Limitations on quantum key repeaters

Karol Horodecki
University of Gdańsk

with Stefan Bäuml, Matthias Christandl and Andreas Winter

arXiv:1402.5927

Outline

- Background – entanglement swapping and quantum (key) repeaters protocols
- Motivation
- The main impossibility result
- The tools: private states, distillable key & properties
- Hiding security states
- Formal statements of the results & ideas of the proof
- Further limitations via entanglement measures
- Conclusions & Open questions

Entanglement swapping

Task: sending quantum signals at large distances

Problem: decoherence

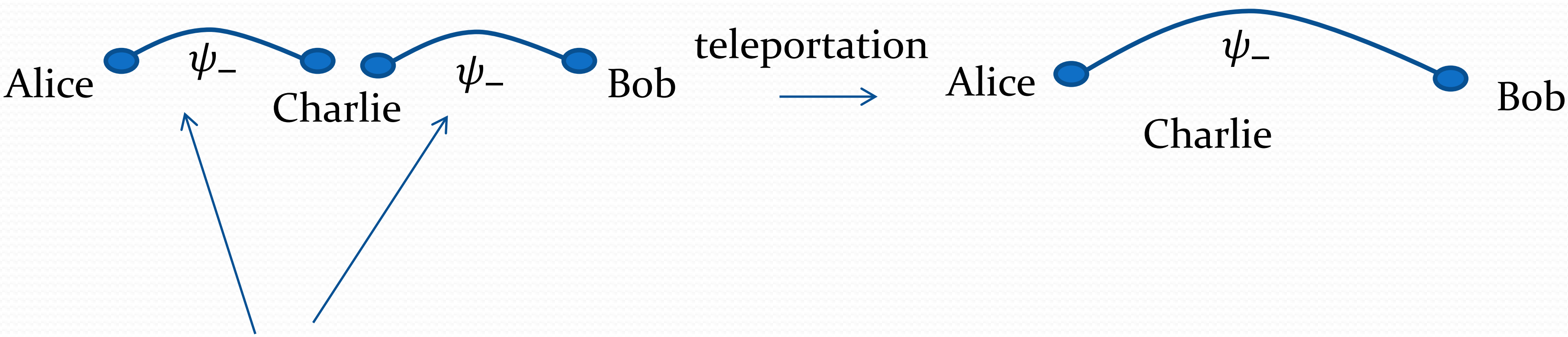
Classical solution: amplification of the signal

Quantum: amplification via coping is forbidded (no quantum ~~cloning~~ !)

[Wootters, Zurek 1982]

The wayout: quantum repeaters

A subprocedure: entaglement swapping



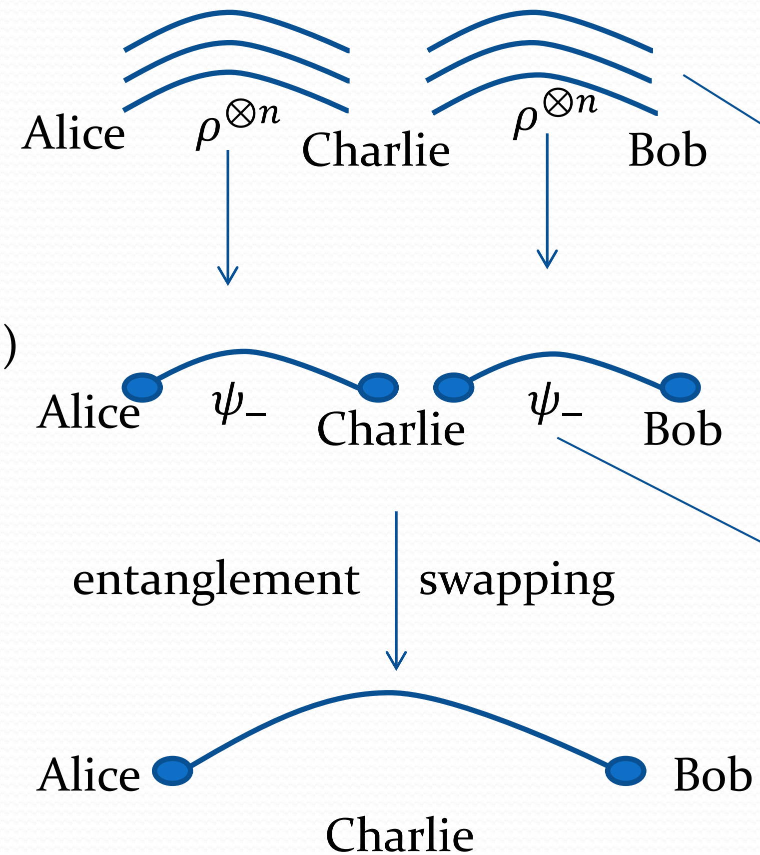
Ideal maximally entangled states
(e-bits)

[Żukowski et al. PRL 1993]

Quantum repeaters

[Briegel,Dür, Cirac 1998]

e-bits distillation
by Local Operations
& Classical
Communication (LOCC)



Many copies
of **noisy** distillable
entangled states

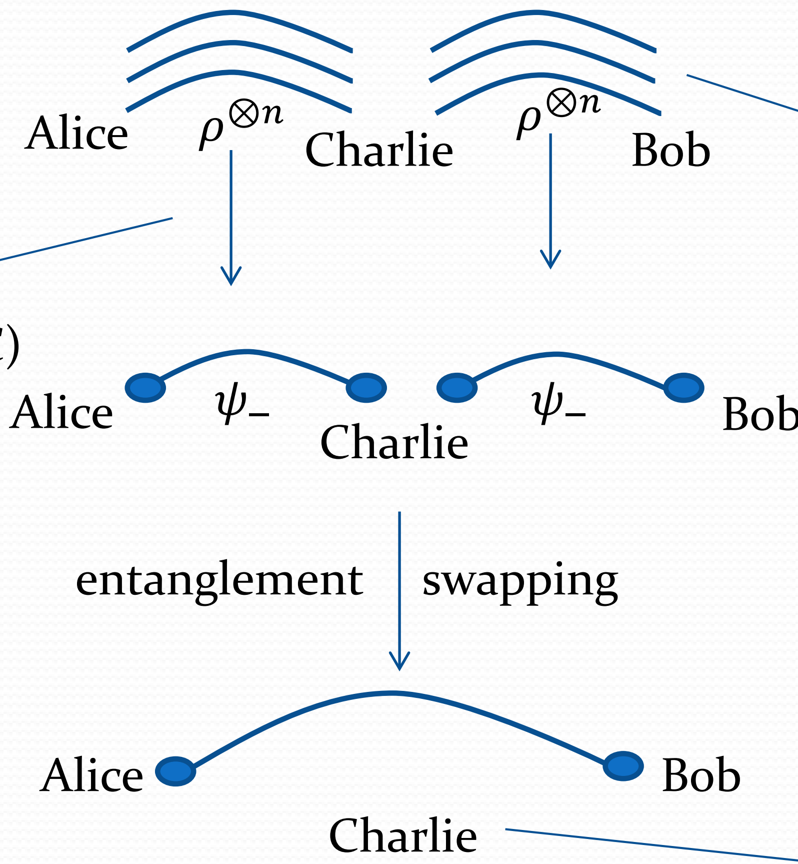
approximate
e-bit

approximate
e-bit

Quantum repeaters as quantum key repeaters

e-bits distillation
By Local Operations
And Classical
Communication (LOCC)

Many copies
of **noisy** distillable
entangled states



we need not trust him!

Finally: QKD between Alice and Bob via any entanglement based protocol like
BBM, E92, BHK '05

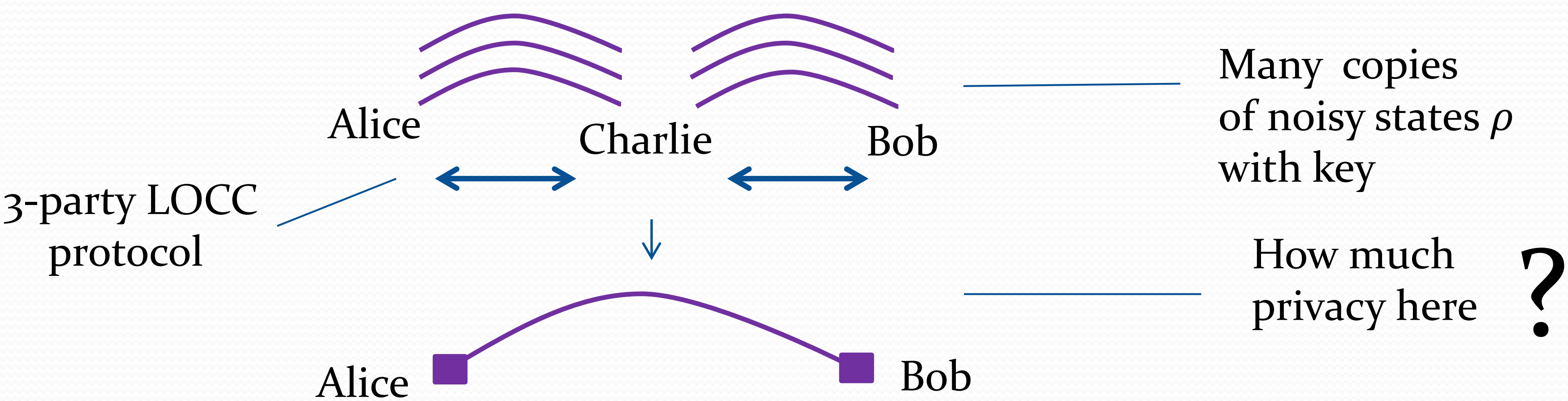
Motivation

There are **states** which have **key for QKD**, but are **useless for e-bit distillation**

Is there another **key swapping** or **quantum key repeaters protocol** which allows for distributing key using these states (does not use teleportation) ?

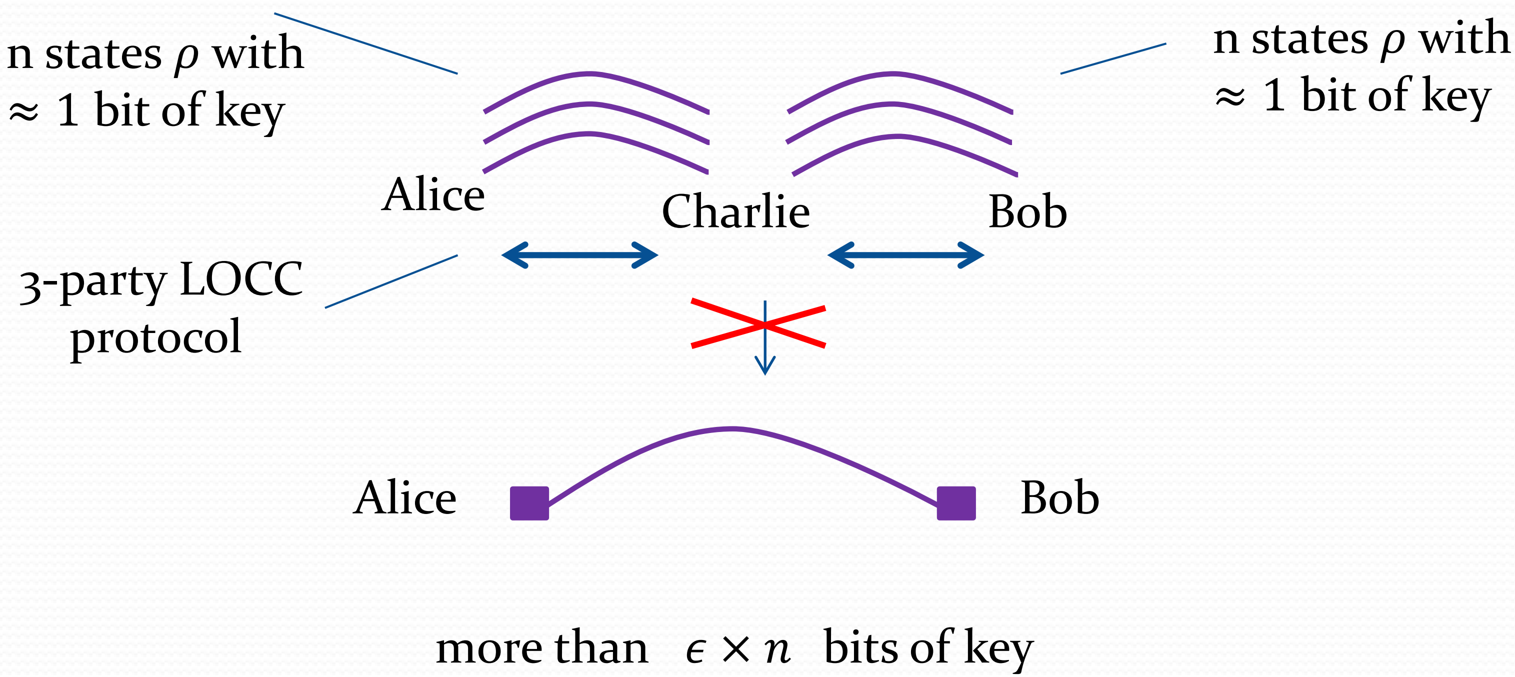
Resource: Noisy distillable state → Noisy state which has key

Protocol: Teleportation → arbitrary 3-party LOCC(A:B:C) protocol



Main result

For some of the states ρ which are useful for QKD, there does not exist efficient quantum key repeater



States with limited repeated key

some ρ which are PPT **approximate private bits** has limited repeated key

- Quantum states that has at least 1 bit of ideal key are called **Private bits**

Structure of private state: „twisted" singlet:

singlet „twisting"

$$\gamma_d = U\,[|\psi_+^d\rangle\langle\psi_+^d|_{AB} \otimes \rho_{A'B'}]\,U^{-1} \quad \text{where} \quad \psi_+^d = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle \quad U = \sum_{i,j=1}^{d}|ij\rangle_{AB}\langle ij| \otimes U_{A'B'}^{ij}$$

- Quantitatively: amount of privacy in state ρ is called **distillable key :**

$$K_D(\rho) = \inf_{\epsilon>0}\ \limsup_{n\to\infty}\ \sup_{\Lambda_n LOCC,\gamma_m}\left\{\frac{m}{n} : \Lambda_n(\rho^{\otimes n}) \approx_\epsilon \gamma_m\right\}$$

[K, M, P Horodeccy & J. Oppenheim PRL 2005]

- States with positive partial transposition (PPT) are useless for e-bit distillation (and teleportation)

$(I \otimes T)\rho_{AB} \geq 0$

[M,P,R. Horodeccy PRL 1998]

Notation: ρ^Γ

Why its use is limited for repeaters ?

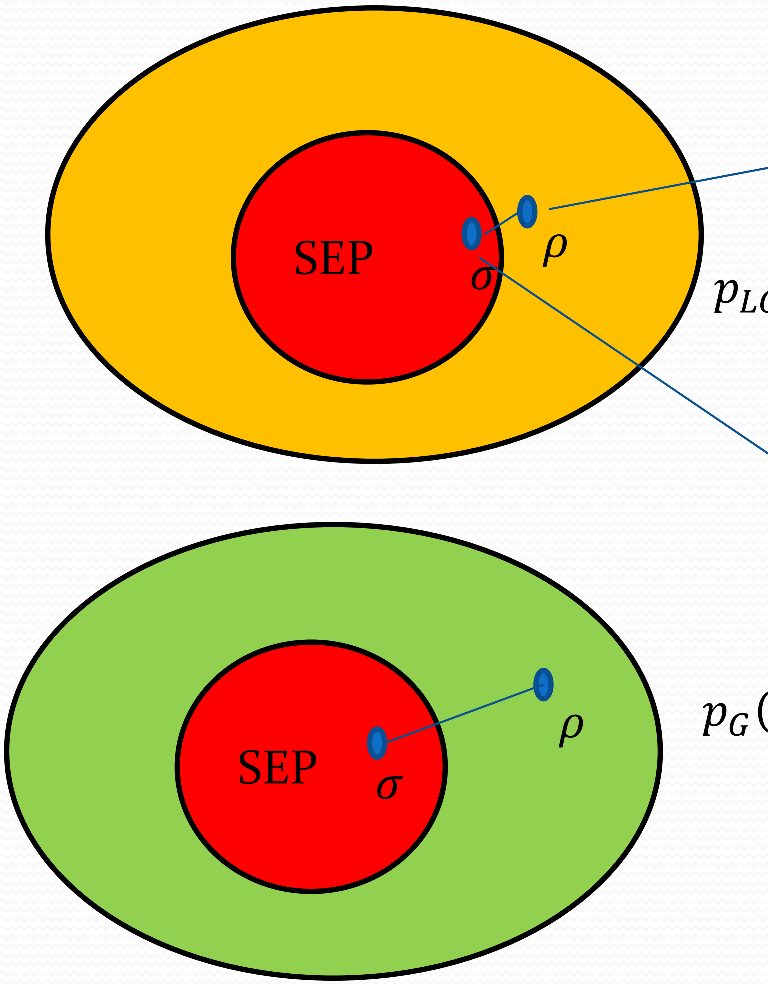
Back to example:

$K_D(\rho) \approx 1 \;\Rightarrow\;$ state useful for QKD secure under coherent attacks

Some approximate private bits can hide security

Alice and Bob in distance:

LOCC distinguishing



approximate private state

$$p_{LOCC}(\rho, \sigma) \leq \frac{1}{2} + \frac{c}{\sqrt{d}}$$

insecure (separable) state

Hiding security states

Alice and Bob meet:

Global distinguishing

$$p_G(\rho, \sigma) \approx 1$$

[see also K.H. Phd thesis ’08]

Limitations on key swapping

One can not swap key using hiding security states

Proof 'Ad absurdum': **suppose** the following **protocol P is possible**:

ρ ρ **P** $P(\rho \otimes \rho)$

Alice Charlie Bob $\longrightarrow$ Alice Bob

Hiding security states: $\exists\ \sigma : p_{LOCC}(\rho, \sigma) \approx \frac{1}{2}$

some **private state**

P $P(\sigma \otimes \sigma)$

Alice σ Charlie σ Bob $\longrightarrow$ Alice Bob

(separable) state

some **separable state**

Protocol **P'**(AB): Alice & Bob join labs and distinguish $P(\rho \otimes \rho)$ from $P(\sigma \otimes \sigma)$ pretty well!

The protocol **P**(A:B:C) + protocol **P'**(AB) of discrimination = P'' (AB : C) which distinguishes between ρ and σ ! → *CONTRADICTION* !

Asymptotic case – limits on quantum key repeaters

Asypmtotic definition of key repeater rate:

$$R_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}) = \underset{\epsilon>0}{inf}\ \underset{n\to\infty}{limsup}\ \underset{\Lambda_n LOCC,\gamma_m}{sup} \left\{\frac{m}{n} : Tr_C\Lambda_n\left((\rho_{AC_A} \otimes \tilde{\rho}_{C_B B})^{\otimes n}\right) \approx_\epsilon \gamma_{[m]}\right\}$$

Intermediate result:

$$R_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}) \leq D^{\infty}_{C\leftrightarrow AB}\ (\rho_{AC_A} \otimes \tilde{\rho}_{C_B \boldsymbol{B}})$$

$$R_{A\leftarrow C\rightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}) \leq D^{\infty}_{C\rightarrow AB}\ (\rho_{AC_A} \otimes \tilde{\rho}_{C_B \boldsymbol{B}})$$

Restricted Relative Entropy of Entanglement see [Piani PRL'09]

Main result:

$$R_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_A} \otimes \tilde{\rho}_{C_B B}) \leq D^{\infty}_{C\leftrightarrow AB}\ (\rho_{AC_A} \otimes \rho_{C_B \boldsymbol{B}}) = D^{\infty}_{C\leftrightarrow AB}\ ({\rho^{\Gamma}}_{AC_A} \otimes {\rho^{\Gamma}}_{C_B \boldsymbol{B}}) \leq 2E_R(\rho^{\Gamma})$$

Relative Entropy of Entanglement

(Similar bound for squashed entanglement)

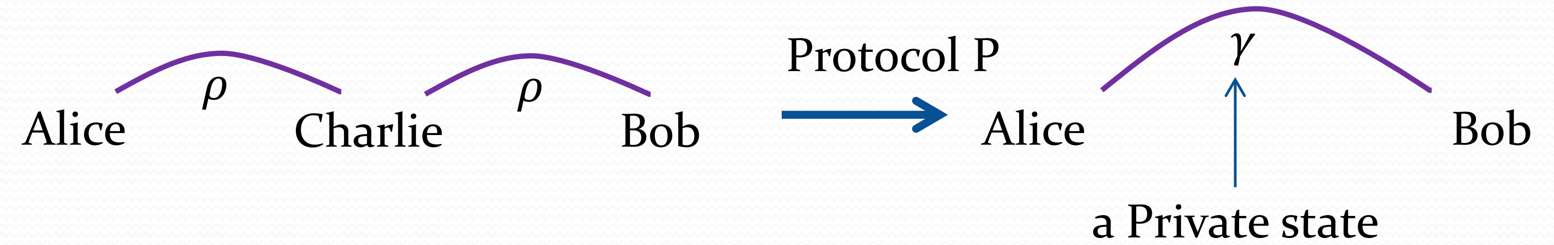
For Hiding security states: $\exists\, \sigma : ||\rho^{\Gamma} - \sigma^{\Gamma}|| < \frac{1}{\sqrt{d}}$

by asymptotoc continuity of $E_R \approx ||\rho^{\Gamma} - \sigma^{\Gamma}|| log\, d \approx 0$

There are bipartite states with $K_D \approx 1$, and $R \leq \frac{2 \log d}{\sqrt{d}} \approx 0$

Easy proof via partial transposition

For every protocol P of key swapping, which is LOCC(A:B:C) …



… there exist another protocol P1
which acts on partially transposed states , ρ^{Γ} with **THE SAME** output:

In summary: $R(\rho \otimes \rho) = R(\rho^{\Gamma} \otimes \rho^{\Gamma})$, => one line proof:

$$R(\rho \otimes \rho) = R(\rho^{\Gamma} \otimes \rho^{\Gamma}) \leq K_D(\rho^{\Gamma}) \leq E_R(\rho^{\Gamma}) \leq c||\rho^{\Gamma} - \sigma^{\Gamma}||\, log d \;\approx\; \frac{\log d}{\sqrt{d}} \to 0$$

Distillable secure key between
Alice and (Bob & Charlie)

Asymptotic continuity

Other bounds on key repeaters rate

Distillable entanglement E_D = Ratio: obtained e-bits / used states

Entanglement cost E_C = Ratio: obtained states / used e-bits

$$R_{A\leftarrow C\leftrightarrow B}(\rho_{AC_A}\otimes\tilde{\rho}_{C_BB}) \leq \frac{1}{2}E_D(\tilde{\rho}_{C_BB}) + \frac{1}{2}E_C(\rho_{AC_A}),$$

$$\begin{aligned} R_{A\leftarrow C\rightarrow B}(\rho_{AC_A}\otimes\tilde{\rho}_{C_BB}) &\leq \frac{1}{2}E_D^{C_A\rightarrow A}(\rho_{AC_A}) + \frac{1}{2}E_C(\tilde{\rho}_{C_BB}) \\ &\leq \frac{1}{2}E_D(\rho_{AC_A}) + \frac{1}{2}E_C(\tilde{\rho}_{C_BB}). \end{aligned}$$

Application: there is a PPT state $\rho\otimes\rho^\Gamma$ (almost P.T. invariant), for which $K_D(\rho\otimes\rho^\Gamma \otimes \rho\otimes\rho^\Gamma)\approx 1$, but $R(\rho\otimes\rho^\Gamma \otimes \rho\otimes\rho^\Gamma)\approx\frac{1}{2}$

Alice & Charlie's states

Charlie & Bob's state

Counterexample for entanglement of formation

Possible technique: degradation of key-swapping rate

Suppose there is entanglement monotone E such that:

1) $E(\rho_{out}) \leq pE_D(\rho_{AC_A}) + (1-p)E(\rho_{C_B B})$
for $0 < p < 1$

$\Rightarrow$ for a PPT state ρ_{AC_A} $(E_D = 0)$: **degradation of E** to $(1-p)^k E(\rho_{C_B B})$ **after using k times key swapping**

If in addition:

2) $R(\rho_{out}) \leq E(\rho_{out})$

One would have degradation of key repeater rate

Exemplary upper bounds: E_R, E_{sq}, E_F, E_C

Our result:

Entanglement of formation E_F and Entanglemen cost E_C does not satisfy the relation 1) i.e. can not be used to limit key repeaters by the above technique

Conclusions & Open problems

- There are states suitable for QKD, which essentially can not be shared at long distances via key repeaters
- Both in single copy and asymptotic case

Implications & some open problems

- Strong support for distillable-entanglement based quantum key repeaters. Is it that only distillable entanglement can be repeated ?
- What about the states invariant under partial transposition? [see K. H., Ł. Pankowski, M. P. Horodeccy PRL 2005 ; M. Ozols, G. Smith, J. Smolin PRL 2014]
- Supporting PPT-square conjecture [M. Christandl]
- More tight bounds ?

Commercial: Techniques and ideas presented here has far reaching applications: „Bounds on quantum non-locality via partial transposition"
K.H & Gláucia Murta arXiv:1407.6999 (DI QKD)

Thank you

for your attention!