# Entanglement Cost of Quantum Channels

*Mario Berta*, *Fernando Brandao, Matthias Christandl, Stephanie Wehner*

-

*Full version: IEEE Transactions on Information Theory, vol. 59, no. 10, pages 6779-6795, 2013*

# Outline

- *Quantum information theory: quantum channel capacities and quantum channel simulations*.

# Outline

- *Quantum information theory: quantum channel capacities and quantum channel simulations.*
- *Main result: entanglement cost of quantum channels.*
- *Idea of the proof.*

# Outline

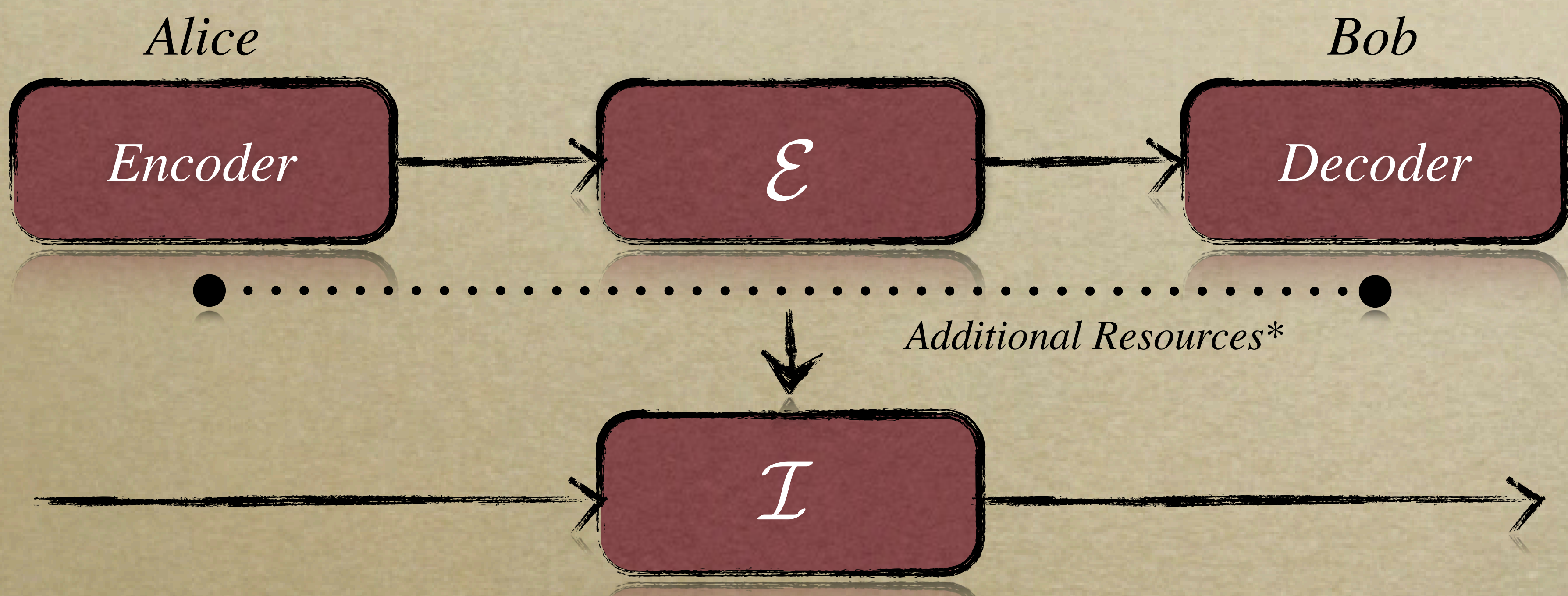
- *Quantum information theory: quantum channel capacities and quantum channel simulations.*
- *Main result: entanglement cost of quantum channels.*
- *Idea of the proof.*
- *Application: an upper bound on the strong converse quantum capacity.*
- *Application: security in the noisy-storage model.*

# Quantum Information Theory: Quantum Capacities of Quantum Channels

- *<u>Quantum Information theory</u>: independent and identical distribution (iid) + interested in asymptotic rates (quantum Shannon theory):* $\rho^{\otimes n}, \mathcal{E}^{\otimes n}$.

# Quantum Information Theory: Quantum Capacities of Quantum Channels

- *<u>Quantum Information theory</u>: independent and identical distribution (iid) + interested in asymptotic rates (quantum Shannon theory):* $\rho^{\otimes n}, \mathcal{E}^{\otimes n}$.

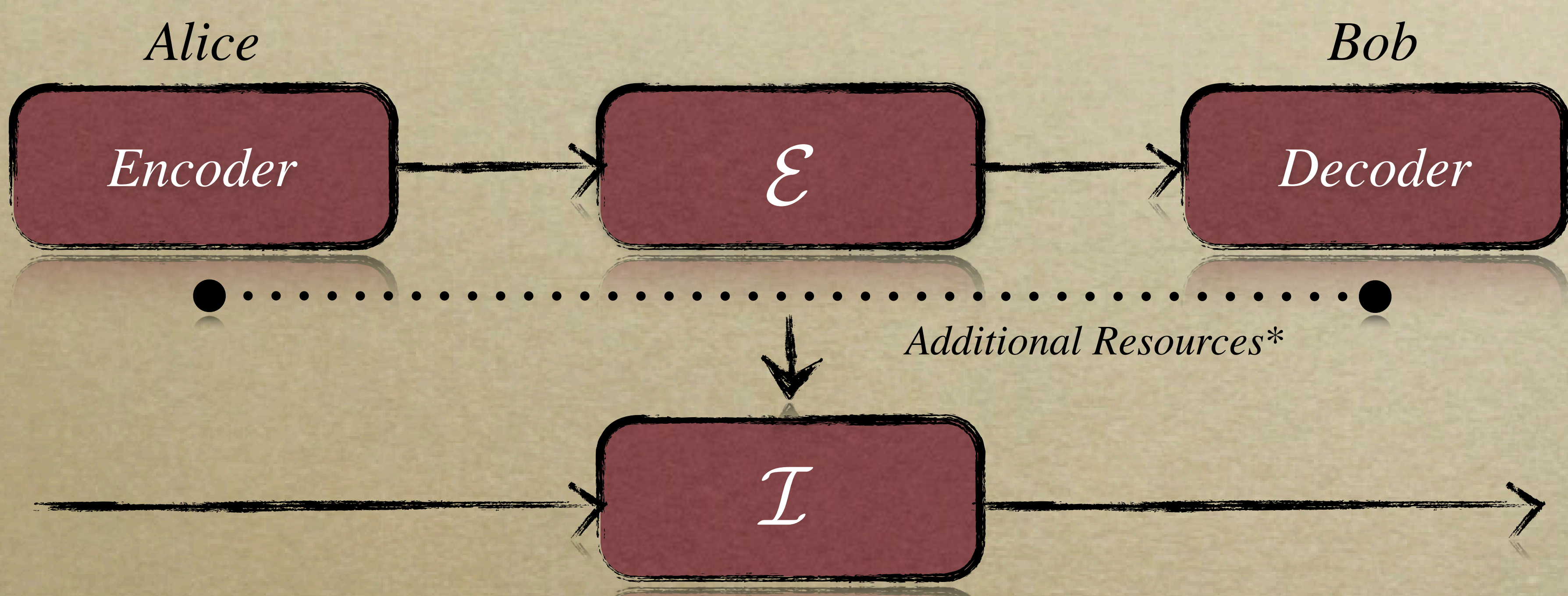



**E.g. entanglement, classical communication (forward, backward, two-way)*

- *How many qubits can Alice transmit on average per use of the channel (asymptotically)?*

# Quantum Information Theory: Quantum Capacities of Quantum Channels

- *Quantum Information theory: independent and identical distribution (iid) + interested in asymptotic rates (quantum Shannon theory):* $\rho^{\otimes n}, \mathcal{E}^{\otimes n}$.

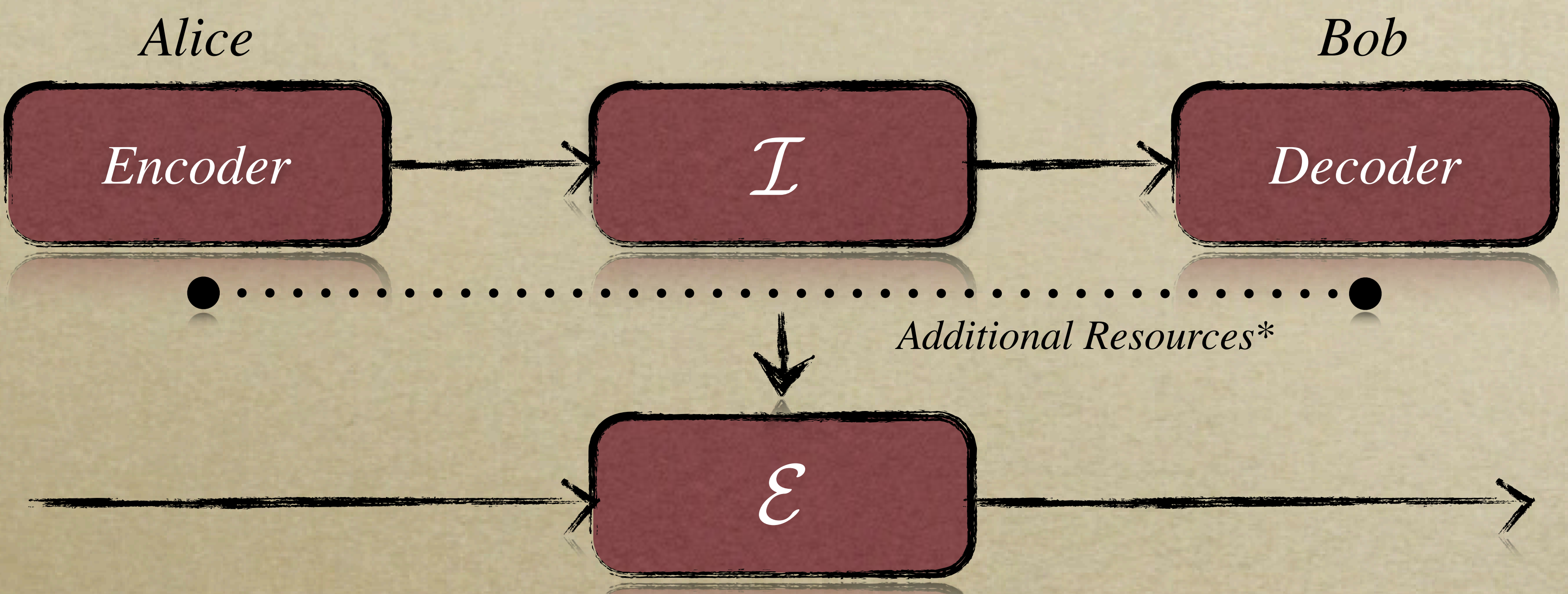



**E.g. entanglement, classical communication (forward, backward, two-way)*

- *How many qubits can Alice transmit on average per use of the channel (asymptotically)?*
- *Quantum channel capacities (quantum Shannon theorem) [...]:*

$$Q, Q_E, Q_{\rightarrow}, Q_{\leftarrow}, Q_{\leftrightarrow}$$

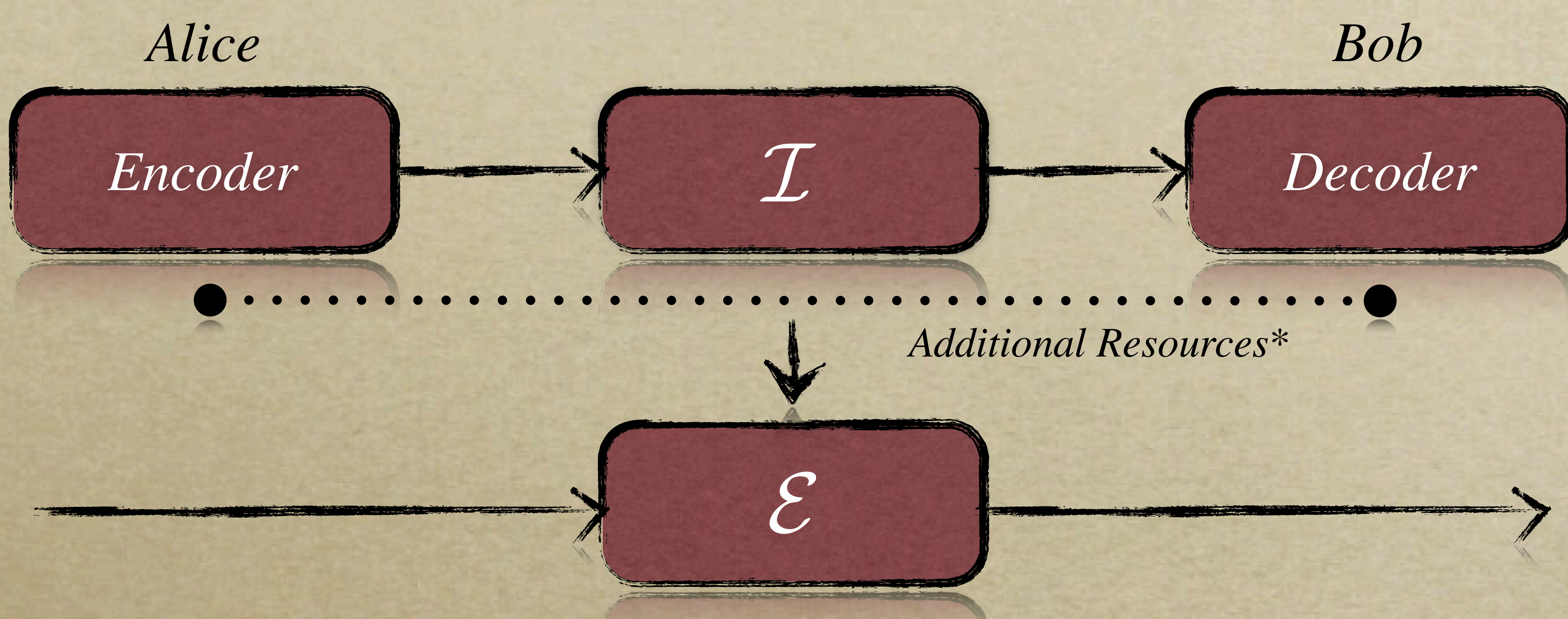
# Quantum Channels Simulations




*E.g. entanglement, classical communication (forward, backward, two-way)*

- *At what asymptotic rate can the identity channel simulate a quantum channel?*

# Quantum Channels Simulations

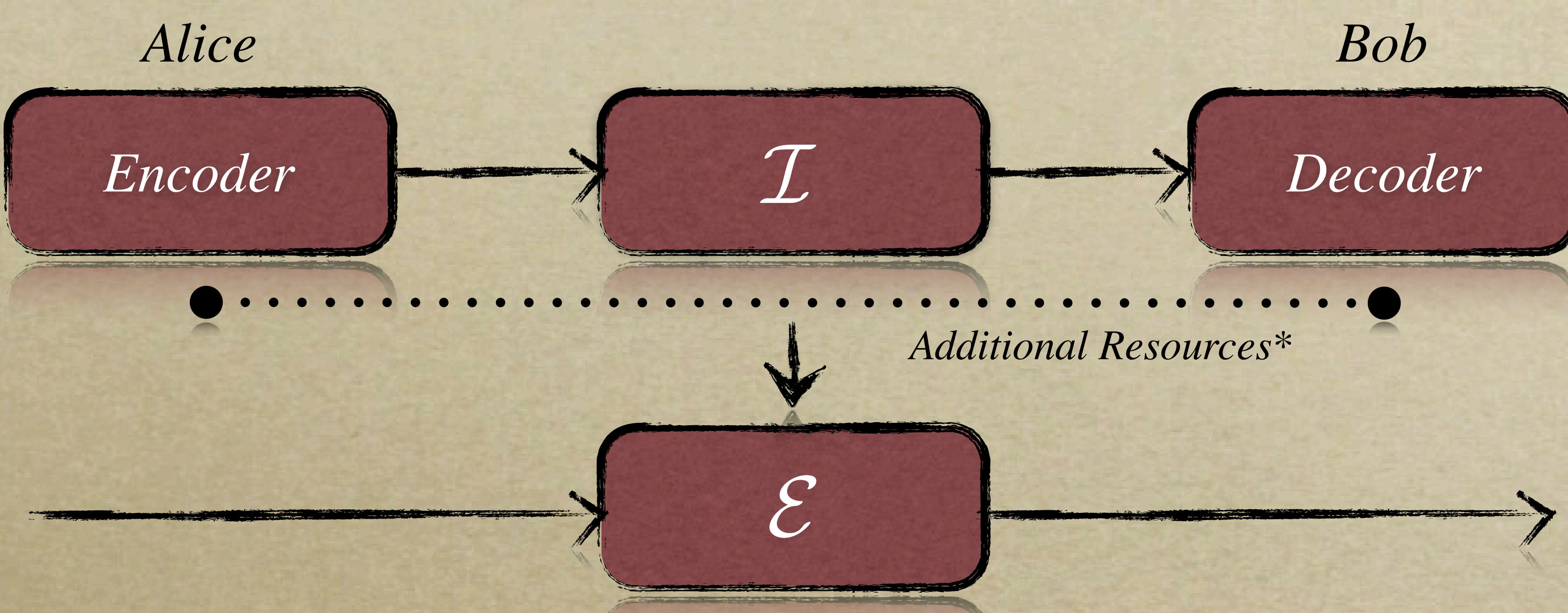



*E.g. entanglement, classical communication (forward, backward, two-way)

- *At what asymptotic rate can the identity channel simulate a quantum channel?*
- *Quantum reverse Shannon theorem: for free entanglement (embezzling states, ebits in general insufficient) the rate is* $Q_{QRST} = 1/Q_E$ *[1,2].*


[1] Bennett. et al., arXiv:0912.5537v2, 2009
[2] B. et al., CMP 306:579, 2011

# Quantum Channels Simulations

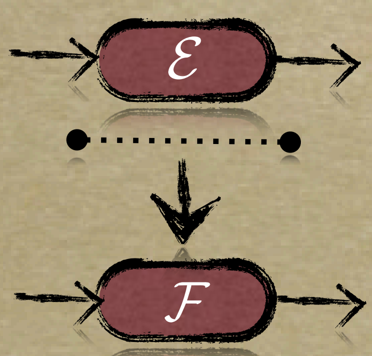



**E.g. entanglement, classical communication (forward, backward, two-way)*

- *At what asymptotic rate can the identity channel simulate a quantum channel?*

- *Quantum reverse Shannon theorem: for free entanglement (embezzling states, ebits in general insufficient) the rate is* $Q_{QRST} = 1/Q_E$ *[1,2].*

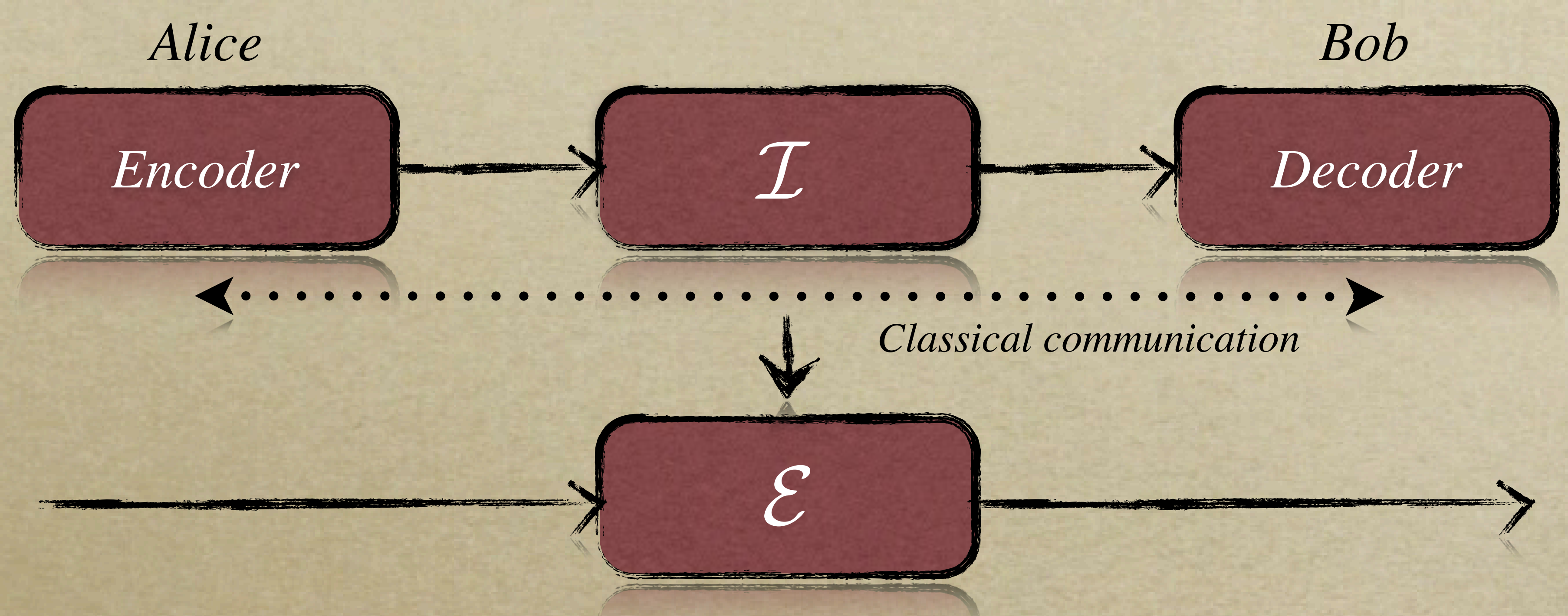
- *Asymptotic capacity of a quantum channel to simulate another quantum channel in the presence of free entanglement:*




$$Q_E(\mathcal{E},\mathcal{F}) = \frac{Q_E(\mathcal{E})}{Q_E(\mathcal{F})}$$

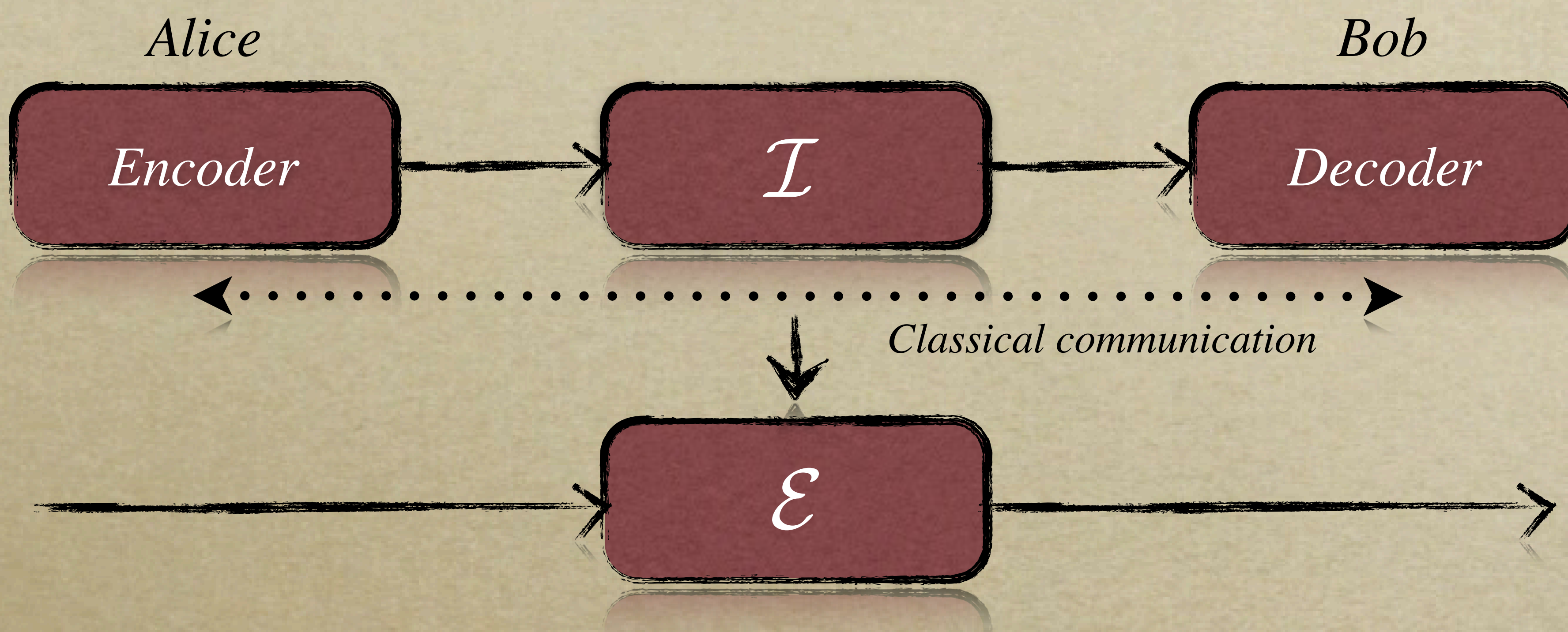
*[1] Bennett. et al., arXiv:0912.5537v2, 2009*
*[2] B. et al., CMP 306:579, 2011*

# Main Contribution



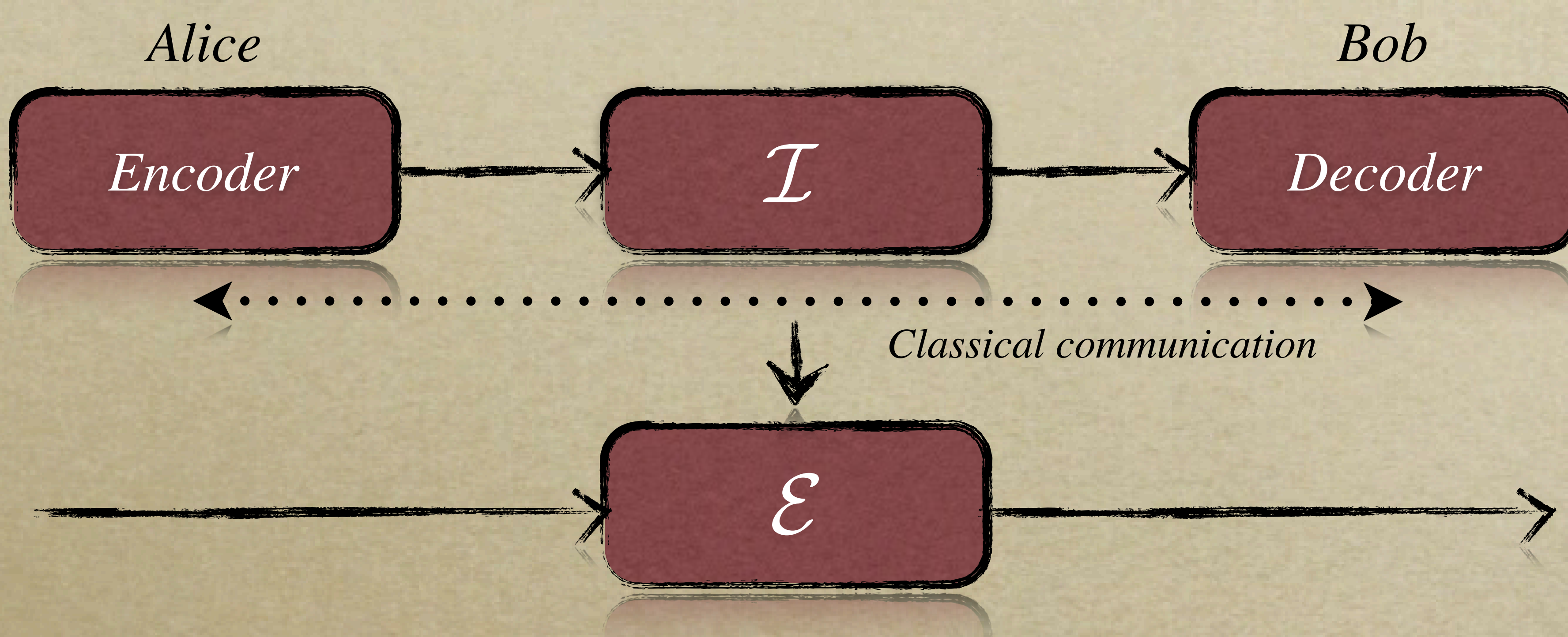

- *What happens for free classical communication instead of entanglement?*

# Main Contribution




- *What happens for free classical communication instead of entanglement?*
- *Question: at what rate is entanglement, in the form of ebits, needed in order to asymptotically simulate a quantum channel, when classical communication is given for free?*

# Main Contribution




- *What happens for free classical communication instead of entanglement?*
- *Question: at what rate is entanglement, in the form of ebits, needed in order to asymptotically simulate a quantum channel, when classical communication is given for free?*
- *Answer:* $$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

$$E_F(\rho_{AB}) = \inf_{\{p_i,\rho^i\}} \sum_i p_i H(A)_{\rho^i} \quad \rho_{AB} = \sum_i p_i \rho^i_{AB} \quad H(A)_\rho = -\mathrm{tr}[\rho_A \log \rho_A]$$

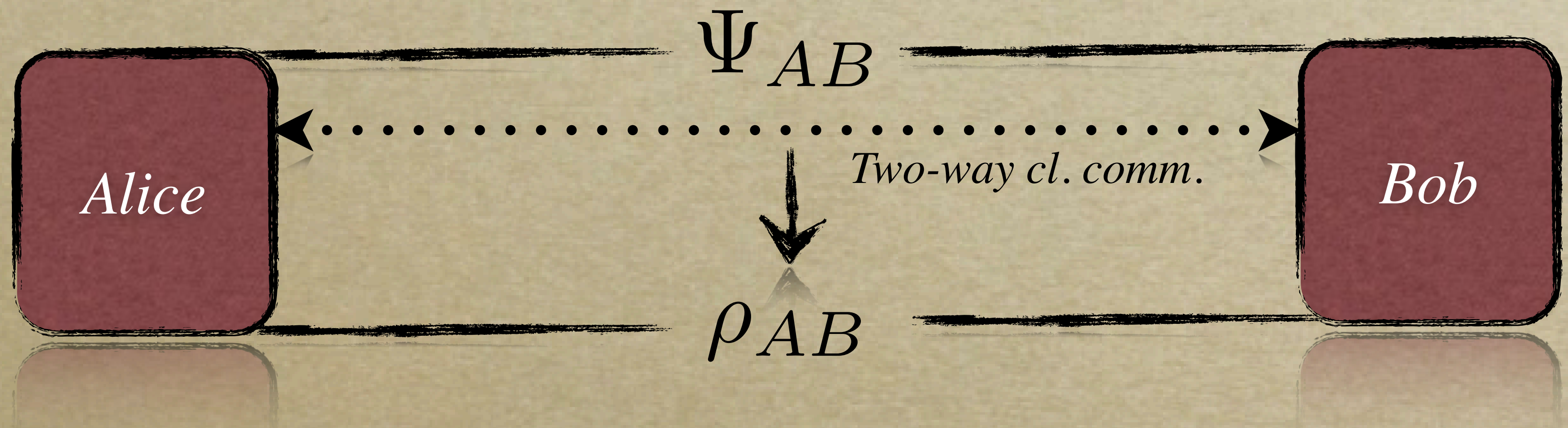
# Remarks about the formula

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

# Remarks about the formula

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

- *Entanglement cost of quantum states [3,4]:* $E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$



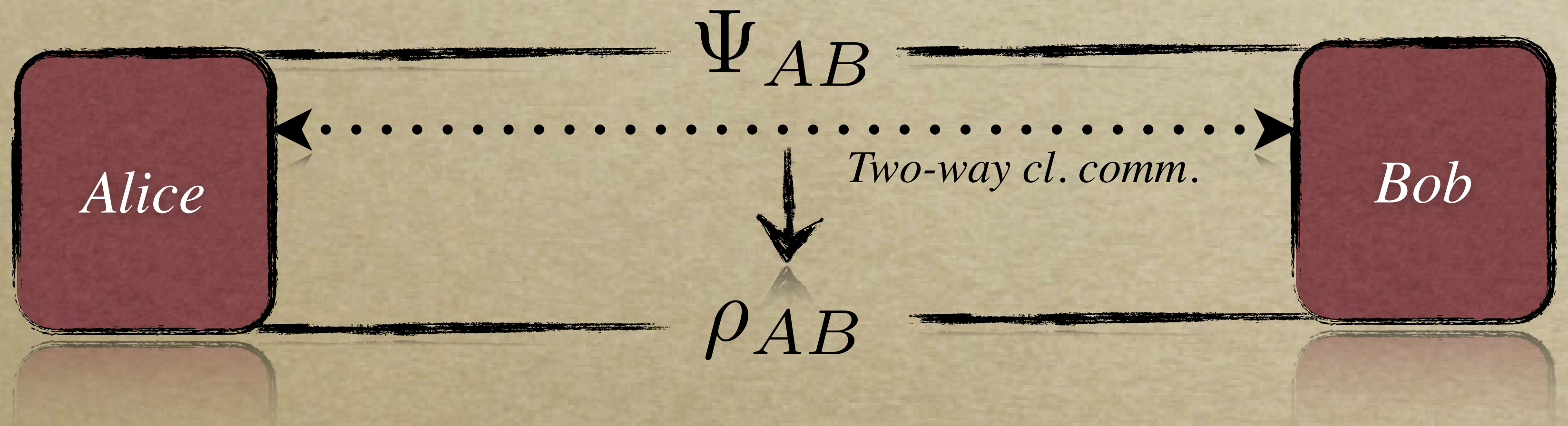


[3] Bennett. et al., PRA 54:3824, 1996
[4] Hayden et al., JPA 34:6891, 2001

# Remarks about the formula

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

- *Entanglement cost of quantum states [3,4]:* $E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$



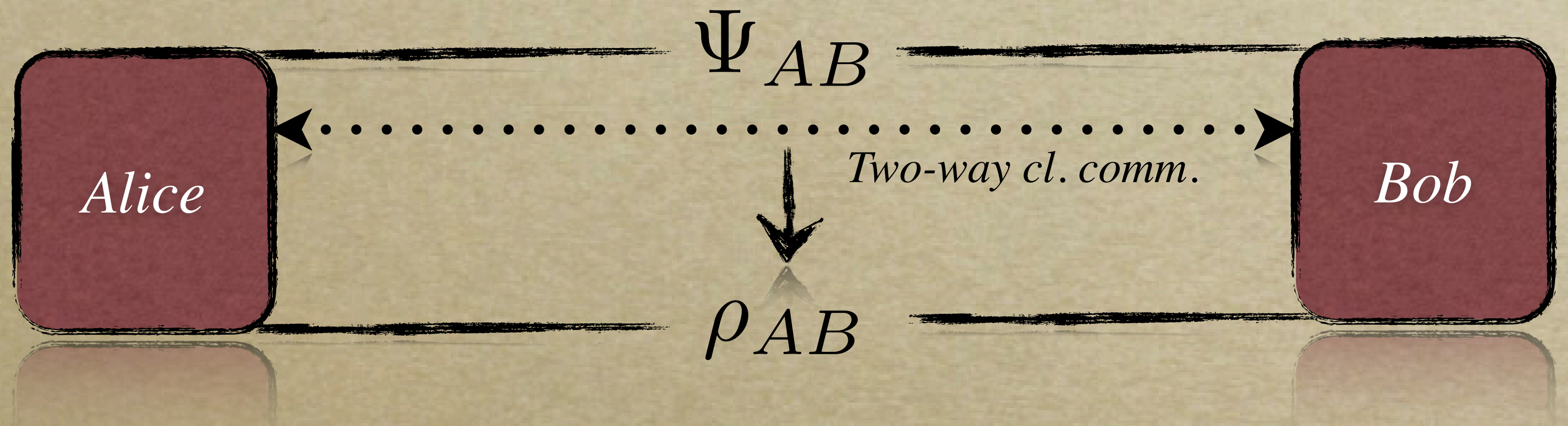

- $\max_{\psi} E_C((\mathcal{E} \otimes \mathcal{I})(\psi)) \le E_C(\mathcal{E}) \le \max_{\psi} E_F((\mathcal{E} \otimes \mathcal{I})(\psi))$


[3] Bennett. et al., PRA 54:3824, 1996
[4] Hayden et al., JPA 34:6891, 2001

# Remarks about the formula

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

- *Entanglement cost of quantum states [3,4]:* $E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$



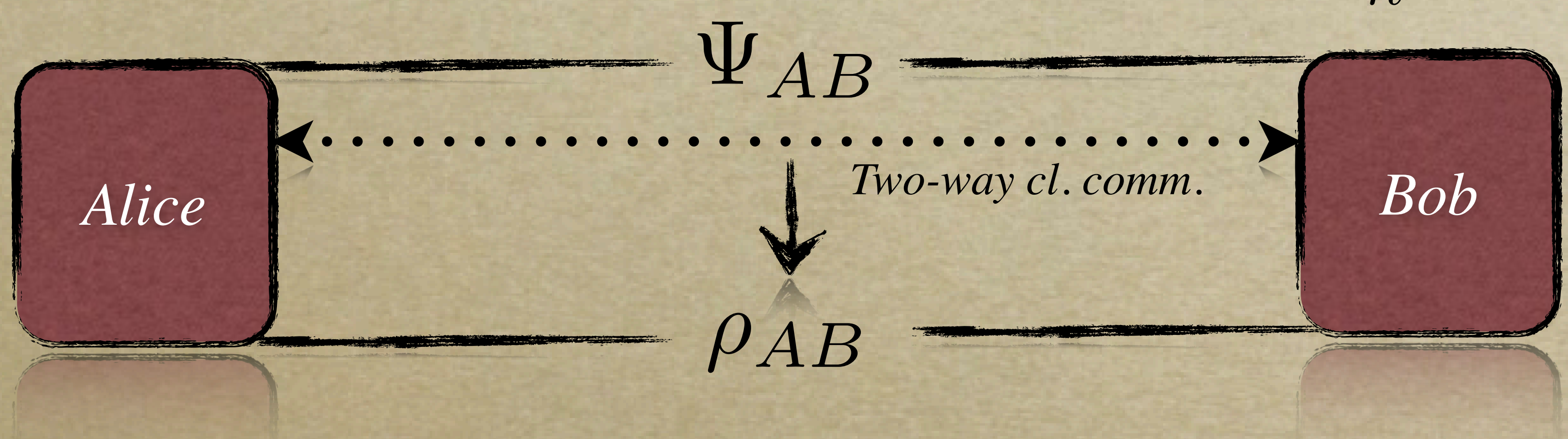

- $\max_{\psi} E_C((\mathcal{E} \otimes \mathcal{I})(\psi)) \leq E_C(\mathcal{E}) \leq \max_{\psi} E_F((\mathcal{E} \otimes \mathcal{I})(\psi))$
- *Bound entangled quantum channels:* $E_C \geq Q_{\leftrightarrow} \quad (\geq Q_{\leftarrow} \geq Q_{\rightarrow} = Q)$.


[3] Bennett. et al., PRA 54:3824, 1996
[4] Hayden et al., JPA 34:6891, 2001

# Remarks about the formula

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

- *Entanglement cost of quantum states [3,4]:* $E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$




- $\max_{\psi} E_C((\mathcal{E} \otimes \mathcal{I})(\psi)) \le E_C(\mathcal{E}) \le \max_{\psi} E_F((\mathcal{E} \otimes \mathcal{I})(\psi))$
- *Bound entangled quantum channels:* $E_C \ge Q_{\leftrightarrow} \quad (\ge Q_{\leftarrow} \ge Q_{\rightarrow} = Q)$.
- $E_C(\mathcal{E}) = 0 \leftrightarrow \mathcal{E}$ *is entanglement breaking.*


[3] Bennett. et al., PRA 54:3824, 1996
[4] Hayden et al., JPA 34:6891, 2001

# A few words about the achievability

- *Channel Simulation has to work for all (entangled) inputs! Simulation* $\mathcal{F}^{n,\varepsilon}$ *with entanglement cost* $E_C^{(1)}(\mathcal{E}^{\otimes n}, \varepsilon)$*:*

# A few words about the achievability

- *Channel Simulation has to work for all (entangled) inputs! Simulation* $\mathcal{F}^{n,\varepsilon}$ *with entanglement cost* $E_C^{(1)}(\mathcal{E}^{\otimes n},\varepsilon)$*:*

$$\boxed{\lim_{\varepsilon\to 0}\lim_{n\to\infty}\|\mathcal{E}^{\otimes n}-\mathcal{F}^{n,\varepsilon}\|_\diamond = 0 \quad \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}E_C^{(1)}(\mathcal{E}^{\otimes n},\varepsilon) = E_C(\mathcal{E})}$$

$$\|\mathcal{E}\|_\diamond = \sup_{k\in\mathbb{N}}\sup_{\|\sigma\|_1\le 1}\|(\mathcal{E}\otimes\mathcal{I})(\sigma)\|_1 \qquad \|\sigma\|_1 = \mathrm{tr}(\sqrt{\sigma^\dagger\sigma})$$


*[5] Christandl et al., PRL 102:020504, 2009*
*[6] Renner, PhD Thesis, ETHZ, 2005*
*[7] Tomamichel, PhD Thesis, ETHZ, 2011*
*[8] Buscemi et al., PRL 106:130503, 2011*
*[9] Hayashi, Springer 2006*

# A few words about the achievability

- *Channel Simulation has to work for all (entangled) inputs! Simulation $\mathcal{F}^{n,\varepsilon}$ with entanglement cost $E_C^{(1)}(\mathcal{E}^{\otimes n}, \varepsilon)$:*

$$\boxed{\lim_{\varepsilon \to 0} \lim_{n \to \infty} \|\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon}\|_\Diamond = 0 \quad \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} E_C^{(1)}(\mathcal{E}^{\otimes n}, \varepsilon) = E_C(\mathcal{E})}$$

$$\|\mathcal{E}\|_\Diamond = \sup_{k \in \mathbb{N}} \sup_{\|\sigma\|_1 \leq 1} \|(\mathcal{E} \otimes \mathcal{I})(\sigma)\|_1 \qquad \|\sigma\|_1 = \mathrm{tr}(\sqrt{\sigma^\dagger \sigma})$$

- *Post-Selection Technique for Quantum Channels [5]:*

$$\|\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon}\|_\Diamond \leq \mathrm{poly}(n) \cdot \|((\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon}) \otimes \mathcal{I})(\zeta^n)\|_1$$

*The quantum state $\zeta^n$ is the purification of a special de Finetti state (a state which consists of n identical and independent copies of a state on a single subsystem) --> no iid structure!*


[5] Christandl et al., PRL 102:020504, 2009
[6] Renner, PhD Thesis, ETHZ, 2005
[7] Tomamichel, PhD Thesis, ETHZ, 2011
[8] Buscemi et al., PRL 106:130503, 2011
[9] Hayashi, Springer 2006

# A few words about the achievability

- *Channel Simulation has to work for all (entangled) inputs! Simulation* $\mathcal{F}^{n,\varepsilon}$ *with entanglement cost* $E_C^{(1)}(\mathcal{E}^{\otimes n}, \varepsilon)$*:*

$$\boxed{\lim_{\varepsilon\to 0}\lim_{n\to\infty} \|\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon}\|_\diamond = 0 \quad \lim_{\varepsilon\to 0}\lim_{n\to\infty} \frac{1}{n} E_C^{(1)}(\mathcal{E}^{\otimes n}, \varepsilon) = E_C(\mathcal{E})}$$

$$\|\mathcal{E}\|_\diamond = \sup_{k\in\mathbb{N}} \sup_{\|\sigma\|_1 \leq 1} \|(\mathcal{E}\otimes\mathcal{I})(\sigma)\|_1 \qquad \|\sigma\|_1 = \mathrm{tr}(\sqrt{\sigma^\dagger\sigma})$$

- *Post-Selection Technique for Quantum Channels [5]:*

$$\|\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon}\|_\diamond \leq \mathrm{poly}(n)\cdot\|((\mathcal{E}^{\otimes n} - \mathcal{F}^{n,\varepsilon})\otimes\mathcal{I})(\zeta^n)\|_1$$

*The quantum state* $\zeta^n$ *is the purification of a special de Finetti state (a state which consists of n identical and independent copies of a state on a single subsystem) --> no iid structure!*

- *One-shot information theory, smooth entropy formalism [6,7]. One-shot entanglement cost of quantum states [8,9] to evaluate:* $E_C^{(1)}(\mathcal{E}^{\otimes n}(\zeta^n), \varepsilon)$.

*[5] Christandl et al., PRL 102:020504, 2009*
*[6] Renner, PhD Thesis, ETHZ, 2005*
*[7] Tomamichel, PhD Thesis, ETHZ, 2011*
*[8] Buscemi et al., PRL 106:130503, 2011*
*[9] Hayashi, Springer 2006*

# Strong Converse Quantum Capacity

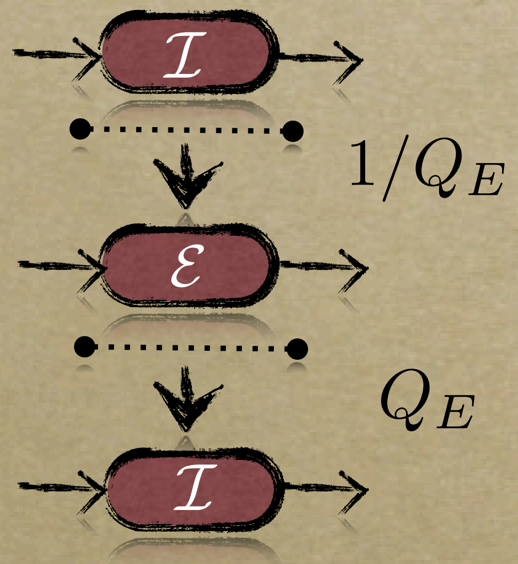
- *Capacity: optimal asymptotic rate at which information can be sent error free.*

# Strong Converse Quantum Capacity

- *Capacity: optimal asymptotic rate at which information can be sent error free.*
- *Strong converse capacity: minimal asymptotic rate above which any attempt to send information necessarily has exponentially small fidelity.*

# Strong Converse Quantum Capacity

- *<u>Capacity</u>: optimal asymptotic rate at which information can be sent error free.*
- *<u>Strong converse capacity</u>: minimal asymptotic rate above which any attempt to send information necessarily has exponentially small fidelity.*
- *Quantum reverse Shannon theorem, $Q_E$ is a strong converse capacity [1]:*

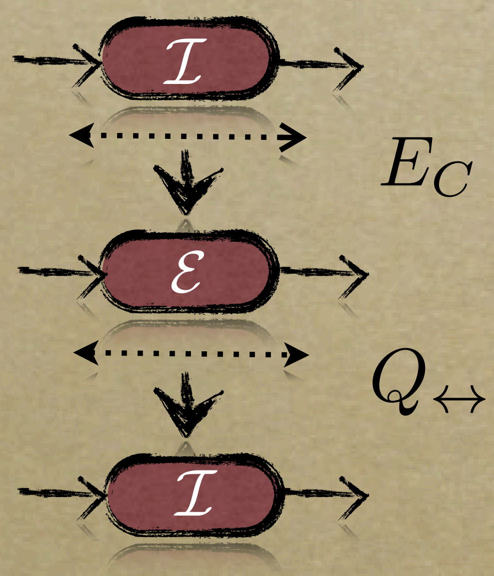




*[1] Bennett. et al., arXiv:0912.5537v2, 2009*
*[10] Wootters, PRL 80:2245, 1998*

# Strong Converse Quantum Capacity

- *<u>Capacity</u>: optimal asymptotic rate at which information can be sent error free.*
- *<u>Strong converse capacity</u>: minimal asymptotic rate above which any attempt to send information necessarily has exponentially small fidelity.*
- *Quantum reverse Shannon theorem, $Q_E$ is a strong converse capacity [1].*

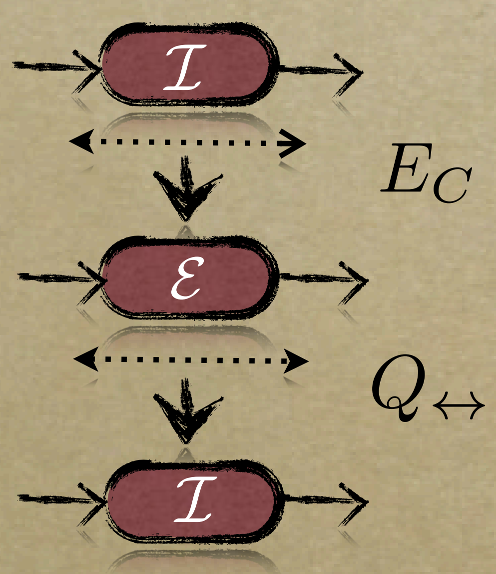



- *Upper bound on the strong converse quantum capacity assisted by cl. comm. (any direction)!*

*[1] Bennett. et al., arXiv:0912.5537v2, 2009*
*[10] Wootters, PRL 80:2245, 1998*

# Strong Converse Quantum Capacity

- *Capacity: optimal asymptotic rate at which information can be sent error free.*
- *Strong converse capacity: minimal asymptotic rate above which any attempt to send information necessarily has exponentially small fidelity.*
- *Quantum reverse Shannon theorem, $Q_E$ is a strong converse capacity [1].*



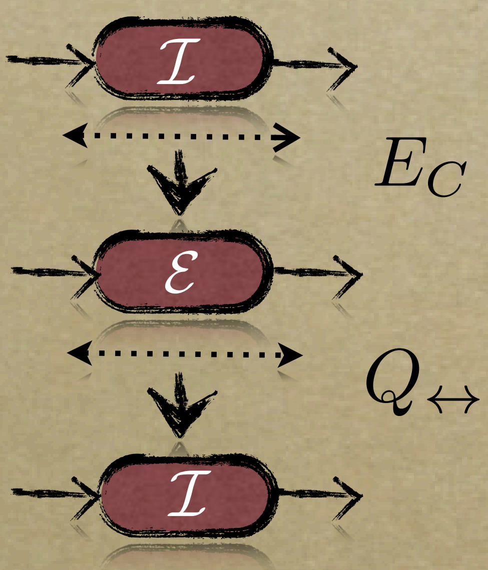

- *Upper bound on the strong converse quantum capacity assisted by cl. comm. (any direction)!*
- *For qubit channels [10]*:*

$$E_C(\mathcal{E}) \leq \max_{\psi} E_F((\mathcal{E}\otimes\mathcal{I})(\psi)) = h(\frac{1}{2}(1+\sqrt{1-C^2((\mathcal{E}\otimes\mathcal{I})(\Psi))}))$$

[1] Bennett. et al., arXiv:0912.5537v2, 2009
[10] Wootters, PRL 80:2245, 1998

# Strong Converse Quantum Capacity

- *Capacity: optimal asymptotic rate at which information can be sent error free.*
- *Strong converse capacity: minimal asymptotic rate above which any attempt to send information necessarily has exponentially small fidelity.*
- *Quantum reverse Shannon theorem, $Q_E$ is a strong converse capacity [1].*

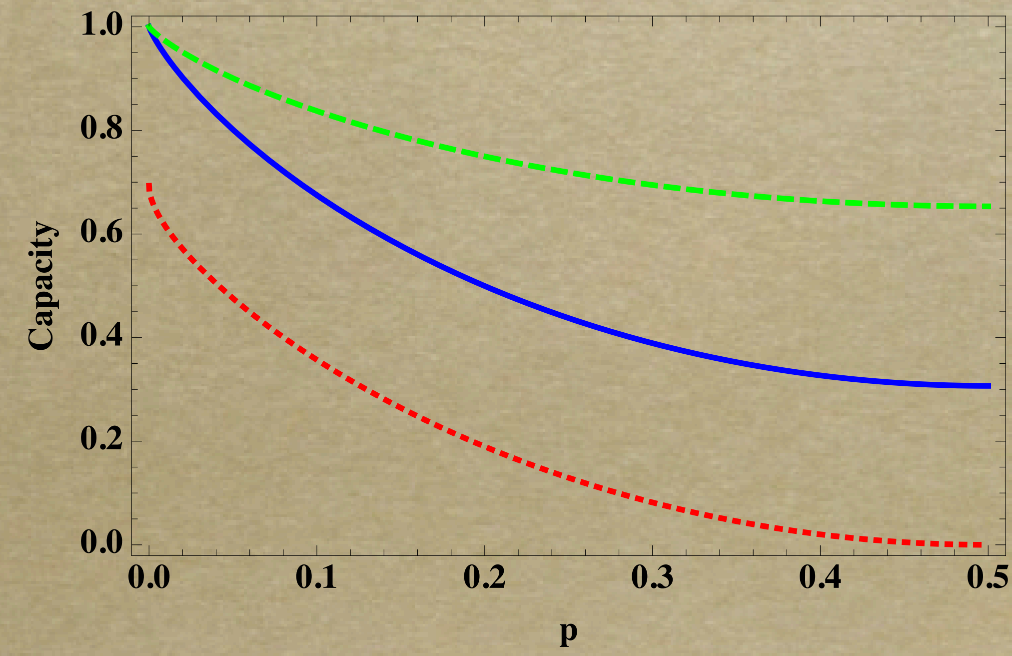



- *Upper bound on the strong converse quantum capacity assisted by cl. comm. (any direction)!*
- *For qubit channels [10]*:*

$$E_C(\mathcal{E}) \leq \max_{\psi} E_F((\mathcal{E} \otimes \mathcal{I})(\psi)) = h(\frac{1}{2}(1 + \sqrt{1 - C^2((\mathcal{E} \otimes \mathcal{I})(\Psi))}))$$

- *Qubit dephasing channel:*

$$\mathcal{E}(\rho) = (1-p) \cdot \rho + p \cdot \sigma_z \rho \sigma_z$$

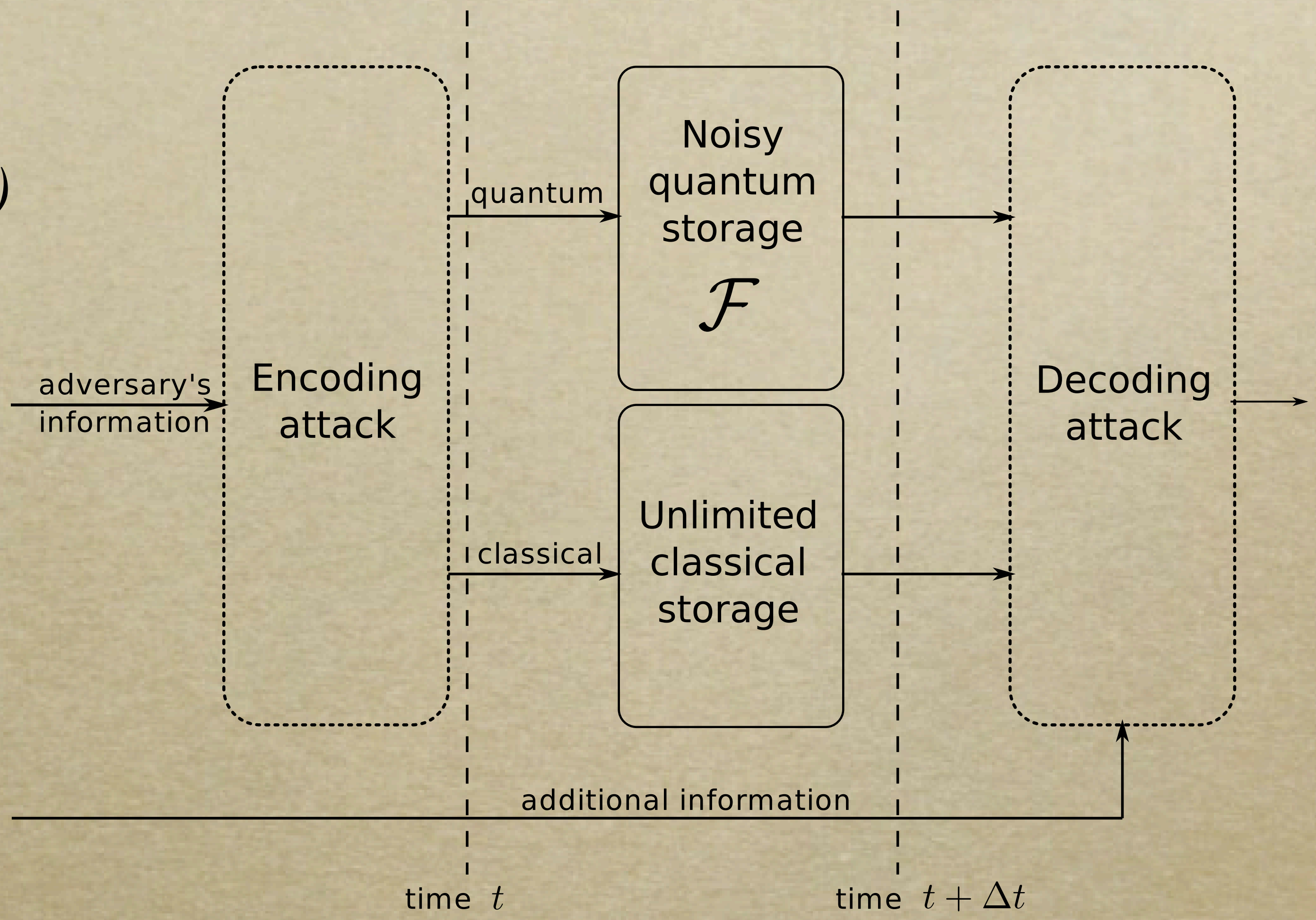



*$Q = Q_{\rightarrow}$ (red)*
*vs. * (blue)*
*vs. $Q_E$ (green)*


*[1] Bennett. et al., arXiv:0912.5537v2, 2009*
*[10] Wootters, PRL 80:2245, 1998*

# Noisy-Storage Model

- *<u>Two-party cryptographic model</u>: adversary has only bounded size (noisy) quantum storage [11]. Solves: bit commitment, oblivious transfer, secure identification etc. [...].*

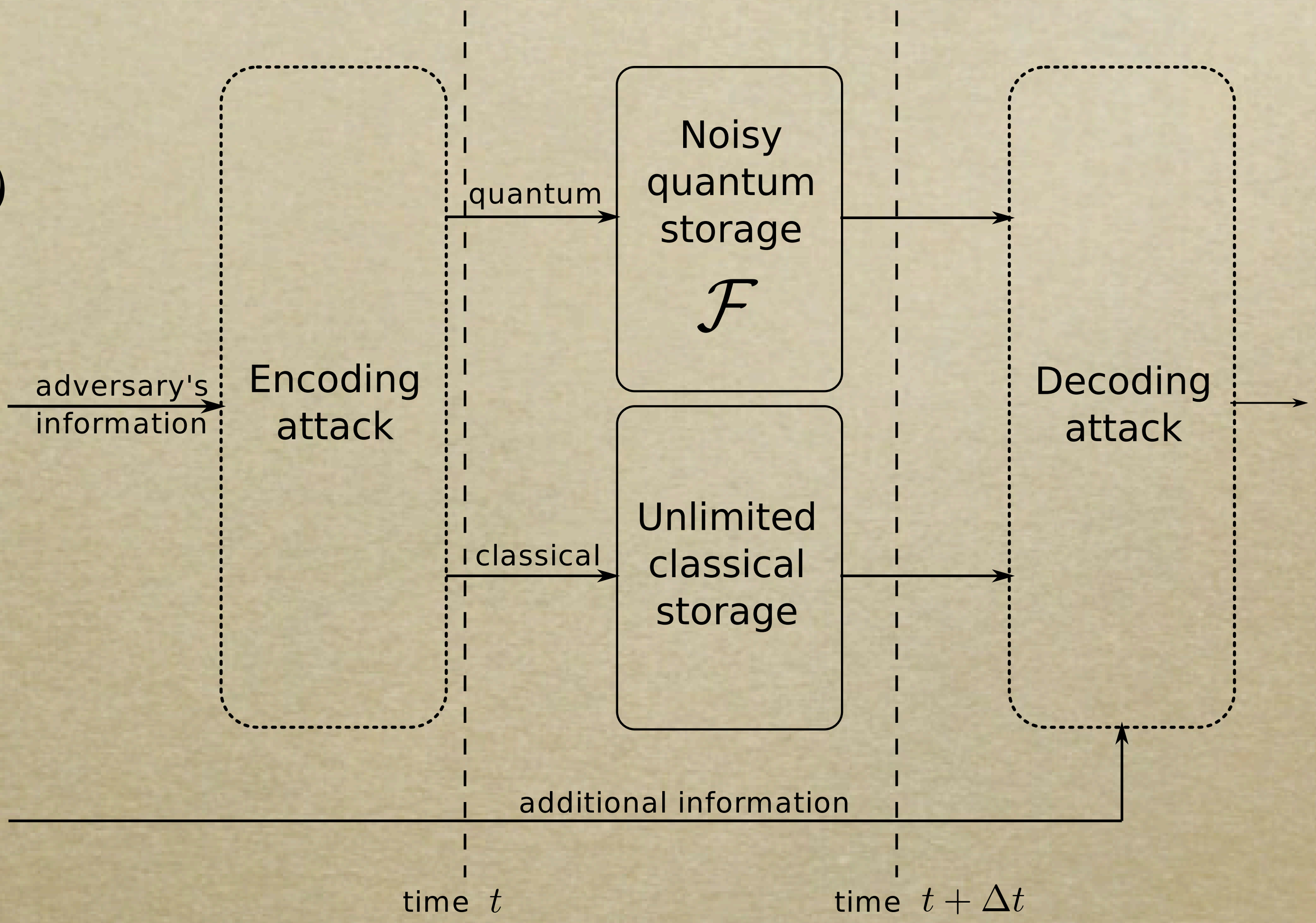




*[11] Wehner et al., PRL 100:220502, 2008*
*[12] König et al., IEEE TIT 58:1962, 2012*

# Noisy-Storage Model

- *<u>Two-party cryptographic model</u>: adversary has only bounded size (noisy) quantum storage [11]. Solves: bit commitment, oblivious transfer, secure identification etc. [...].*




- *Special case* $\mathcal{F} = \mathcal{E}^{\otimes \nu \cdot m}$, *m=number of qubits transmitted during protocol [12]:*

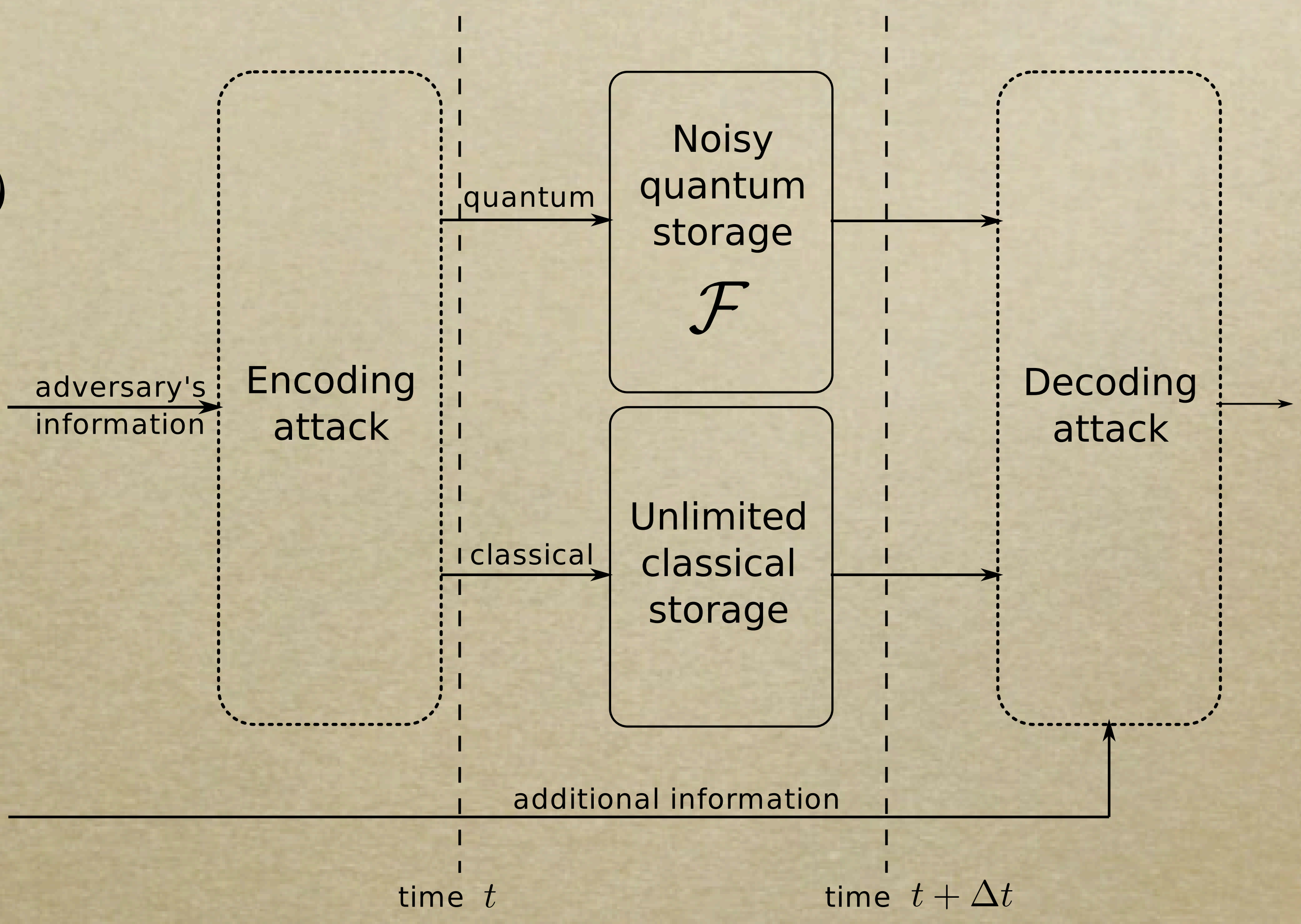
$$C^{\text{strong}}(\mathcal{E}) \cdot \nu < \frac{1}{2}$$

[11] Wehner et al., PRL 100:220502, 2008
[12] König et al., IEEE TIT 58:1962, 2012

# Noisy-Storage Model

- *Two-party cryptographic model*: adversary has only bounded size (noisy) quantum storage [11]. Solves: bit commitment, oblivious transfer, secure identification etc. [...].

- *Special case* $\mathcal{F} = \mathcal{E}^{\otimes \nu \cdot m}$, *m=number of qubits transmitted during protocol [12]:*
  $C^{\text{strong}}(\mathcal{E}) \cdot \nu < \frac{1}{2}$
- *Our improvement:* $E_C(\mathcal{E}) \cdot \nu < \frac{1}{2}$

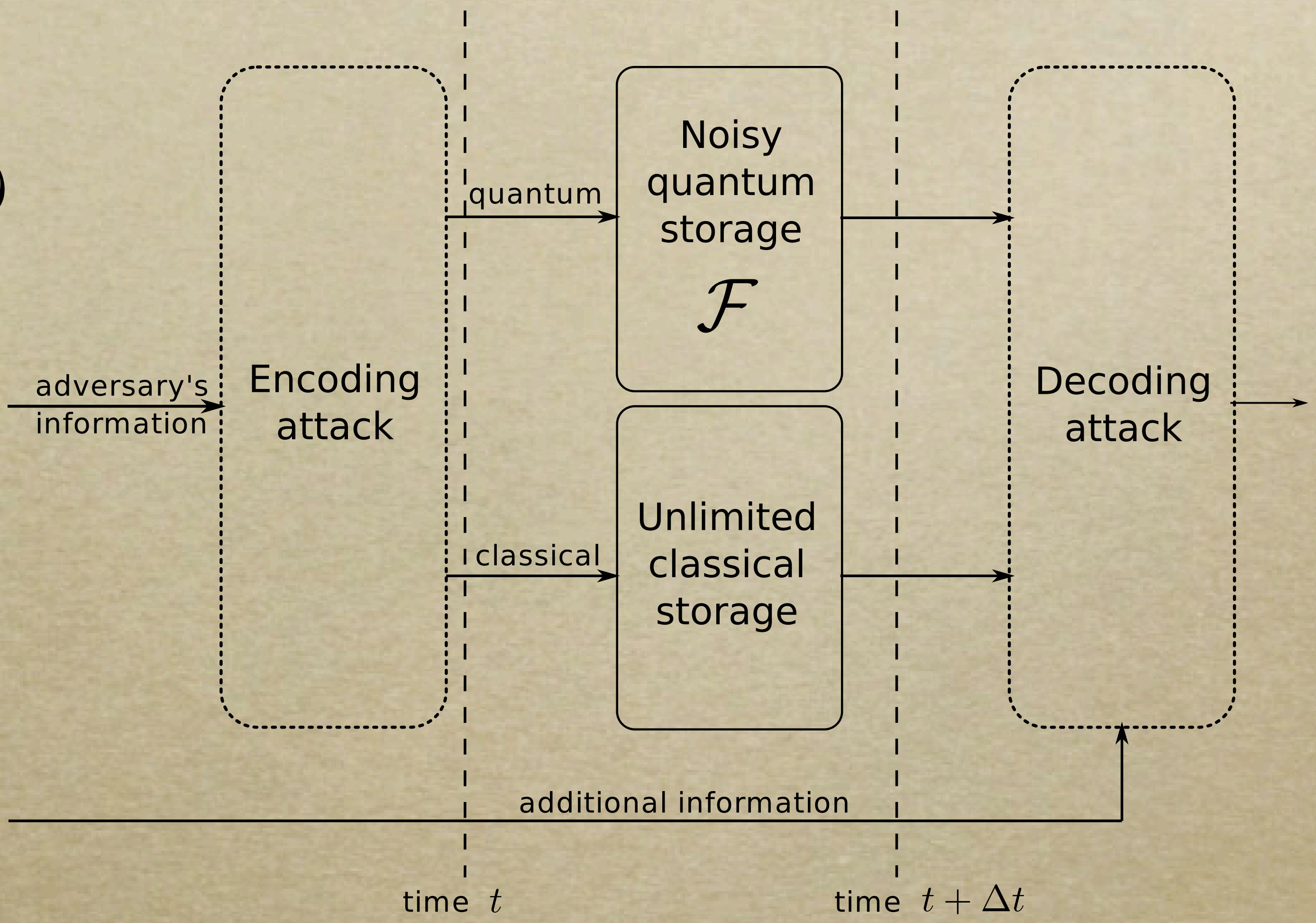




[11] Wehner et al., PRL 100:220502, 2008
[12] König et al., IEEE TIT 58:1962, 2012

# Noisy-Storage Model

- *<u>Two-party cryptographic model</u>: adversary has only bounded size (noisy) quantum storage [11]. Solves: bit commitment, oblivious transfer, secure identification etc. [...].*




- *Special case* $\mathcal{F} = \mathcal{E}^{\otimes \nu \cdot m}$*, m=number of qubits transmitted during protocol [12]:*

$$C^{\text{strong}}(\mathcal{E}) \cdot \nu < \frac{1}{2}$$

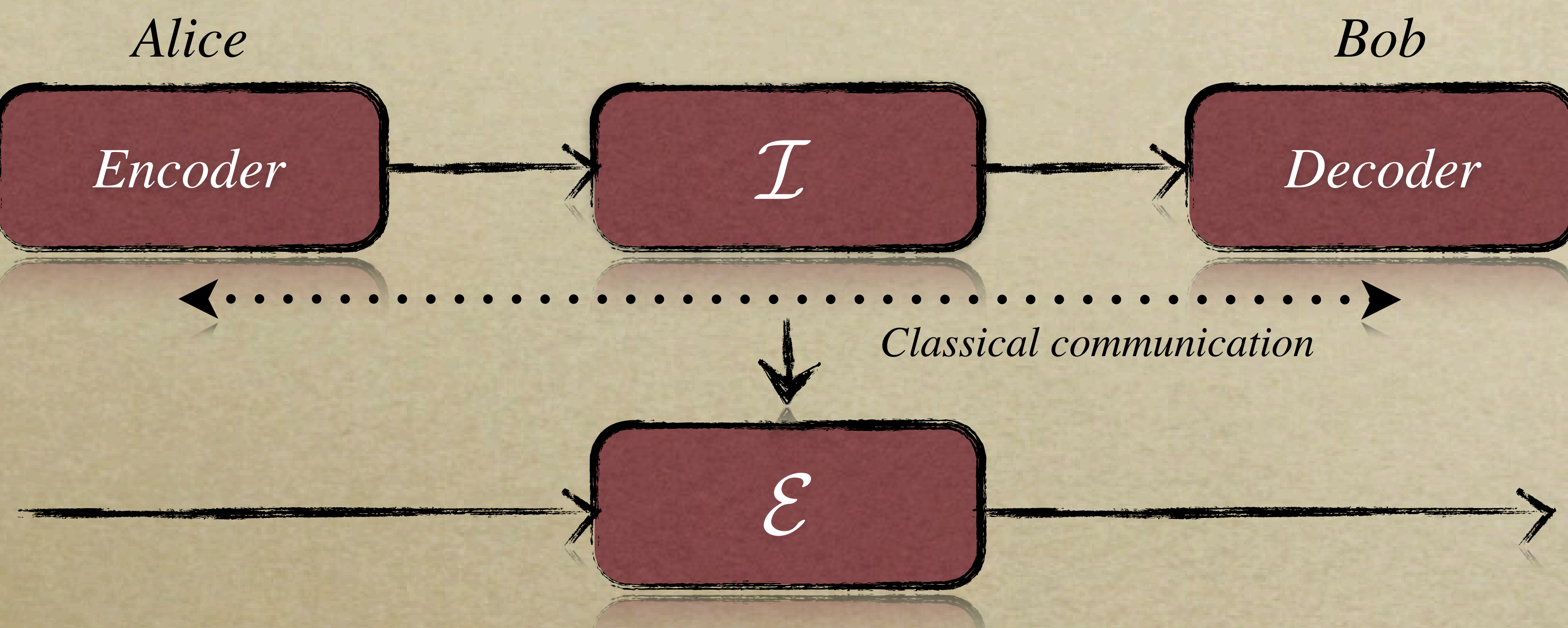
- *Our improvement:* $E_C(\mathcal{E}) \cdot \nu < \frac{1}{2}$

- *New results in arXiv:1111.2026v3 (B., Fawzi, Wehner) --> ICITS 12, CRYPTO 12:*

$$Q^{\text{strong}}(\mathcal{E}) \cdot \nu < \frac{1}{2}$$


*[11] Wehner et al., PRL 100:220502, 2008*
*[12] König et al., IEEE TIT  58:1962, 2012*

# Conclusions




- *Question: at what rate is quantum communication, or equivalently entanglement, needed in order to asymptotically simulate a quantum channel, when classical communication is given for free?*

- *Answer:*

$$\boxed{E_C(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\psi^n} E_F((\mathcal{E}^{\otimes n} \otimes \mathcal{I})(\psi^n))}$$

$$E_F(\rho_{AB}) = \inf_{\{p_i,\rho^i\}} \sum_i p_i H(A)_{\rho^i} \quad \rho_{AB} = \sum_i p_i \rho^i_{AB} \quad H(A)_\rho = -\mathrm{tr}[\rho_A \log \rho_A]$$