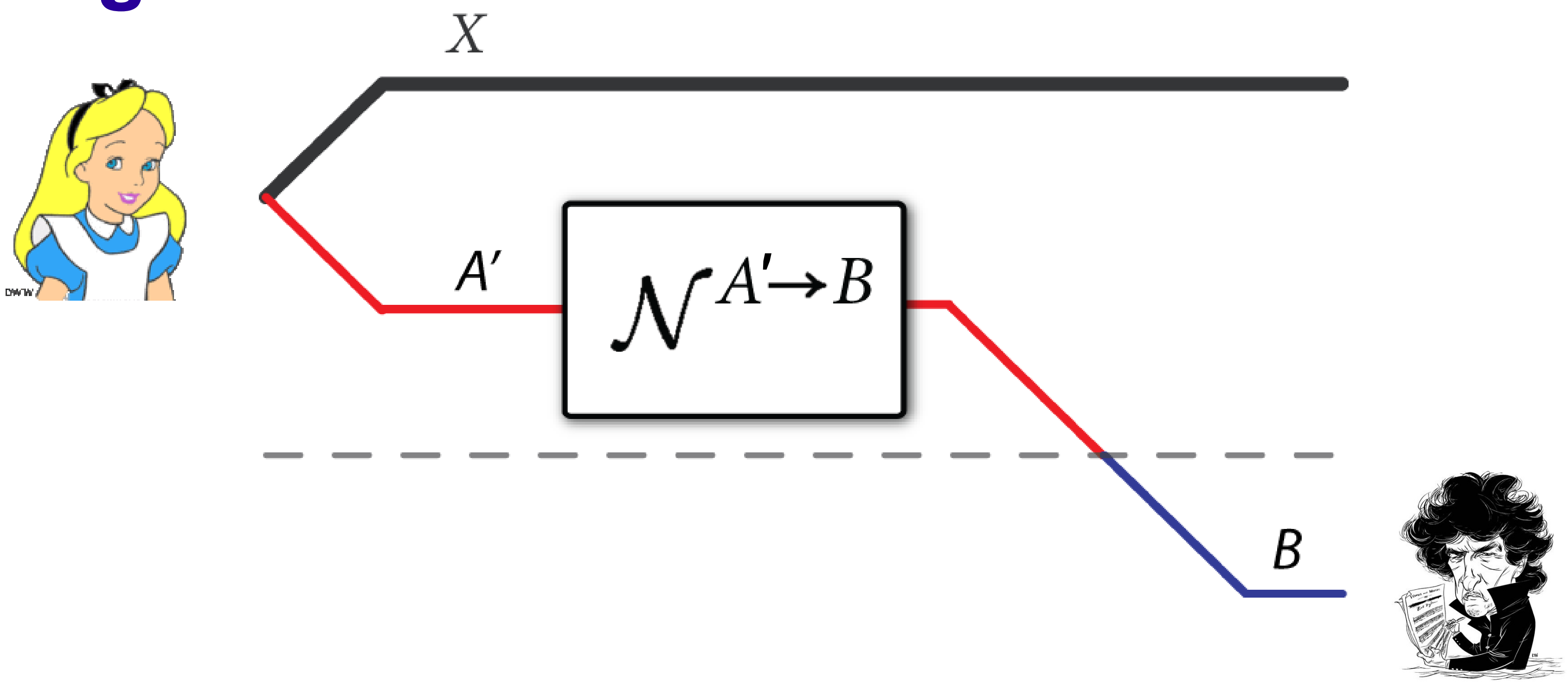
Channel input states are **product states**

Allow for small error but show that the error vanishe
large block length



Holevo, IEEE Trans. Inf. Theory, 44, 269-273 (1998).
Schumacher & Westmoreland, PRA, 56, 131-138 (1997).

Sending Classical Data over Quantum Channels



Correlate classical data with quantum states:

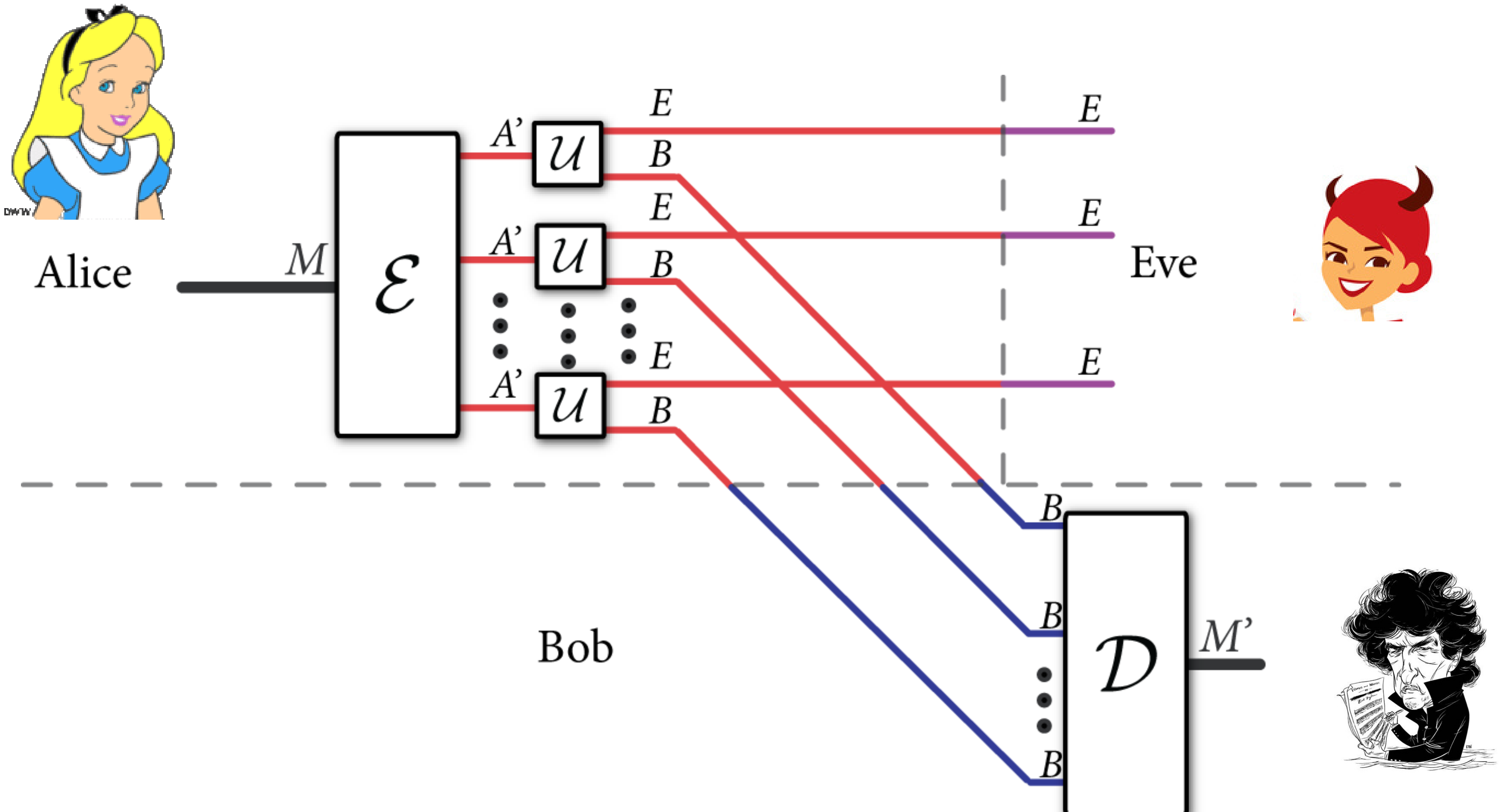
$$\sum_x p_X(x) |x\rangle\langle x|^X \otimes \mathcal{N}^{A'\to B}(\phi_x^{A'})$$

Holevo information of a quantum channel:

$$\chi(\mathcal{N}) \equiv \max_{\{p_X(x),\phi_x\}} I(X;B)$$

Holevo (1998), Schumacher and Westmoreland (1997)

Sending Private Data over Quantum Channels

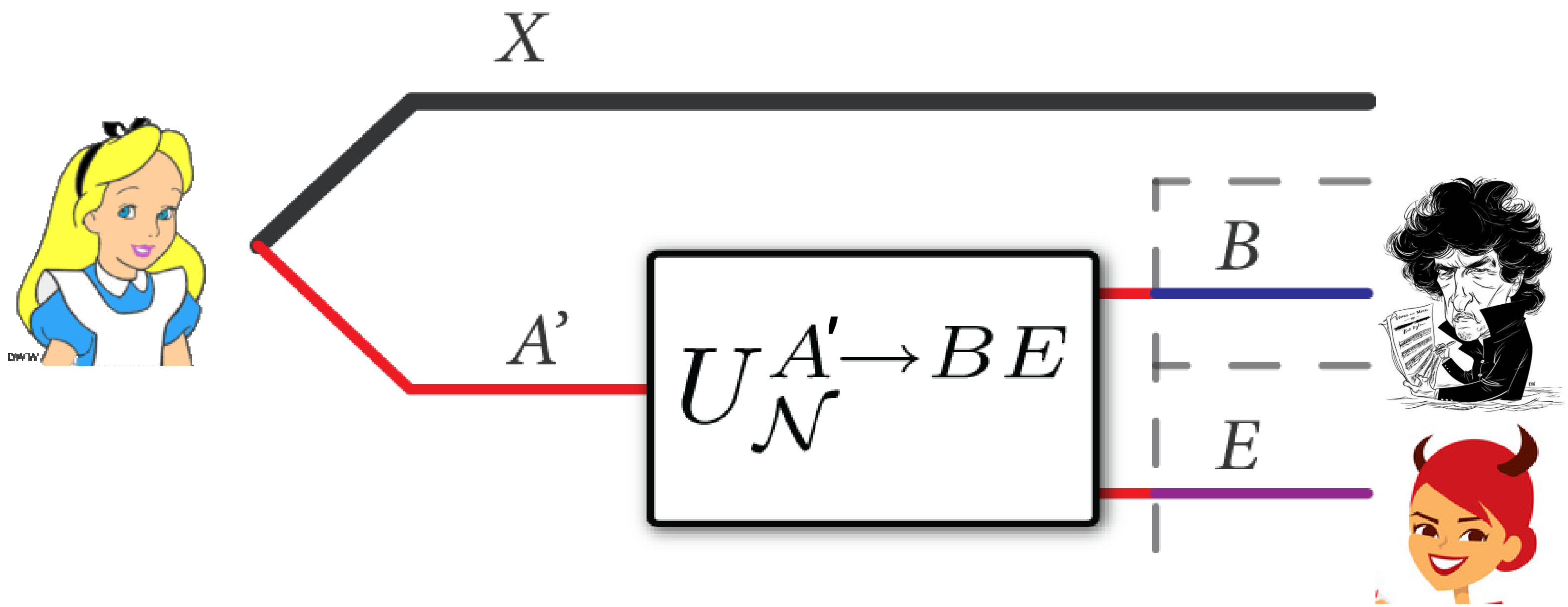


Encoder just maps classical signal to a **tensor product state**

Decoder performs a measurement over all the output states to determine transmitted classical signal

Devetak (2005), Cai, Winter, Yeung (2004)

Sending Private Data over Quantum Channels



Correlate classical data with channel input

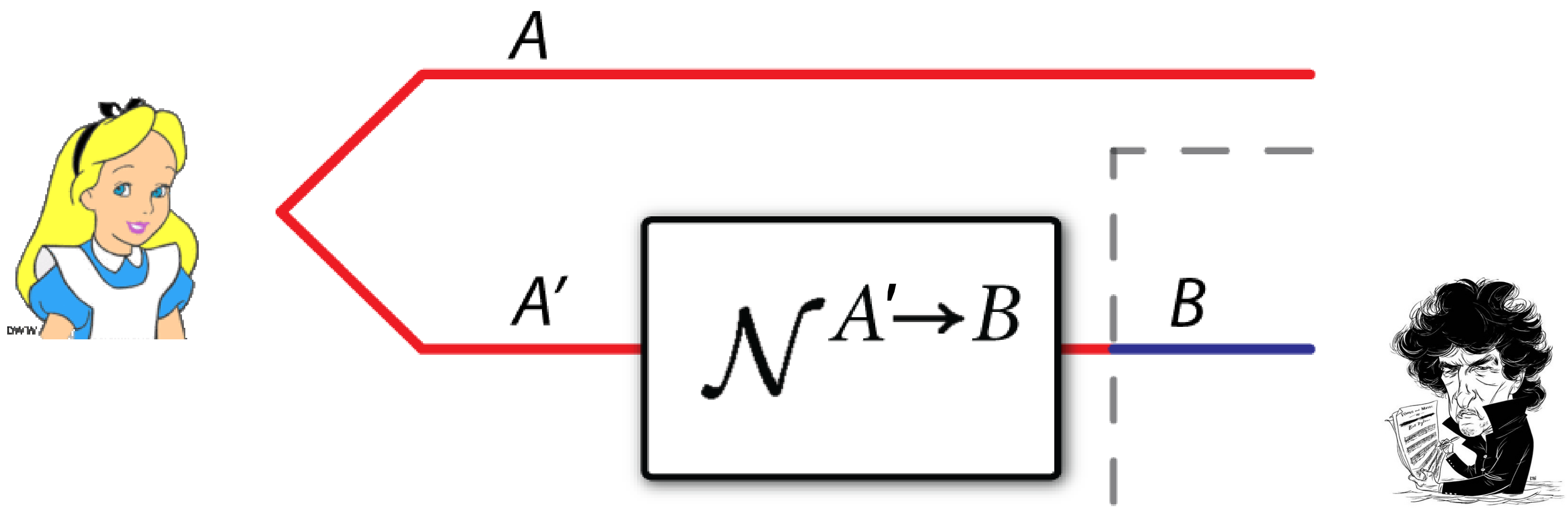
$$\sum_x p_X(x)|x\rangle\langle x|^X \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_x^{A'})$$

Private information of a quantum channel:

$$P(\mathcal{N}) \equiv \max_{\{p_X(x),\rho_x\}} I(X;B) - I(X;E)$$

Devetak (2005), Cai, Winter, Yeung (2004)

Sending Quantum Data over Quantum Channels



Preserving entanglement is the same as transmitting quantum data

$$\mathcal{N}^{A'\to B}(\phi^{AA'})$$

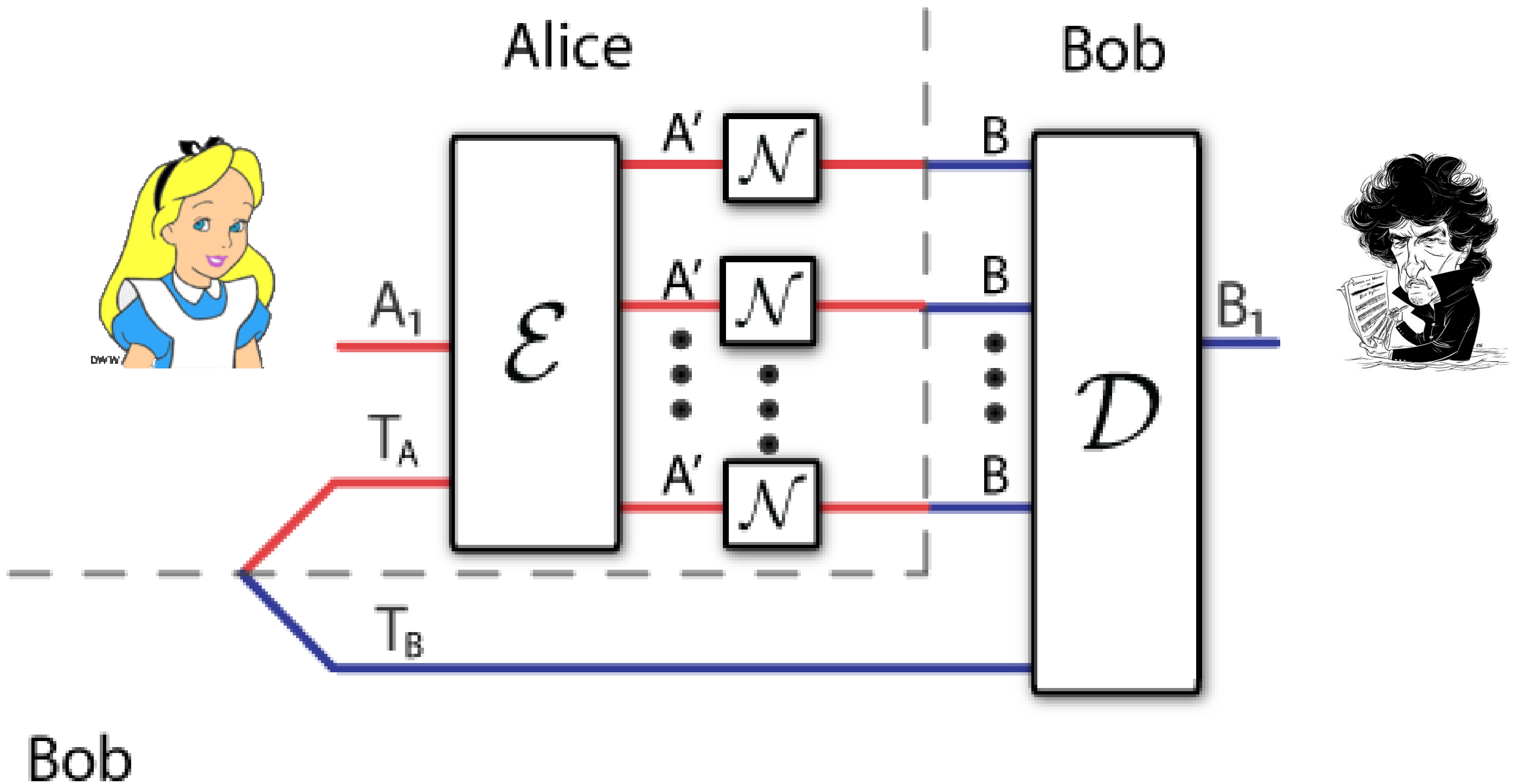
Coherent information of a quantum channel:

$$Q(\mathcal{N}) \equiv \max_{\phi} I(A\rangle B)$$

where $$I(A\rangle B) \equiv H(B) - H(AB)$$

Lloyd (1997), Shor (2002), Devetak (2005)

Sending Quantum Data with Entanglement Assistance



Encoder is a random unitary mapping

Decoder decouples from Eve the quantum information Alice would like to protect

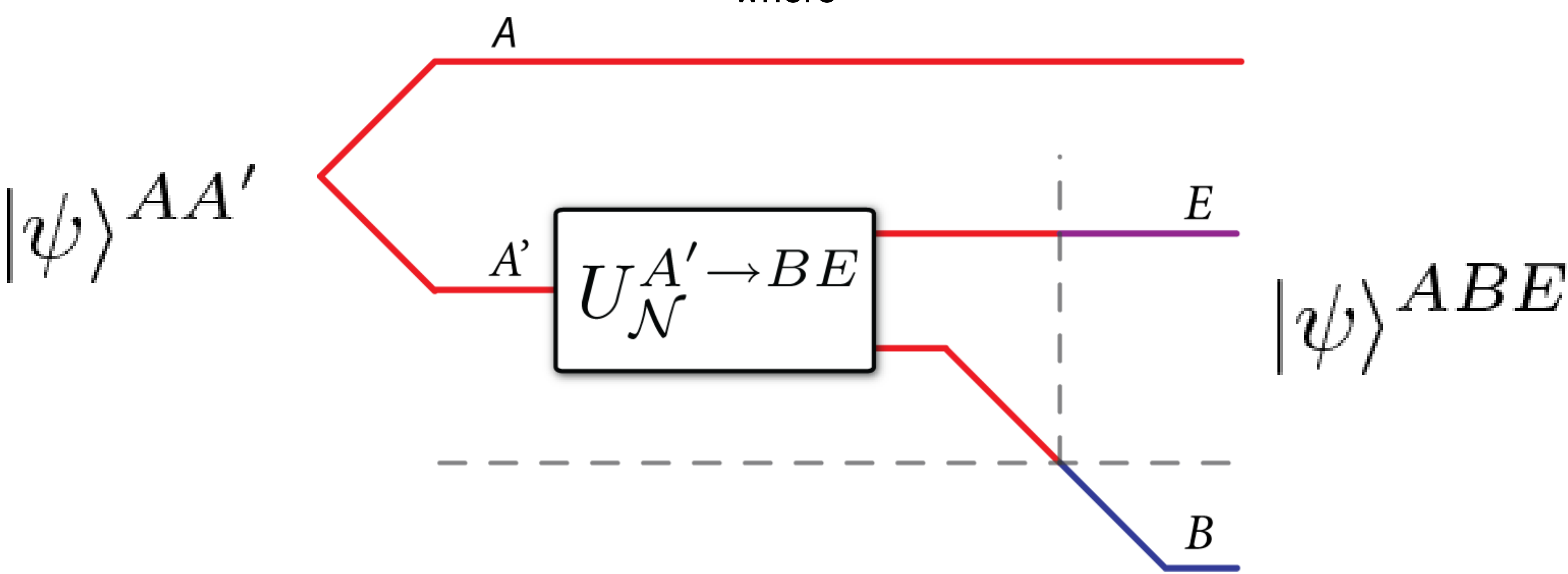
Devetak, Harrow, Winter, IEEE Trans. Information Theory vol. 54, no. 10, pp. 4587-4618, Oct 2008
Devetak, Harrow, Winter, Phys. Rev. Lett., 93, 230504 (2004).

Father Protocol

Can achieve the following resource inequality:

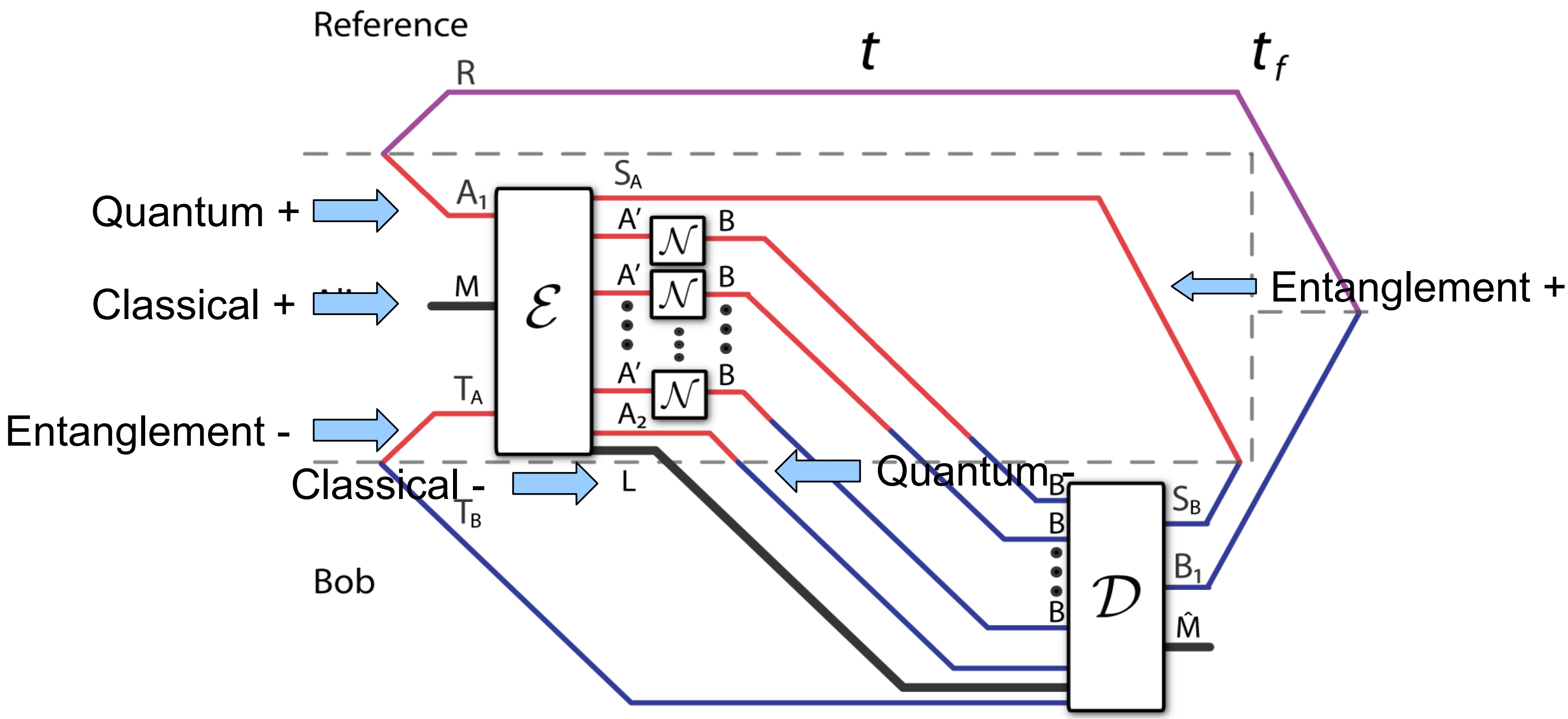
$$\langle \mathcal{N}^{A' \to B} \rangle + \frac{1}{2} I(A;E)_\psi [qq] \geq \frac{1}{2} I(A;B)_\psi [q \to q]$$

where



Devetak, Harrow, Winter, IEEE Trans. Information Theory vol. 54, no. 10, pp. 4587-4618, Oct 2008
Devetak, Harrow, Winter, Phys. Rev. Lett., 93, 230504 (2004).

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. *IEEE Transactions on Information Theory*, September 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

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

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

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

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

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

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

Achievability Proof

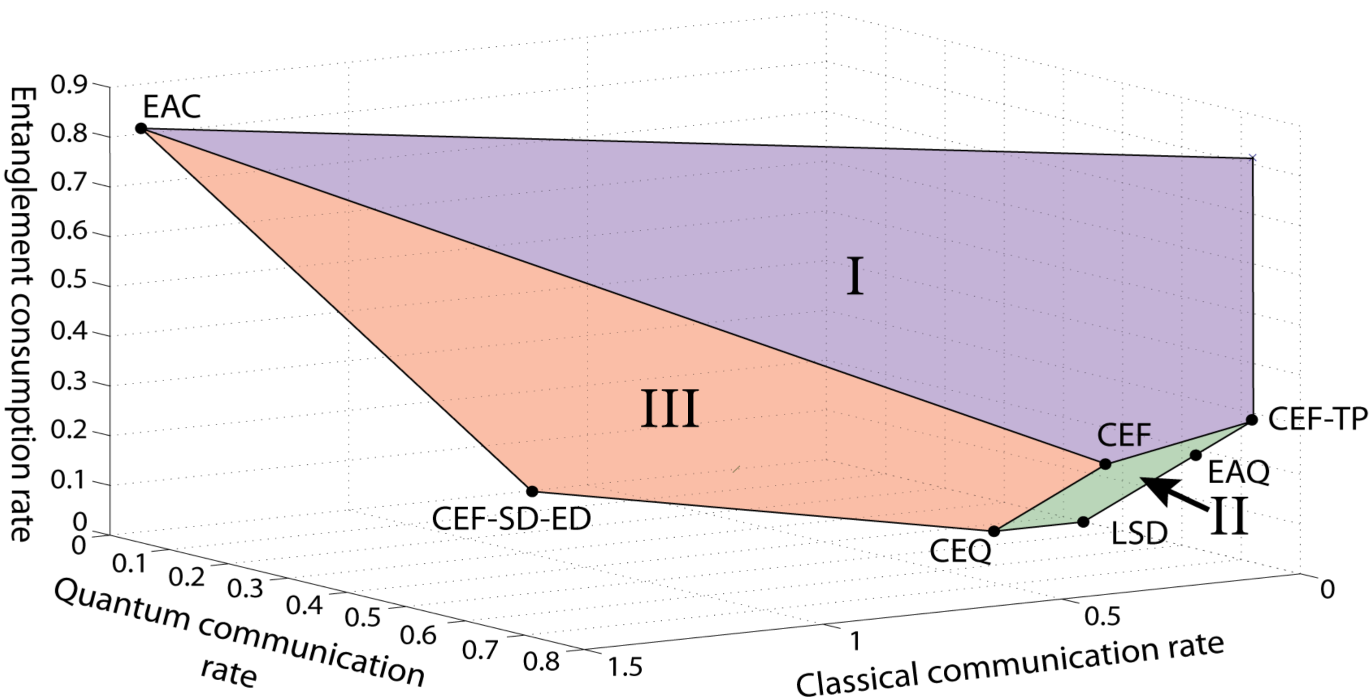
There exists a protocol for

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. *IEEE Transactions on Information Theory*, September 2010.

Father Code Definitions

Unencoded State:

$$|\varphi\rangle^{RA_1} \otimes |\Phi\rangle^{T_A T_B}$$

where

$$|\varphi\rangle^{RA_1} \equiv \sum_{k=1}^{2^{nQ}} \alpha_k |k\rangle^R |k\rangle^{A_1}, \quad |\Phi\rangle^{T_A T_B} \equiv \frac{1}{\sqrt{2^{nE}}} \sum_{m=1}^{2^{nE}} |m\rangle^{T_A} |m\rangle^{T_B}$$

Encoded State:

$$\mathcal{E}^{A_1 T_A \to A'^n} \left(|\varphi\rangle^{RA_1} \otimes |\Phi\rangle^{T_A T_B} \right) = \sum_{k=1}^{2^{nQ}} \alpha_k |k\rangle^R |\phi_k\rangle^{A'^n T_B}$$

$$|\phi_k\rangle^{A'^n T_B} \equiv \frac{1}{\sqrt{2^{nE}}} \sum_{m=1}^{2^{nE}} |\phi_{k,m}\rangle^{A'^n} |m\rangle^{T_B}$$

$$|\phi_{k,m}\rangle^{A'^n} \equiv \mathcal{E}^{A_1 T_A \to A'^n} \left(|k\rangle^{A_1} |m\rangle^{T_A} \right)$$

Hsieh and Wilde, IEEE Trans. Inf. Theory, September 2010.

Random Father Codes

Random father code is an ensemble of father codes:

$$\{p_{\mathcal{C}}, \mathcal{C}\}$$

Expected
code density operator:

$$\overline{\rho}^{A'^n T_B} \equiv \mathbb{E}_{\mathcal{C}}\left\{\rho^{A'^n T_B}(\mathcal{C})\right\}$$

Expected
channel input density operator:

$$\overline{\rho}^{A'^n} \equiv \mathbb{E}_{\mathcal{C}}\left\{\rho^{A'^n}(\mathcal{C})\right\}$$

Can make expected input close to a **tensor power state!**

$$\left\|\overline{\rho}^{A'^n} - \rho^{\otimes n}\right\|_1 \leq \epsilon$$

HSW coding theorem accepts tensor product input states!

Hsieh and Wilde, IEEE Trans. Inf. Theory, September 2010.

“Piggybacking” Classical Information

Given an ensemble: $\{p_x, \rho_x^{A'}\}$

Given a typical input sequence: x^n

Can rewrite typical input sequence as follows:

$$x^n \rightarrow \underbrace{x_1 \cdots x_1}_{n[p_{x_1} - \delta]} \underbrace{x_2 \cdots x_2}_{n[p_{x_2} - \delta]} \cdots \underbrace{x_{|\mathcal{X}|} \cdots x_{|\mathcal{X}|}}_{n[p_{x_{|\mathcal{X}|}} - \delta]} x_g$$

Choose |*X*| father codes each with

Quantum communication rate:

$$\frac{1}{2} I(A;B)_{\phi_x}$$

Entanglement Consumption rate:

$$\frac{1}{2} I(A;E)_{\phi_x}$$

Devetak and Shor, Communications in Mathematical Physics, 256, 287-303 (2005)

Hsieh and Wilde, IEEE Trans. Inf. Theory, September 2010.

"Piggybacking" Classical Information (ctd.)

"Pasted" random father code has total rates:

Total Quantum Communication rate:

$$\frac{1}{2} I\left(A;B|X\right)_{\sigma} = \sum_{x \in \mathcal{X}} p\left(x\right) \frac{1}{2} I\left(A;B\right)_{\phi_x}$$

Total Entanglement Consumption rate:

$$\frac{1}{2} I\left(A;E|X\right)_{\sigma} = \sum_{x \in \mathcal{X}} p\left(x\right) \frac{1}{2} I\left(A;E\right)_{\phi_x}$$

Can piggyback classical information with rate

$$I\left(X;B\right)_{\sigma}$$

By the **HSW coding theorem**

Devetak and Shor, Communications in Mathematical Physics, 256, 287-303 (2005)
Hsieh and Wilde, IEEE Trans. Inf. Theory, September 2010.

Proof Strategy for Coding Theorem

Random Coding

Show that **expectation of average classical error probability** and **quantum error** over all random classically-enhanced father codes is small

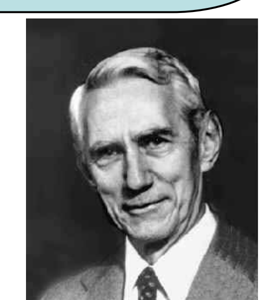
Derandomization

Pick one that has small error.

Expurgation

Remove the father codes from the classically-enhanced father code that **classical error probability**. Ensures that resulting code has low maxim probability.

Hey, that's my idea!!!!



Hsieh and Wilde, IEEE Trans. Inf. Theory, September 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.

Computing Boundary Points

To find a boundary point, consider **parallel planes** and find the plane that just "**kisses**" the boundary of the capacity region

Can phrase this task as a **convex optimization program:**

$$\max_{C,Q,E,p(x),\phi_x} \quad w_C C + w_Q Q + w_E E$$

subject to

$$\begin{aligned} C + 2Q &\leq I(AX;B^n)_\sigma, \\ Q + E &\leq I(A\rangle B^n X)_\sigma, \\ C + Q + E &\leq I(X;B^n)_\sigma + I(A\rangle B^n X)_\sigma, \end{aligned}$$

where

$$\sigma^{XAB^n} \equiv \sum_x p(x)|x\rangle\langle x|^X \otimes \mathcal{N}^{A'^n \to B^n}(\phi_x^{AA'^n})$$

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

Computing Boundary Points (Ctd.)

The **Lagrangian** of this convex optimization program is

$$\mathcal{L}\left(C, Q, E, p_X\left(x\right), \phi_x^{AA'^n}, \lambda_1, \lambda_2, \lambda_3\right)$$

and equal to

$$\begin{aligned} w_C C + w_Q Q + w_E E + \lambda_1 \left(I\left(AX; B^n\right)_\sigma - \left(C + 2Q\right)\right) \\ + \lambda_2 \left(I\left(A\rangle B^n X\right)_\sigma - \left(Q + E\right)\right) \\ + \lambda_3 \left(I\left(X; B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma - \left(C + Q + E\right)\right) \end{aligned}$$

Its **Lagrangian dual** is

$$g\left(\lambda_1, \lambda_2, \lambda_3\right) \equiv \sup_{C, Q, E, p(x), \phi_x^{AA'^n}} \mathcal{L}\left(C, Q, E, p_X\left(x\right), \phi_x^{AA'^n}, \lambda_1, \lambda_2, \lambda_3\right)$$

Wilde and Hsieh. The quantum dynamic capacity formula of a quantum channel. arXiv:1004.0458
Boyd and Vandenberghe. Convex Optimization. 2004

The Quantum Dynamic Capacity Formula

The **Lagrangian dual** splits into two different optimizations:

$$\sup_{C,Q,E} \left(w_C - \lambda_1 - \lambda_3\right) C + \left(w_Q - 2\lambda_1 - \lambda_2 - \lambda_3\right) Q + \left(w_E - \lambda_2 - \lambda_3\right) E$$

$$+\lambda_1 \left(\max_{p(x),\phi_x^{AA'n}} I\left(AX;B^n\right)_\sigma + \frac{\lambda_2}{\lambda_1} I\left(A\rangle B^n X\right)_\sigma + \frac{\lambda_3}{\lambda_1}\left(I\left(X;B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma\right)\right)$$

The second part we call
the **quantum dynamic capacity formula**

If it **single-letterizes**, then the Lagrangian dual simplifies,
implying that the *original convex optimization program is tractable*!

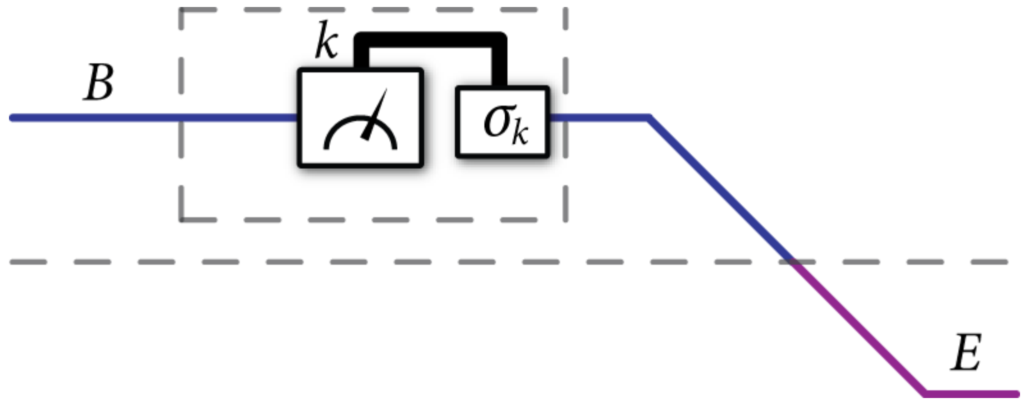
For some channels, we can even get **analytic solutions**

Wilde and Hsieh. The quantum dynamic capacity formula of a quantum channel. ArXiv:1004.0458
Boyd and Vandenberghe. Convex Optimization. 2004

Channels with Single-Letter Capacity Regions

Hadamard channel:

Degradable, and the degrading map to Eve is entanglement-breaking



Examples: dephasing channel, cloning channel, Unruh channel

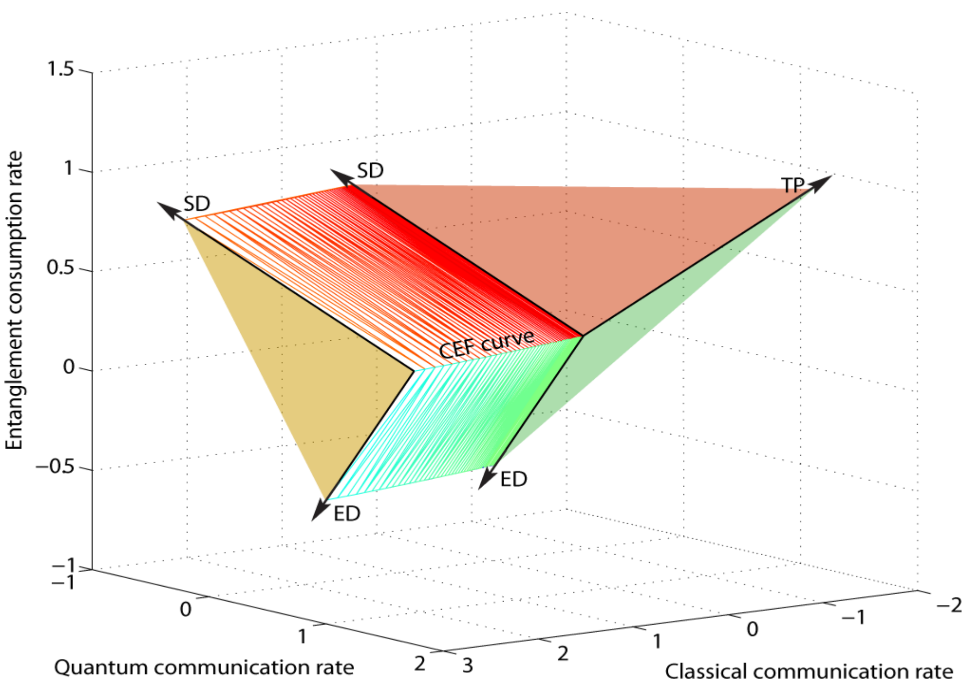
Erasure channel:

With some probability give state to Bob and erasure flag to Eve.
With complementary prob., give state to Eve and flag to Bob.

King, Matsumoto, Nathanson, Ruskai. Markov Processes and Related Fields, 13(2):391-423, 2007.
Hsieh and Wilde (2010), Bradler, Hayden, Touchette, Wilde (2010)

Example CQE Regions

Dephasing Channel

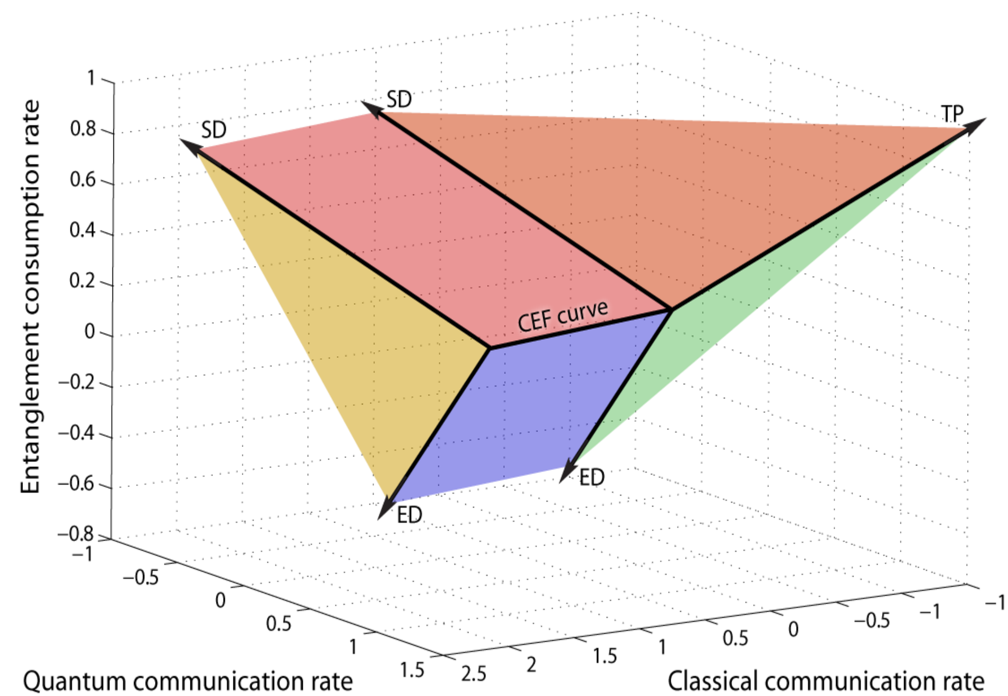


$$
\begin{aligned}
C + 2Q &\leq 1 + H_2(\nu) - H_2(\gamma(\nu, p)), \\
Q + E &\leq H_2(\nu) - H_2(\gamma(\nu, p)), \\
C + Q + E &\leq 1 - H_2(\gamma(\nu, p))
\end{aligned}
$$

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

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

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

Public classical communication

Secret Key

Private classical communication

Quantum Resources

Classical communication

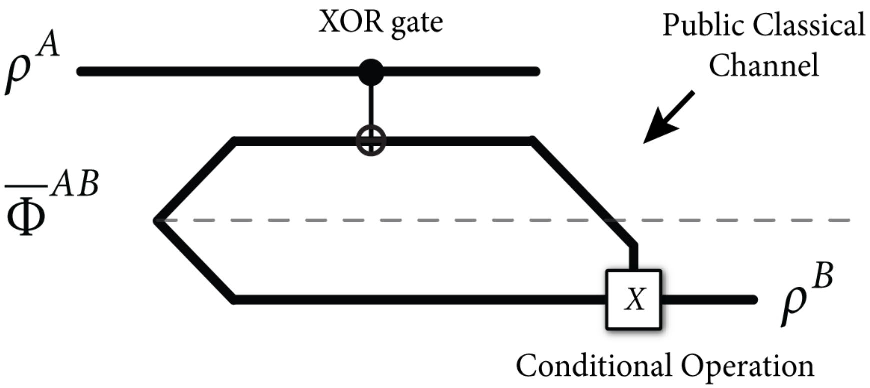
Entanglement

Quantum communication

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

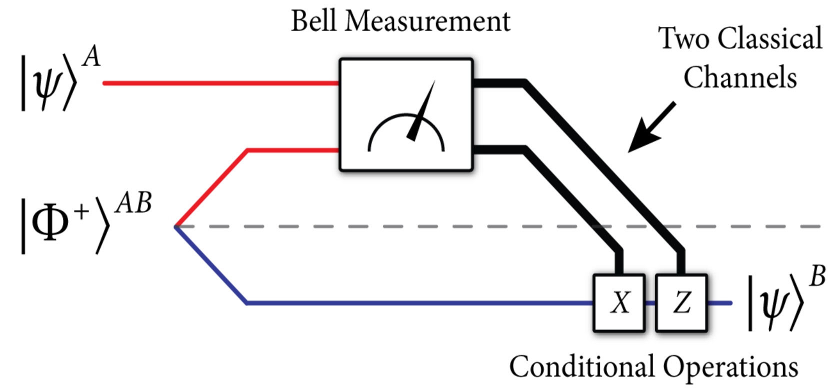
Collins-Popescu Analogy (ctd.)

One-Time Pad

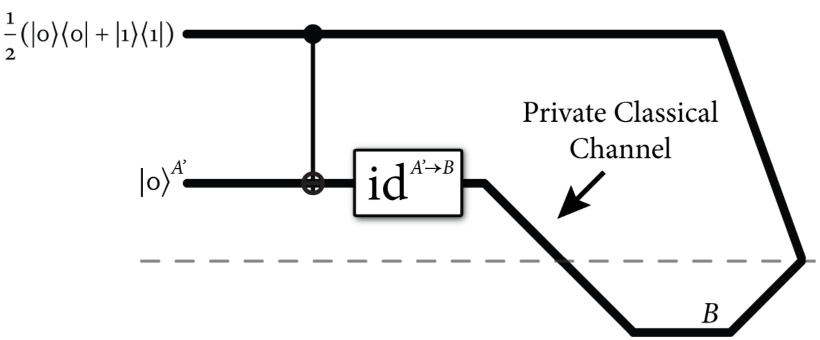


⟺

Teleportation

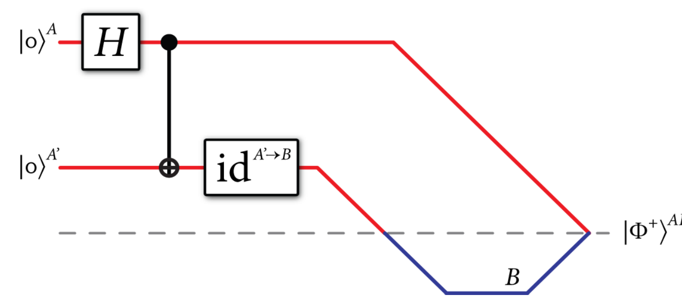


Secret Key Distribution



⟺

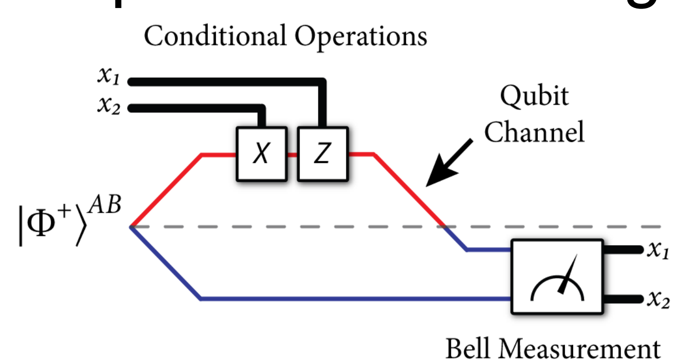
Entanglement Distribution



Super-dense Coding

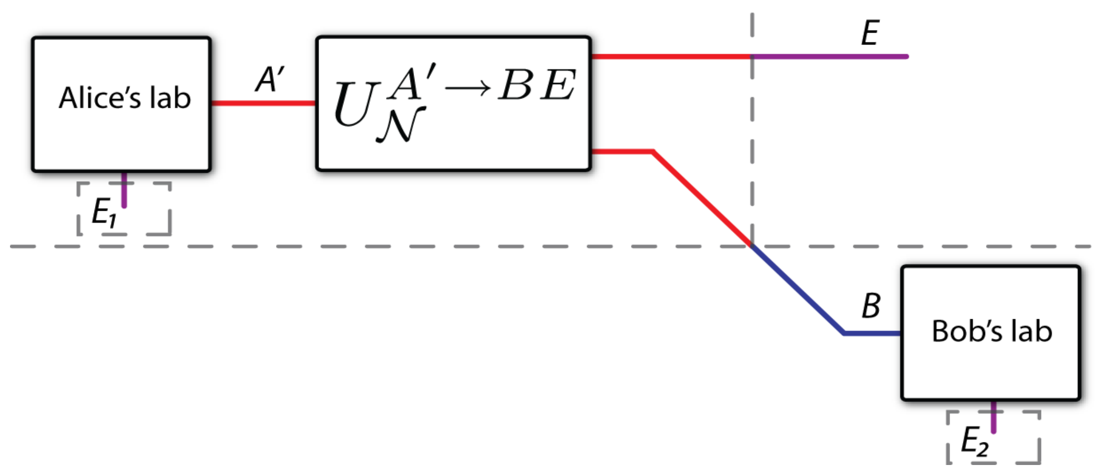
?????????

⟺



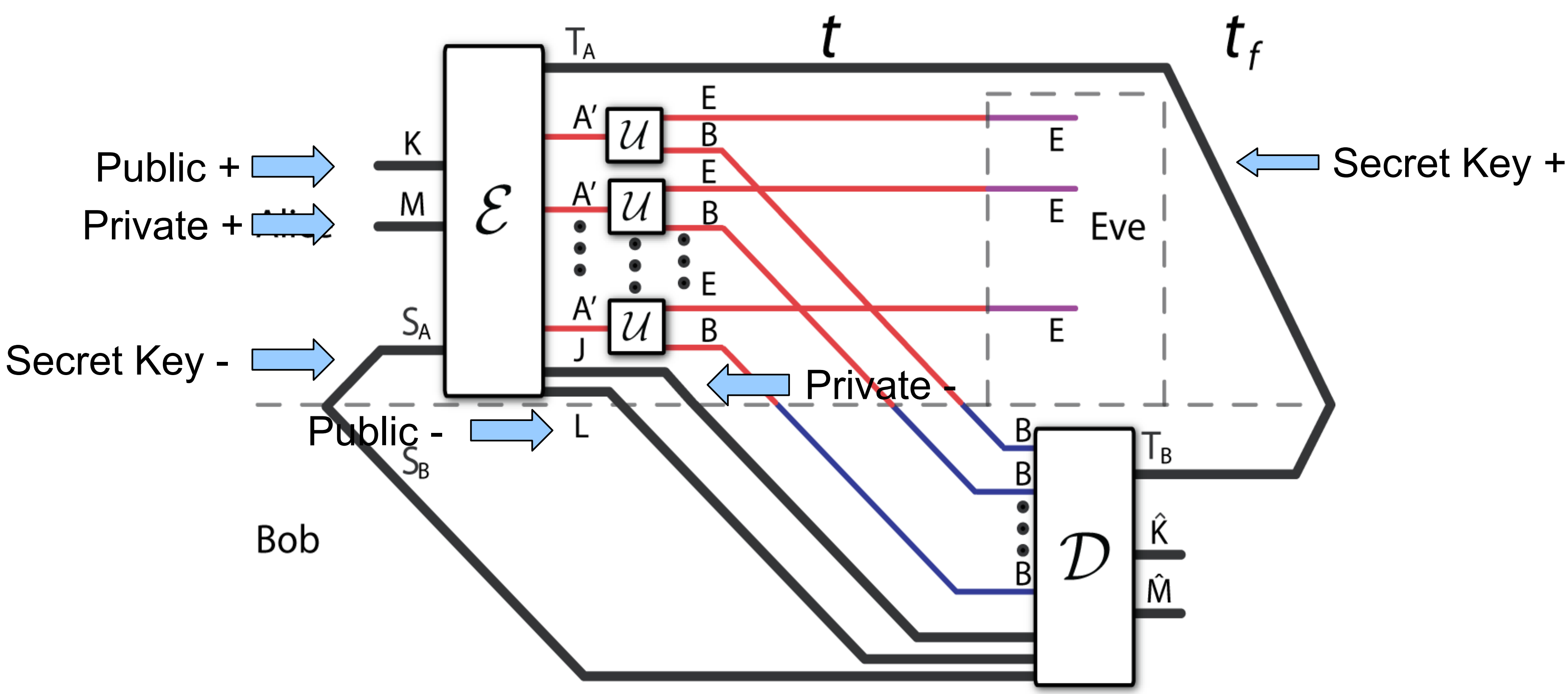
Collins-Popescu Analogy for Channels

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

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

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

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

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

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

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

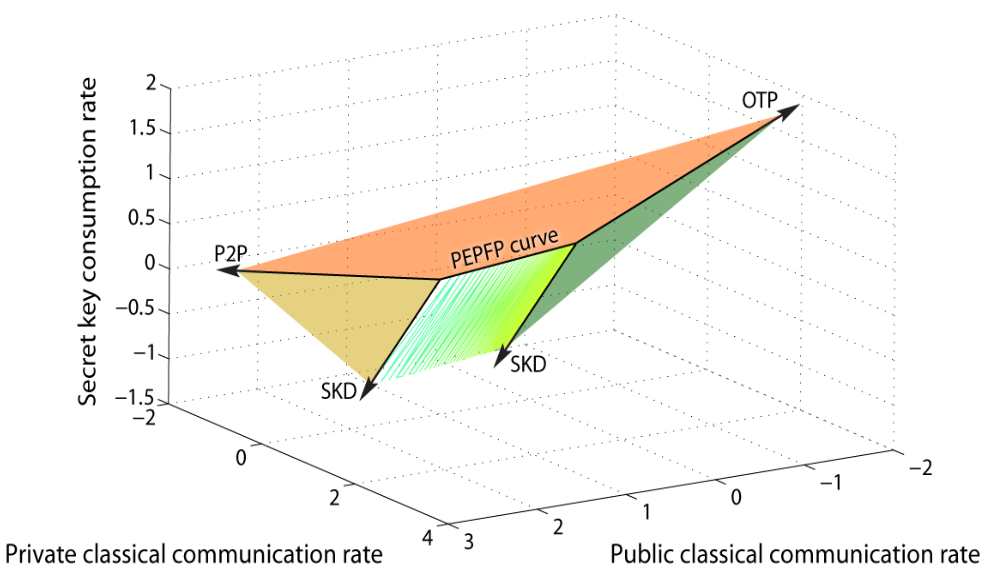
(Data processing cannot increase classical or quantum correlations)

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



$$R + P \leq 1,$$

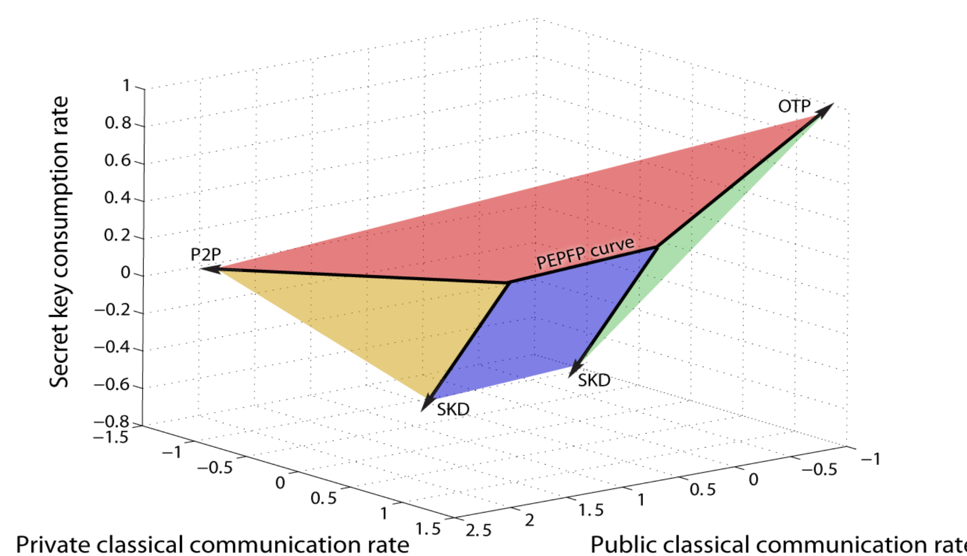
$$P + S \leq H_2(\nu) - H_2(\gamma(\nu, p)),$$

$$R + P + S \leq 1 - H_2(\gamma(\nu, p))$$

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

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

Erasure Channel



$$R + P \leq (1 - \epsilon),$$

$$P + S \leq (1 - 2\epsilon) H_2(p),$$

$$R + P + S \leq 1 - \epsilon - \epsilon H_2(p)$$

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

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: Trade-offs in network quantum Shannon theory?

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