Quantum entanglement as a resource

Michał Horodecki

KCIK, IFTiA

QIPA’11

Entanglement of pure states

A pure state of two systems is *entangled* if
it cannot be written as a product of two states:

$$\psi_{AB} \neq \psi_A \otimes \psi_B$$

Two-qubit maximally entangled state:

$$\psi_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right)$$

1 e-bit

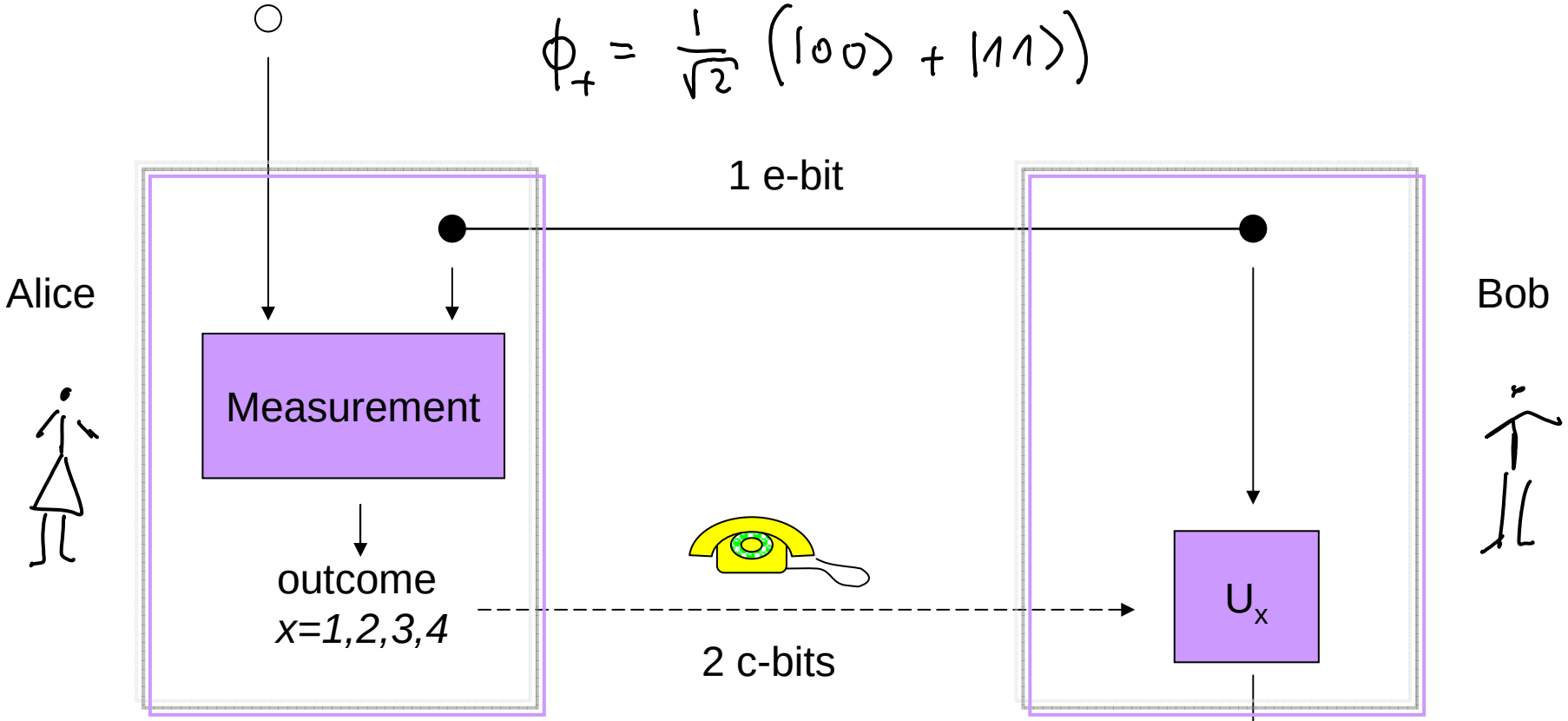
Basic entanglement-based protocols

Quantum communication: Teleportation

[Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters '93]

$\psi = a|0\rangle + b|1\rangle$

$\phi_+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



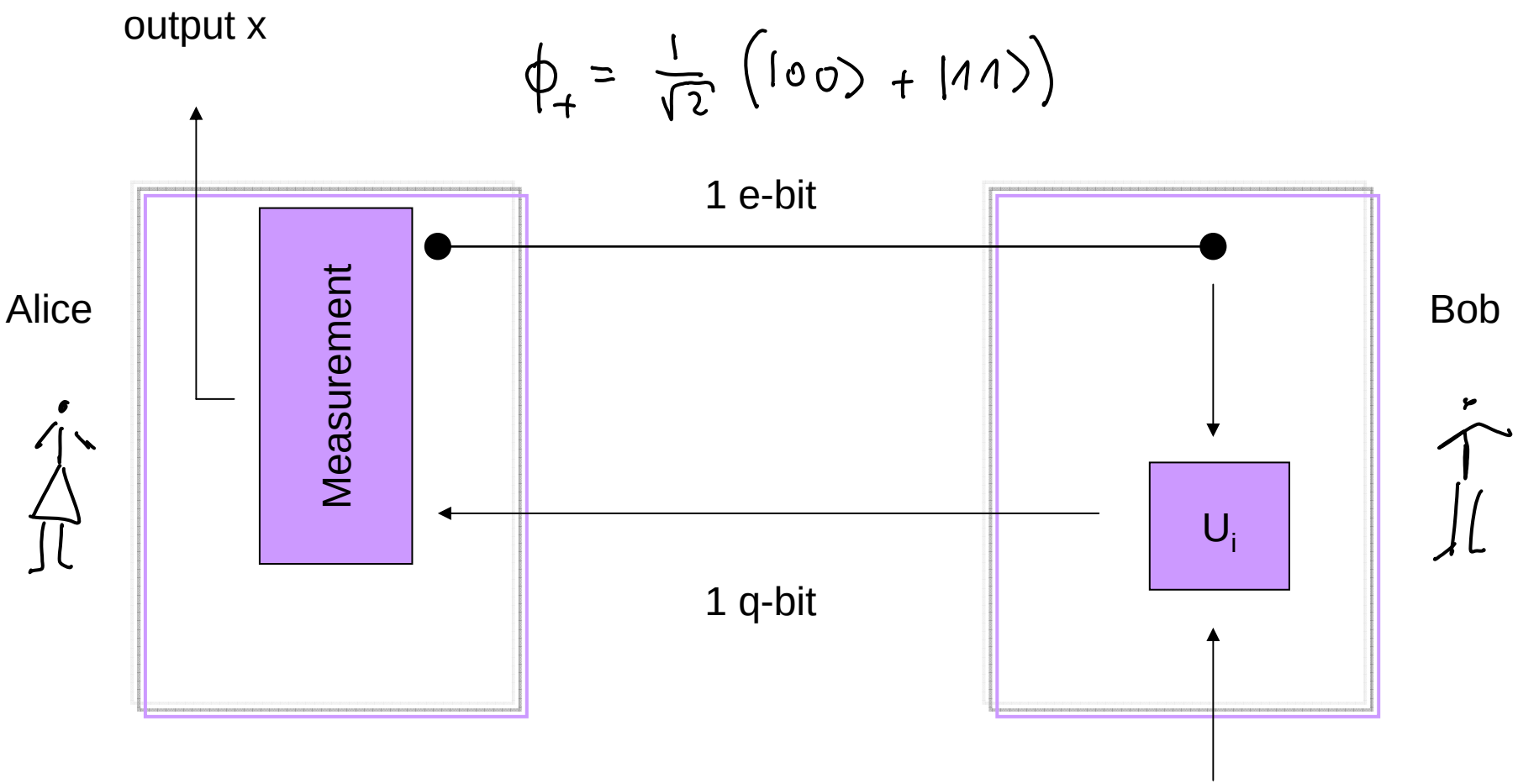
1 e-bit + 2 c-bits ≥ 1 q-bit

$\psi = a|0\rangle + b|1\rangle$

Basic entanglement-based protocols

Classical communication: Dense coding

[Bennett, Wiesner '92]



1 e-bit + 1 q-bit ≥ 2 c-bits

Coherent dense coding

[A. Harrow '03]

Keep the input and dense code:

$$X_A \rightarrow X_A X_{A'} \longrightarrow X_A X_B$$

But dense coding protocol can do more:

$$\sum_x a_x |x\rangle_A \rightarrow \sum_x a_x |x\rangle_A |x\rangle_{A'} \rightarrow \sum_x a_x |x\rangle_A |x\rangle_B$$

Dense coding protocol transfers **coherent bits**!

1 e-bit + 1 q-bit ≥ 2 co-bits

Coherent teleportation

What happens, if in teleportation we use coherent bits ?

Answer: we shall obtain in addition 2 e-bits!

1 e-bit + 2 co-bits $\geq$ 1 q-bit + 2 e-bits

2 co-bits $\geq$ 1 q-bit + 1 e-bit

Unification of teleportation and dense coding

Coherent dense coding:

1 e-bit + 1 q-bit $\geq$ 2 co-bits

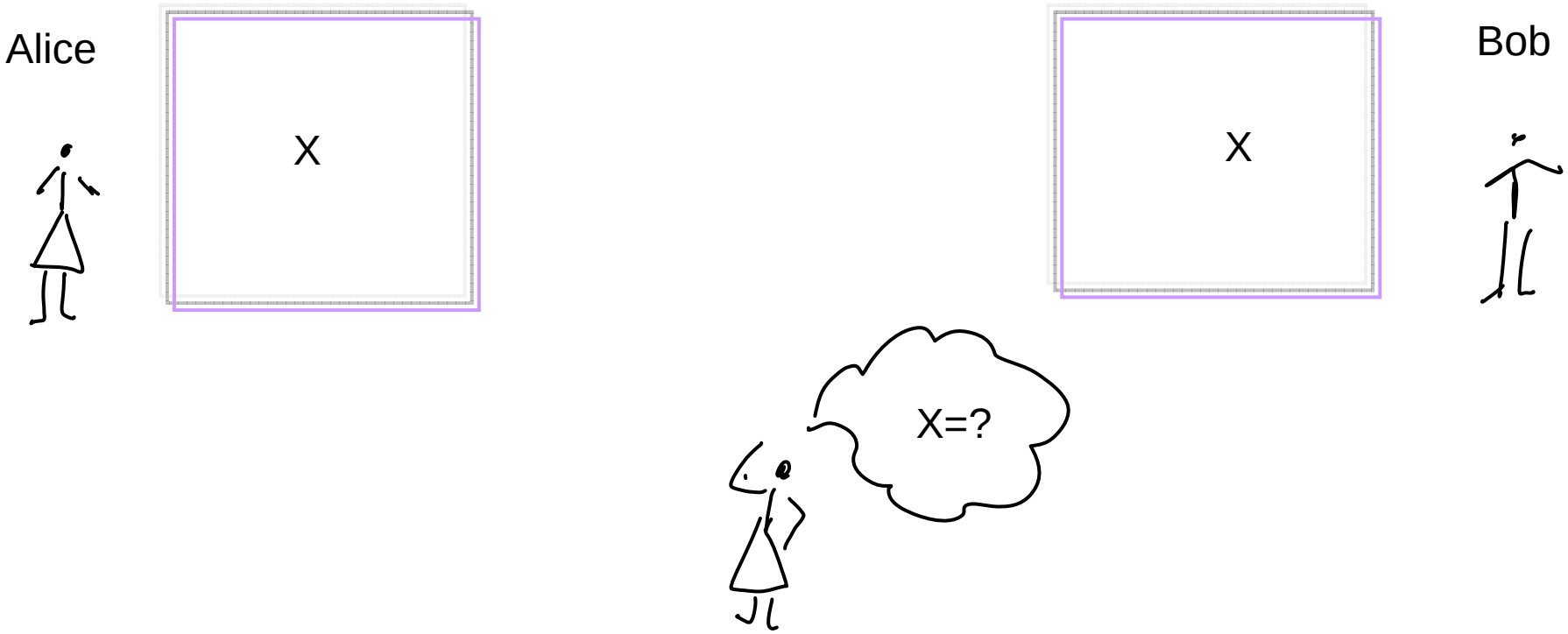
Coherent teleportation:

2 co-bits $\geq$ 1 q-bit + 1 e-bit

2 co-bits = 1 q-bit + 1 e-bit

Private key

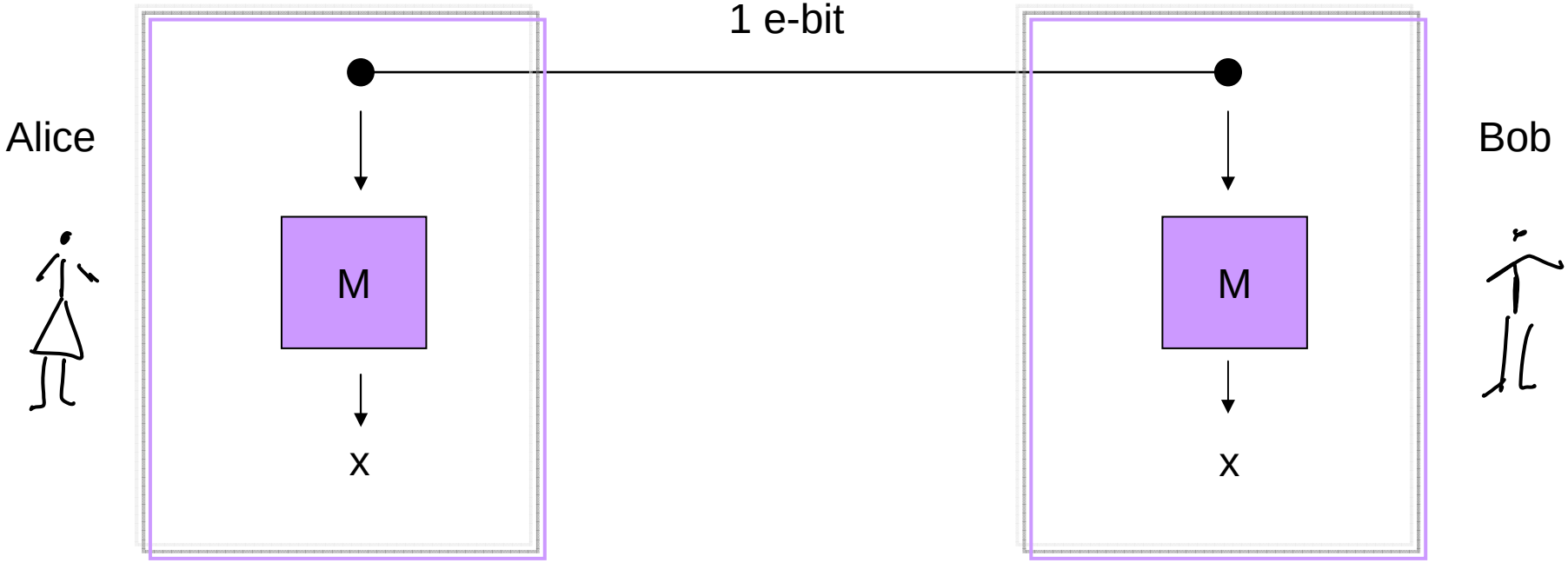
Random bit shared by Alice and Bob, but unknown to Eve (rest of world)



Private key from entanglement

Ekert ‘91

$$\phi_+ = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



1 e-bit ≥ 1 p-bit

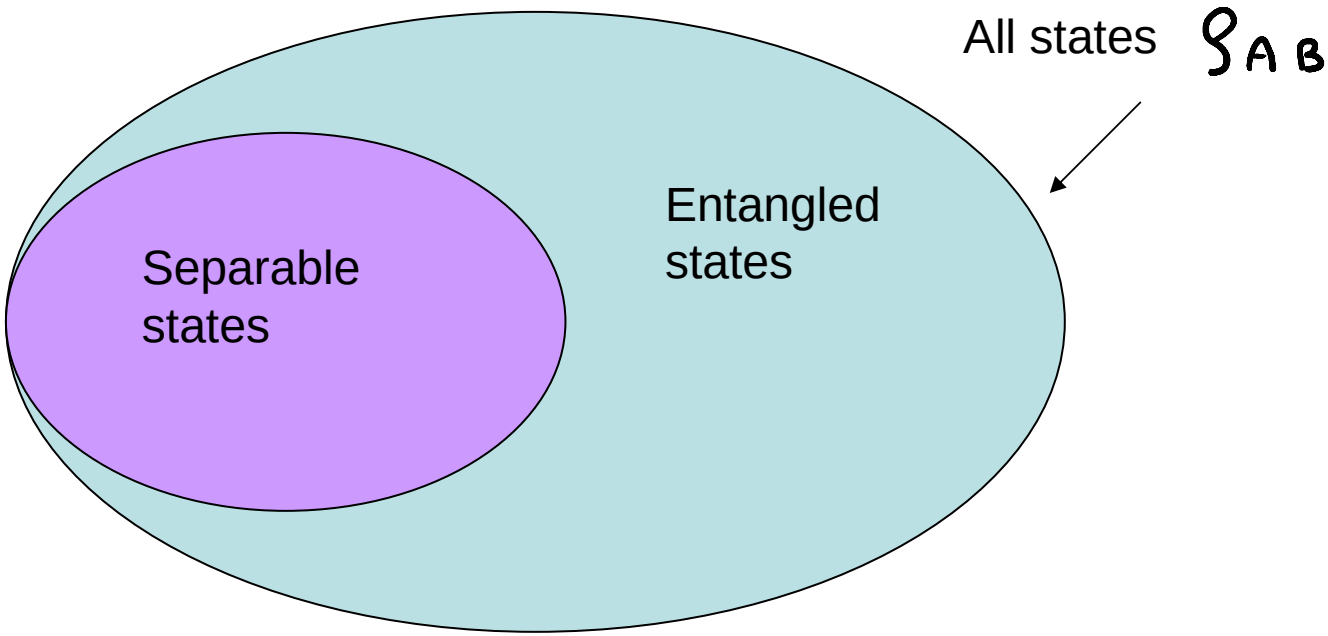
Problem: is the maximally entangled state the only state offering private bit of key?

Entanglement of mixed states

Werner ‘89

Negative definition: a state ρ is entangled if it is not separable, i.e. It is not a mixture of product states:

$$\rho_{AB} \neq \sum_i p_i \rho_A^i \otimes \rho_B^i$$



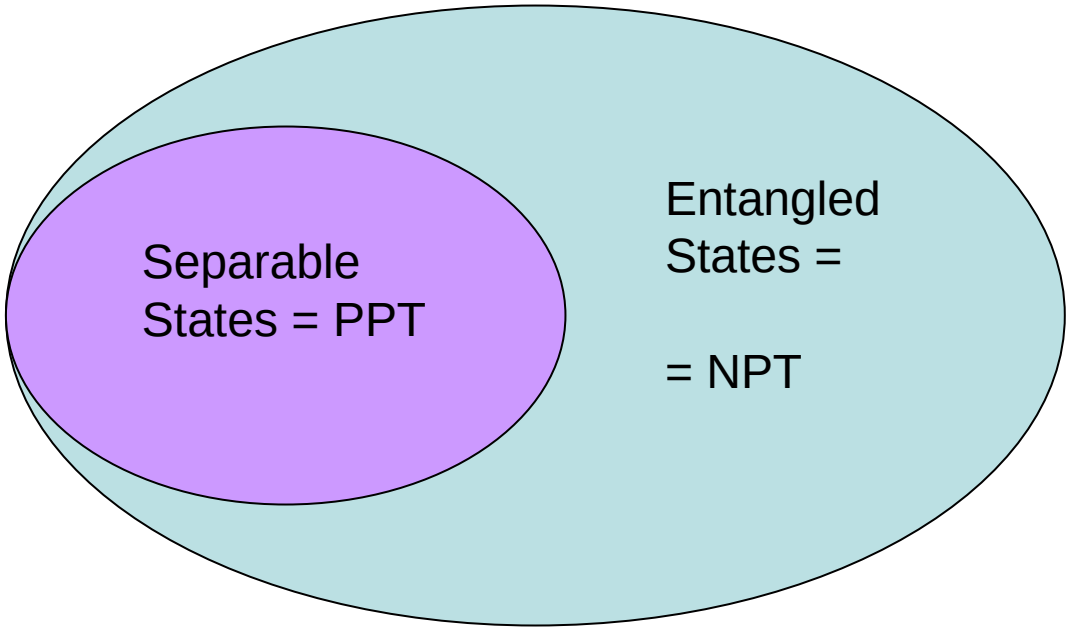
Problem: Given a state, verify if it is entangled or separable?

Two qubit case

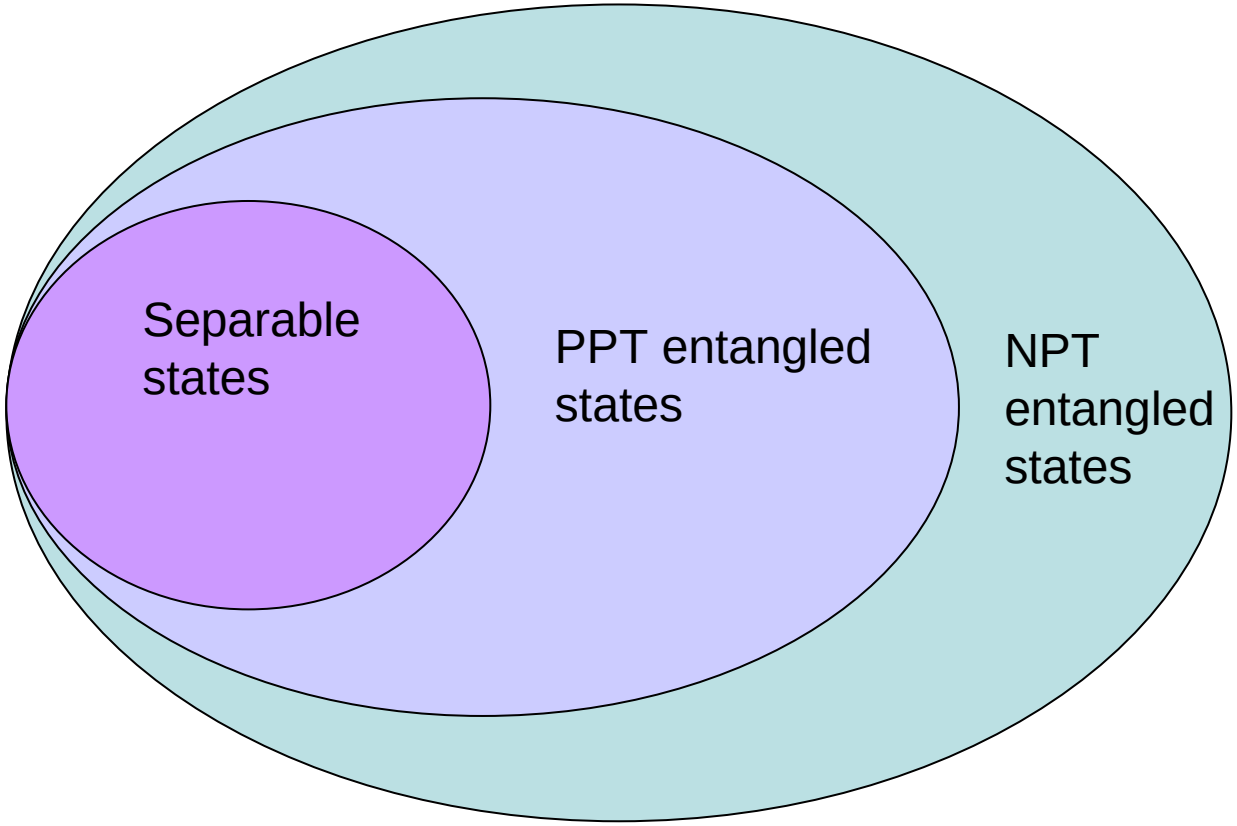
[Peres & Horodeccy ’96, Osaki ’80-ties etc.]

Theorem: For Hilbert space $C^2 \otimes C^2$ and $C^2 \otimes C^3$ a state is separable If and only if its ***partial transposition*** if a semidefinite positive matrix:

ρ is separable iff $\rho_{AB}^{T_B} \geq 0$ i.e. ρ is PPT



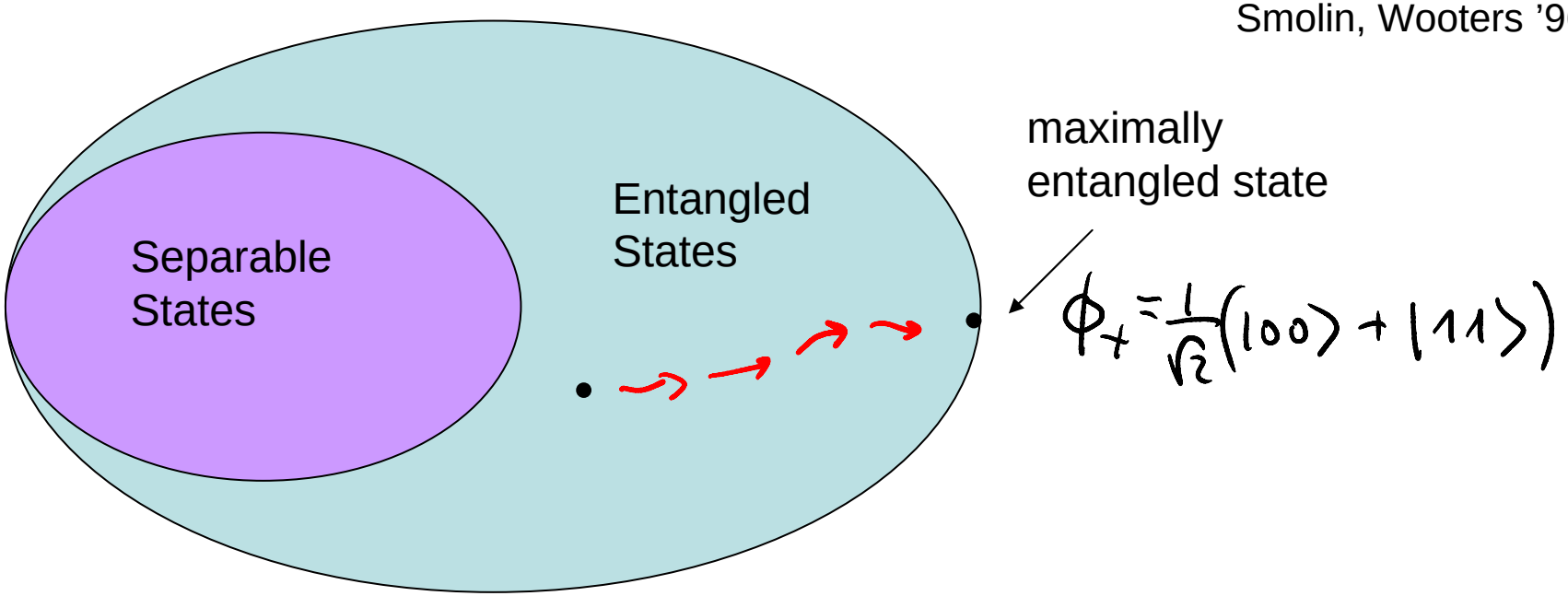
Higher dimension



There is no easy way to determine whether a given state is separable or not
- it is NP-hard problem (Gurvitz and Barnum)

Entanglement distillation (or purification)

[Bennett, Brassard, Popescu, Schumacher, Smolin, Wooters '96]



Distillation of entanglement:

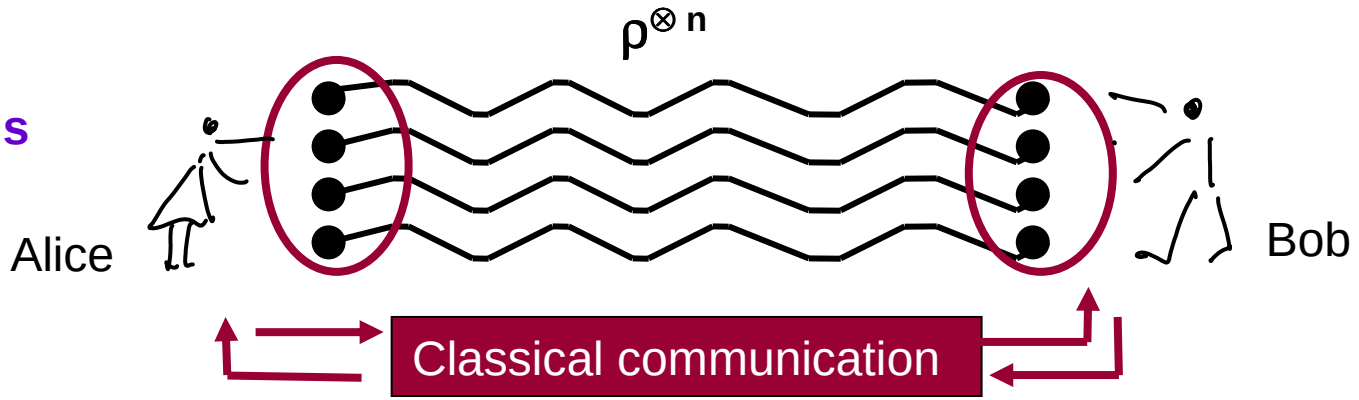
Obtaining (almost) maximally entangled state by means of

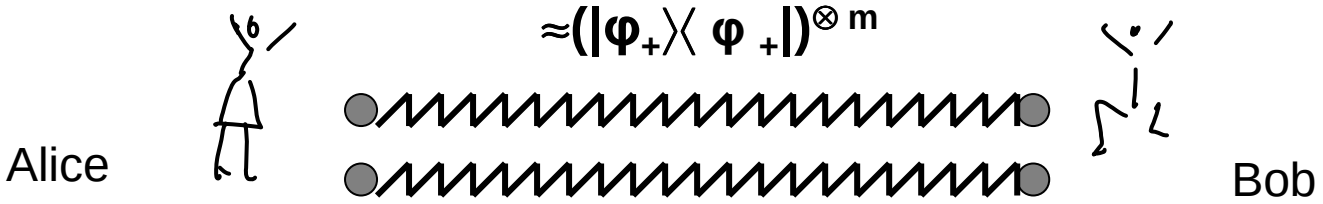
Local Operations and Classical Communication

Entanglement distillation

[Bennett, Brassard, Popescu, Smolin, Schumacher, Wooters Phys. Rev. Lett. 1996]

LOCC Operations



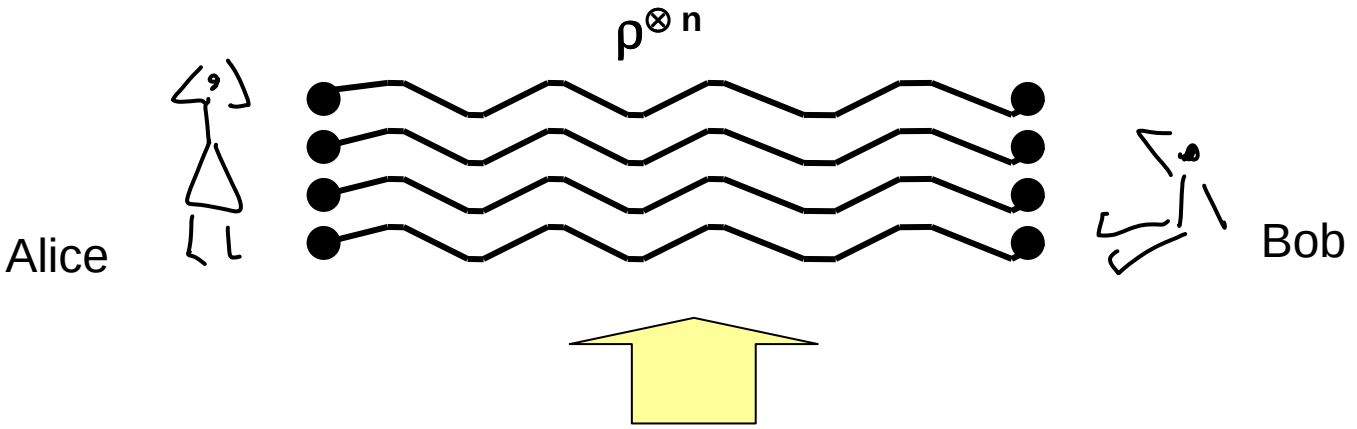


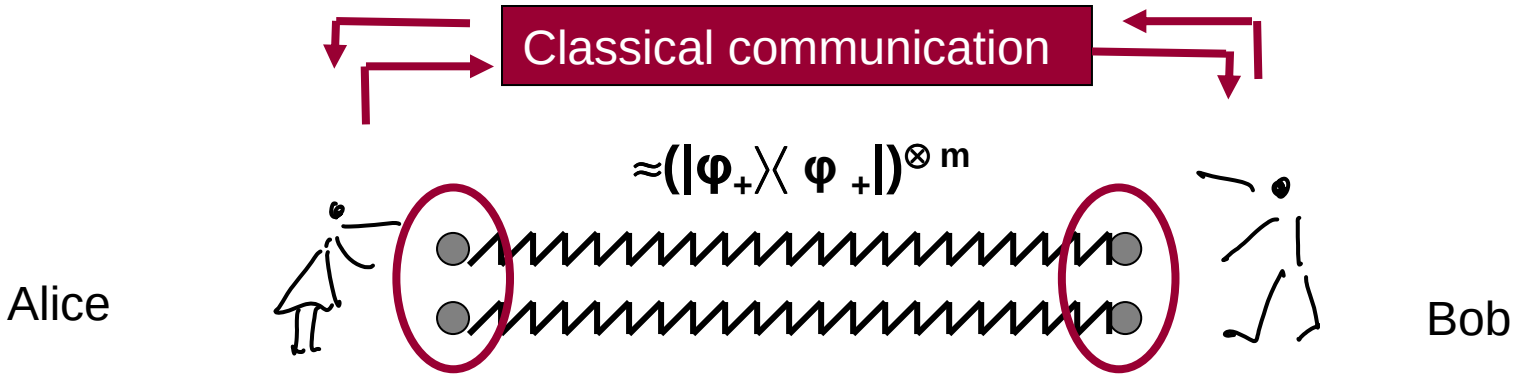
Df. Optimal protocol rate is called ***distillable entanglement*** $E_D(\rho)=\lim m/n$

$$E_D(\rho) \simeq \frac{\#\text{ copies of } \Phi_+}{\#\text{ copies of } \rho}$$

Entanglement formation

[Bennett, Brassard, Popescu, Smolin, Schumacher, Wooters Phys. Rev. Lett. 1996]



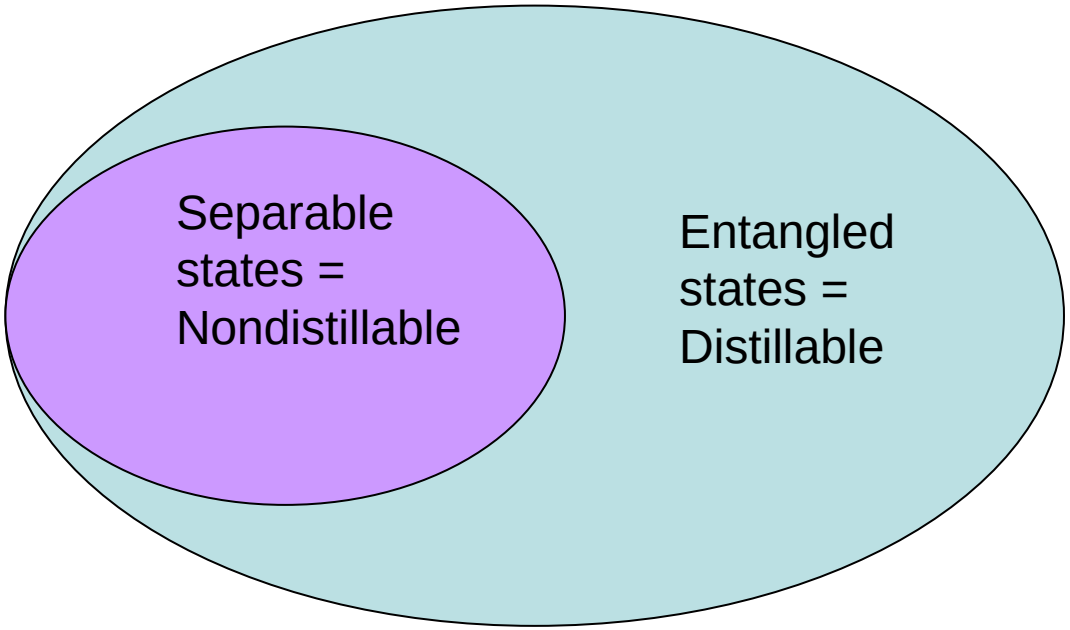


Df. Optimal protocol rate is called ***entanglement cost*** $E_C(\rho)=\lim m/n$

$$E_C(\rho) \simeq \frac{\#\text{ copies of } \phi_+}{\#\text{ copies of } \rho}$$

Two qubits

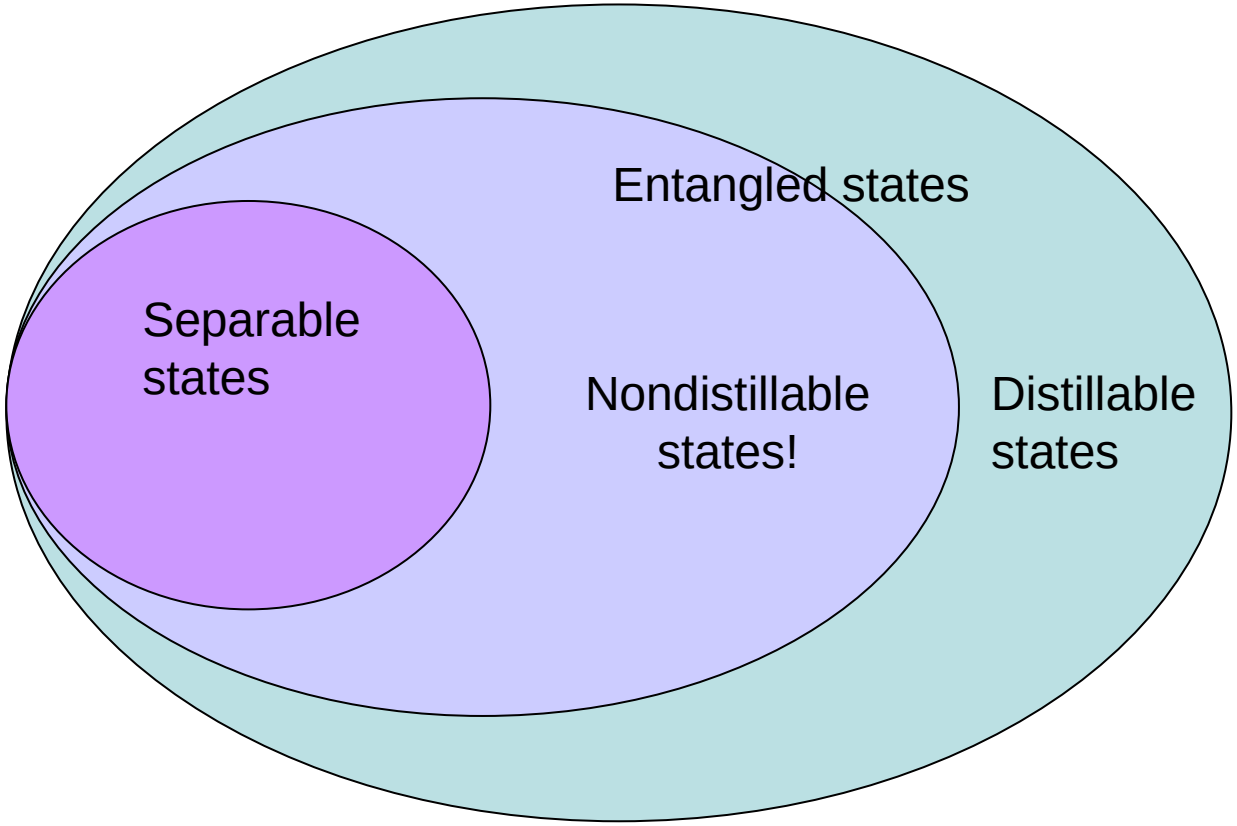
[Horodeccy ‘97]



Two qubit entanglement is always useful!

Higher dimension

[Horodeccy ‘98]



There exists a passive type of entanglement which does not allow for quantum communication: we have called it

Bound entanglement

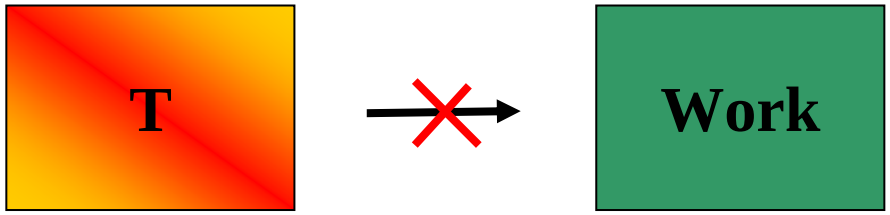
Thermodynamical analogy: basic irreversibility

[Horodeccy ‘98, Horodeccy & Oppenheim ’02]

entanglement – energy

quantum communication – performing work

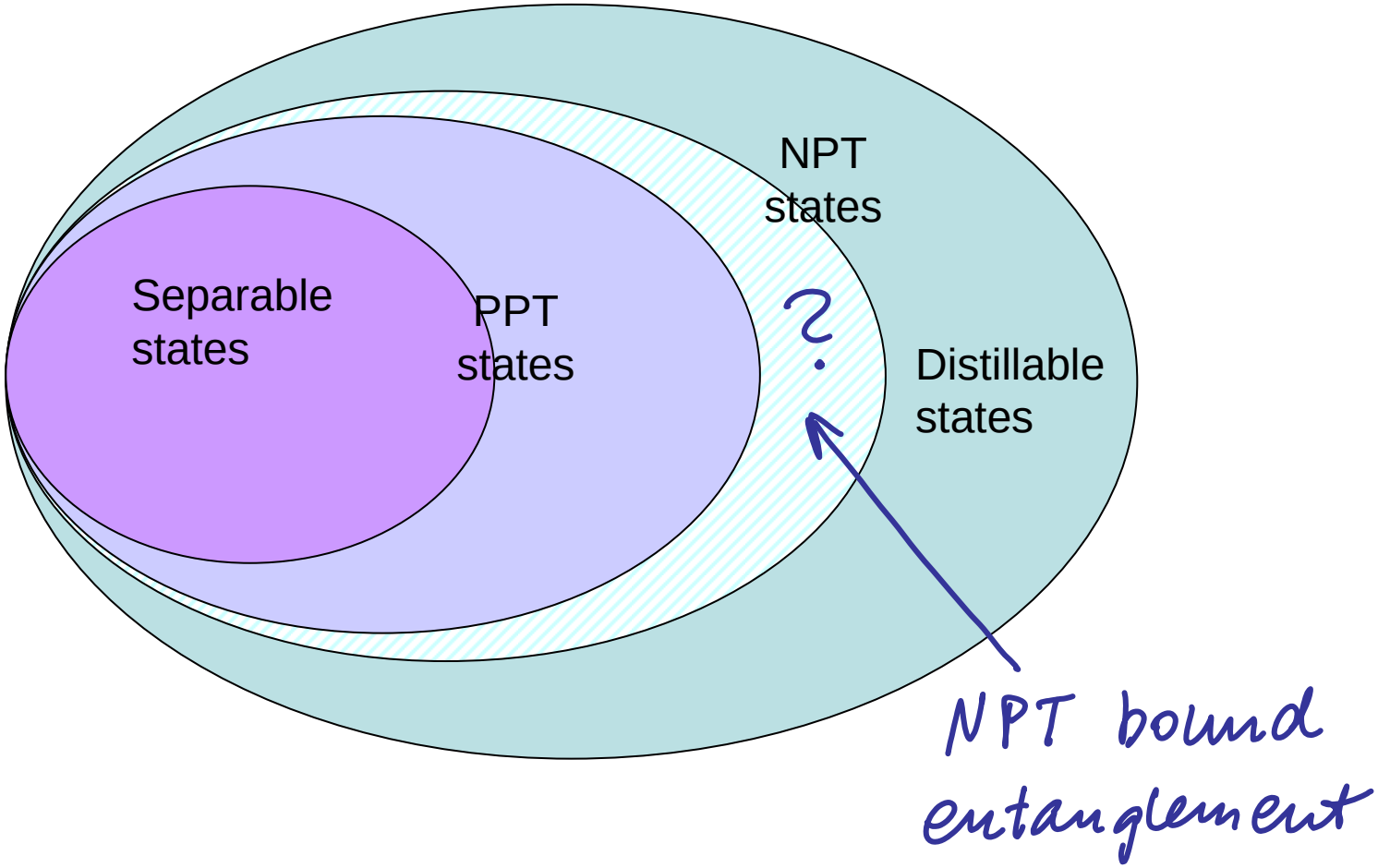
maximally entangled state – mechanical energy



Bound entanglement:
useless „energy”

Digression: Bound entanglement vs positive partial transpose

Fact: If a state has positive partial transpose (PPT) then it is not distillable



Is this set nonempty? Does NPT bound entanglement exist?

Papers related to the problem of existence of NPT bound entanglement

[1] D. P. Divincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
[2] M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach, J. Mod. Opt. **47**, 2481 (2000).
[3] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).
[4] B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. A **65**, 042327 (2002).
[5] S. Bandyopadhyay and V. Roychowdhury, Phys. Rev. A **68**, 022319 (2003).
[6] J. Watrous, Phys. Rev. Lett. **93**, 010502 (2004).
[7] L. Clarisse, Phys. Rev. A **71**, 032332 (2005).
[8] L. Clarisse, Quant. Inf. Comput. **6**, 539 (2006).
[9] R. O. Vianna and A. C. Doherty, Phys. Rev. A **74**, 052306 (2006).
[10] R. Simon, quant-ph/0608250.
[11] I. Chattopadhyay and D. Sarkar, quant-ph/0609050.
[12] F. G. S. L. Brandao and J. Eisert, quant-ph/0709.3835.
[13] Ł. Pankowski, M. Piani, M. Horodecki, and P. Horodecki, IEEE, quant-ph/0711.2613.
[14] Vogel arXiv/09xxxxxx
[15] Brandao, Horodecki, Pankowski, Smith, arXiv/11xxxxxx

L. Clarisse, arXiv:quant-ph/0612072, PhD Thesis
Entanglement Distillation; A Discourse on Bound Entanglement in Quantum Information Theory

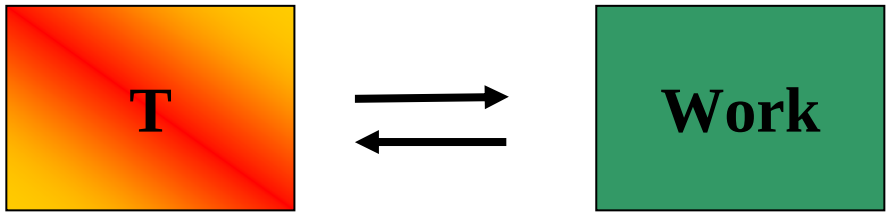
Regaining reversibility

[Brandao & Plenio 09]

Brandao and Plenio (Nature Physics 2009) considered a greater class of operations: non-entangling operations (actually ε-entangling operations).

Theorem: Under the above class, the process of formation is **reversible.**

$$\rho \rightleftarrows \phi_+$$

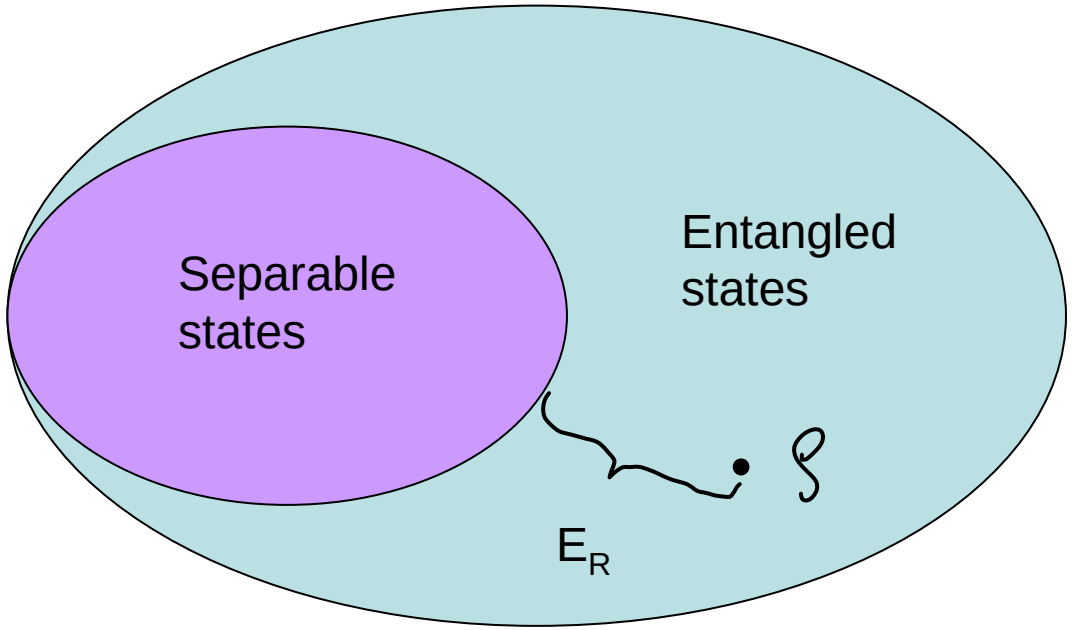


Non-entangling operations - „non-physical operations”

They establish analogue of the **First Law of Thermodynamics.**

Relative entropy of entanglement

[Plenio, Vedral, Rippin, Knight, 98]



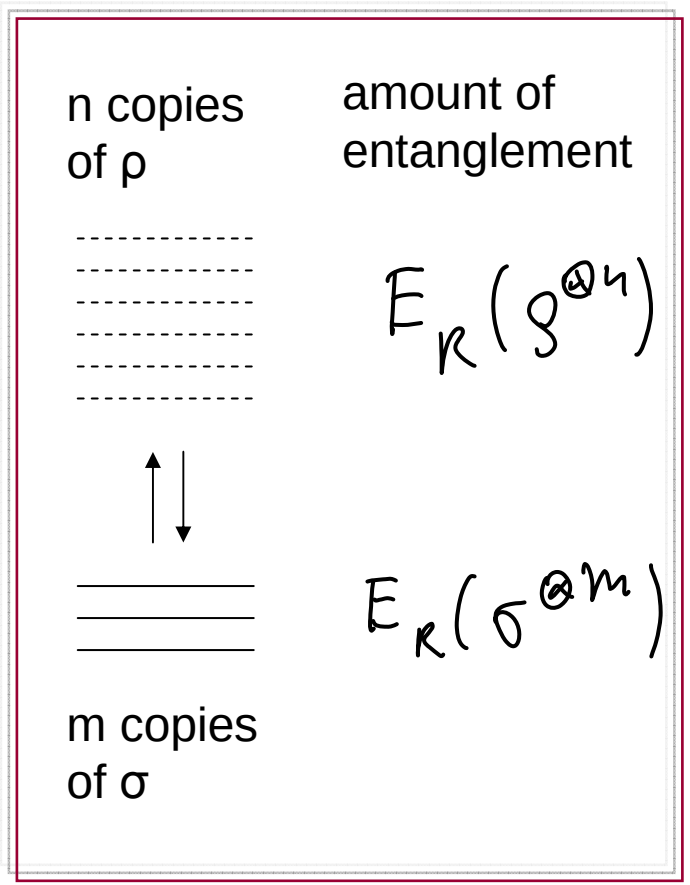
$$E_R = \inf_{\sigma \in SEP} S(\rho|\sigma)$$

with $S(\rho|\sigma) = Tr(\rho \log \rho) - Tr(\rho \log \sigma)$

E_R as a unique entanglement measure in the paradigm with non-entangling operations

Any entangled state can be transformed into any other entangled state, at the rate given by unique entanglement measure:

$$R(\rho \to \sigma) \simeq \frac{E_R^{\infty}(\sigma)}{E_R^{\infty}(\rho)}$$



where

$$E_R^{\infty}(\rho) = \lim_{n \to \infty} \frac{E(\rho^{\otimes n})}{n}$$

E_R^{∞} does not vanish for any entangled state (Brandao, Plenio, indep. proof – Marco Piani)

Distillation of private key

Problem: are e-bits the only states providing perfect key?

In other words:

Is private key related just to e-bits, or to entanglement in general?

- We can draw private key if we can distill e-bits.

- But can we draw private key from bound entangled states?

P-bits from bound entangled states

[Horodeccy & Oppenheim 04]

YES, we can draw p-bits from bound entangled states!

$$\Psi_{ABE} = |\phi_+\rangle_{AB}|+\rangle_E + |\phi_-\rangle_{AB}|-\rangle_E$$

$$\phi_\pm = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

1) Stupid Eve's strategy: measure in $\{|+\rangle, |-\rangle\}$ basis

2) Clever strategy: use interference!

Measure in $\{|0\rangle, |1\rangle\}$ basis:

$$\Psi_{ABE} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB}|0\rangle_E + |11\rangle_{AB}|1\rangle_E\right)$$

P-bits from bound entangled states

Let us destroy interference:

$$\Psi_{ABE} = |\phi_+\rangle_{AB}\,|\xi_+\rangle_{A'B'}\,|+\rangle_E + |\phi_-\rangle_{AB}\,|\xi_-\rangle_{A'B'}\,|-\rangle_E$$

Now Eve can get only the knowledge of type ϕ_+ or ϕ_-

The resulting state of Alice and Bob is now:

$$\rho_{AB\,A'B'} = \frac{1}{2}|\phi_+\rangle_{AB}\langle\phi_+| \otimes |\xi_+\rangle\langle\xi_+|_{A'B'} + \frac{1}{2}|\phi_-\rangle_{AB}\langle\phi_-| \otimes |\xi_-\rangle\langle\xi_-|_{A'B'}$$

Equivalent to e-bit ☹ (by LOCC Alice and Bob can distinguish flags)

P-bits from bound entangled states

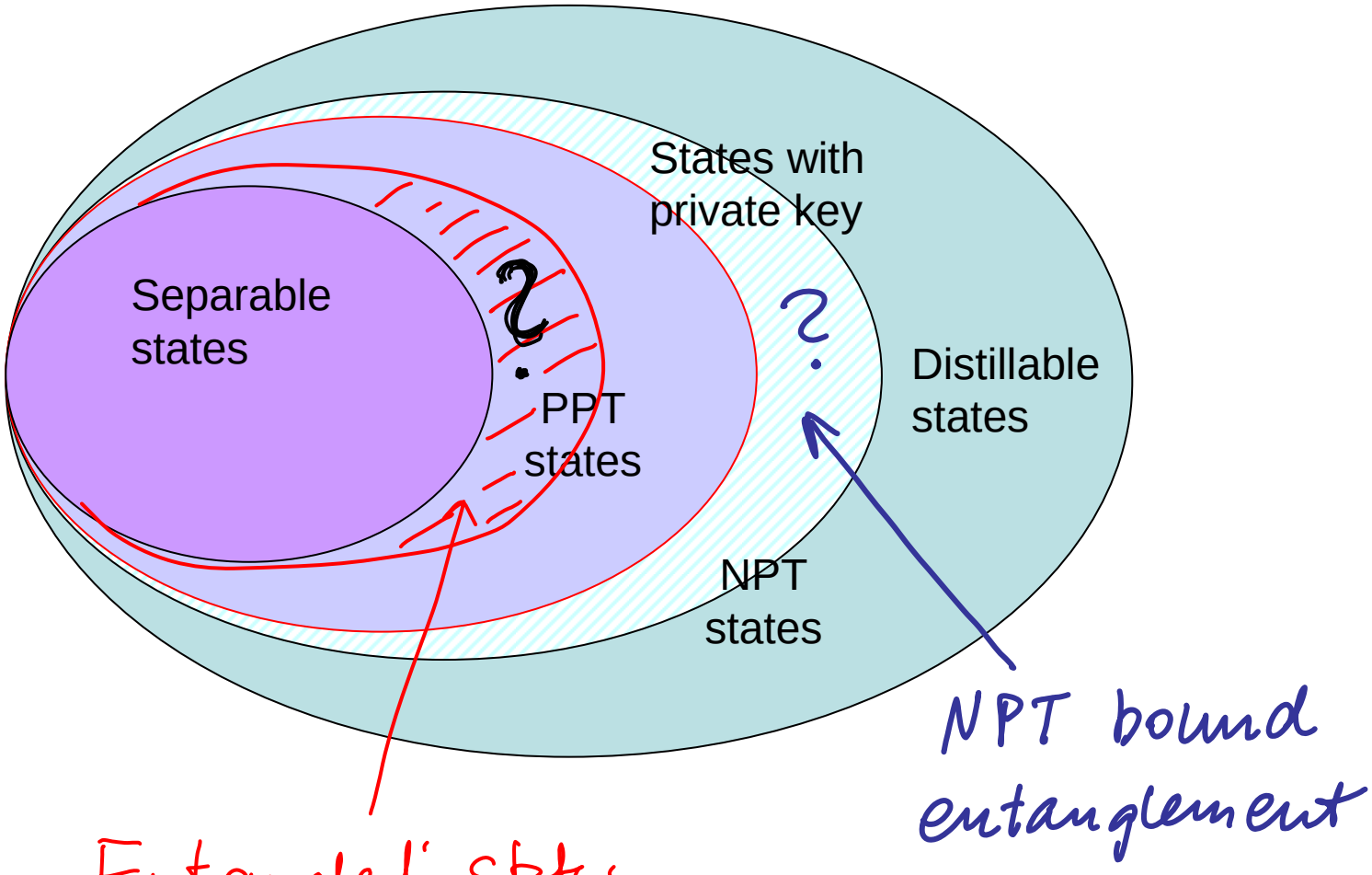
$$\tilde{\rho}_{AB\,A'B'} = \frac{1}{2}|\phi_+\rangle\langle\phi_+|_{AB} \otimes \rho^{+}_{A'B'} + \frac{1}{2}|\phi_-\rangle\langle\phi_-|_{AB} \otimes \rho^{-}_{A'B'}$$

where ρ_+ and ρ_- are so-called hiding states: it is hard to distinguish them by LOCC

The above state:

- Offers one perfect p-bit
- Does not allow to distill e-bit!

Conclusion: Private key – is due to entanglement in general, rather than pure entanglement


States with
private key
Separable
states
?
PPT
states
?
Distillable
states
NPT
states
Entangled states
with no private key?
NPT bound
entanglement