Limitations on Quantum Key Repeaters

Stefan Bäuml, Matthias Christandl, Karol Horodecki,
Andreas Winter

14. January 2015

arXiv:1402.5927

Outline

1. Background
   - Bound Entanglement
   - Quantum Key Distribution
   - Entanglement Swapping
2. Quantum Key Repeaters
   - Key Swapping and Distinguishability
   - Main Result
   - Example
   - Second Result
   - Improvable?
3. Summary and Open Questions

Bound Entanglement

Maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle_{AB}.$$

Two ways of quantifying entanglement of mixed state ρ:

- $E_C(\rho)$: Amount of maximal entanglement necessary to create ρ by LOCC.
- $E_D(\rho)$: Amount of maximal entanglement obtainable from ρ by LOCC.

- Bound entanglement: $E_C(\rho) > 0$ and $E_D(\rho) = 0$.
- PPT entangled $\Rightarrow$ bound entangled.

Quantum Key Distribution

- Goal: Secure communication between Alice and Bob in presence of Eve.
- Requiring secret key, i.e. classical state completely correlated between Alice and Bob but completely uncorrelated to Eve. Eve assumed to have quantum memory:

$$\rho_{ABE}^{\text{key}} = \frac{1}{d}\sum_{i=0}^{d-1} |ii\rangle\langle ii|_{AB} \otimes \rho_E$$

- Obtainable by measuring $|\Psi\rangle\langle\Psi|_{AB}$ in computational basis.
- Maximal entanglement necessary? What about bound entanglement?

Quantum Key Distribution

- Horodecki et al. 2005: Security iff Alice and Bob have *private state* (or *pdit*):

$$\gamma^d_{AA'BB'} = U^{\text{twist}} |\Psi\rangle\langle\Psi|_{AB} \otimes \sigma_{A'B'} U^{\text{twist}\dagger}$$
$$= \frac{1}{d} \sum_{ij=0}^{d-1} \underbrace{|ii\rangle\langle jj|_{AB}}_{\text{measure!}} \otimes \underbrace{U^{(i)} \sigma_{A'B'} U^{(j)\dagger}}_{\text{keep away from Eve!}},$$

  where $U^{\text{twist}} = \mathbf{1}_A \otimes \sum_i |i\rangle\langle i|_B \otimes U^{(i)}$. Worst case scenario: Eve allowed to have purification.

- Measure of key

$$K_D(\rho) = \lim_{\epsilon\to 0} \lim_{n\to\infty} \sup_{\Lambda_n \text{ LOCC}, \gamma^d \text{pdit}} \left\{ \frac{\log d}{n} : \|\Lambda_n(\rho^{\otimes n}) - \gamma^d\|_1 \leq \epsilon \right\}$$

- $K_D \gg E_D = 0$ possible. $\exists$ PPT states arbitrarily close to pdits.

Example (Horodecki et al. 2005):

- Quantum data hiding: σ^+_{AB} and σ^-_{AB} indistinguishable by LOCC operations, distinguishable by global operations:

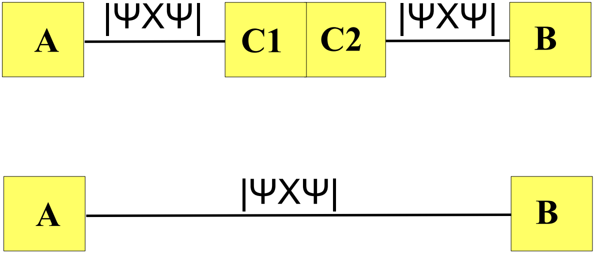
$$\rho_{bAB} = \frac{1}{2}|0\rangle\langle 0|_b \otimes \sigma^+_{AB} + \frac{1}{2}|1\rangle\langle 1|_b \otimes \sigma^-_{AB}$$

- Hide the entanglement

$$\rho^{\text{flag}}_{ABA'B'} = \frac{1}{2}|\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \sigma^+_{A'B'} + \frac{1}{2}|\Phi^-\rangle\langle\Phi^-|_{AB} \otimes \sigma^-_{A'B'}$$

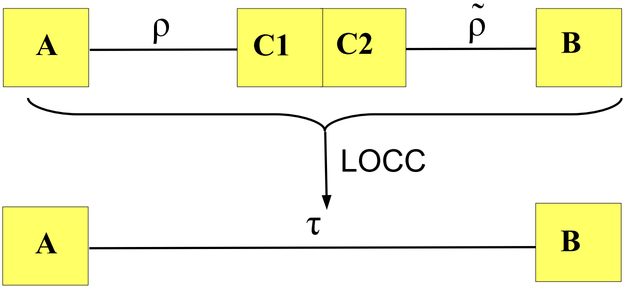
- $K_D \approx 1$, $E_D \approx 0$. For separable $\sigma^\pm$, ρ^{flag} obtainable from $|\Phi^+\rangle\langle\Phi^+|$ by LOCC, hence $E_C(\rho^{\text{flag}}) \leq 1$.

Entanglement Swapping



- Application: Distribution of maximally entangled states over long absorptive channels.
- Absorption scaling exponentially with the length of the channel. Divide channel into segments, distribute entanglement between nodes and connect by swapping.

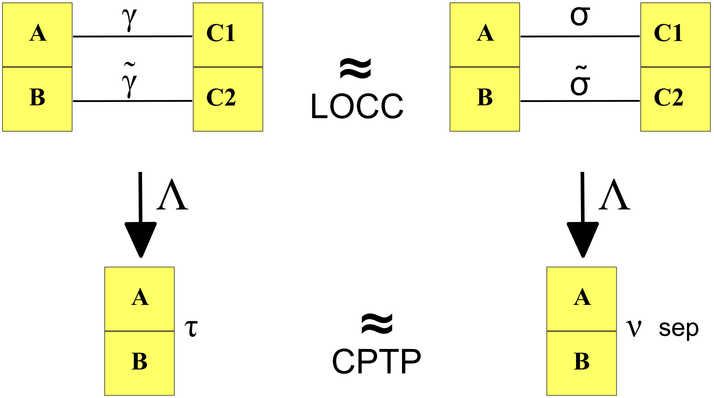
Quantum Key Swapping?



- Arbitrary states ρ and $\tilde{\rho}$ between the nodes. For example private states.
- General LOCC protocol performed by Alice, Charlie and Bob.
- Resulting state τ useful for QKD?

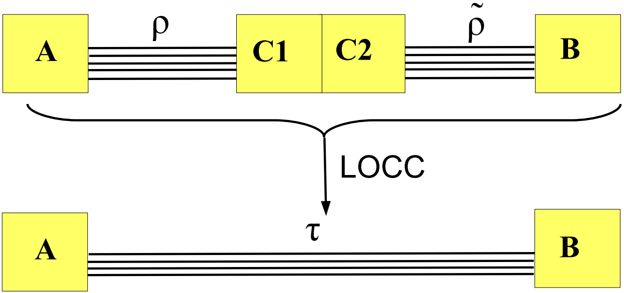
Key Swapping and Distinguishability

- Private states γ almost indistinguishable from separable states σ and $\tilde{\sigma}$ by LOCC.
- Alice and Bob sharing lab.



$K_D(\tau) \approx 0$

Many Copies: Quantum Key Repeater



- n copies of ρ and $\tilde{\rho}$ between the nodes.
- Resulting in k states τ close to private bit.
- *Repeatable Key*: $K_{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_1} \otimes \tilde{\rho}_{C_2B}) \approx \frac{k}{n}$: Key rate achievable by LOCC operation.

Main Result

- Upper bound on $K_{A\leftrightarrow C\leftrightarrow B}$ using entanglement measures.

Theorem

Let ρ and $\tilde{\rho}$ be PPT. Then

$$K_{A\leftrightarrow C\leftrightarrow B}(\rho \otimes \tilde{\rho}) \leq \min\left\{K_D(\rho^\Gamma), K_D(\tilde{\rho}^\Gamma)\right\}$$
$$\leq \min\left\{E_R^\infty(\rho^\Gamma), E_R^\infty(\tilde{\rho}^\Gamma), E_{sq}(\rho^\Gamma), E_{sq}(\tilde{\rho}^\Gamma)\right\},$$

where the transpose is taken w.r.t. Charlie's subsystems.

- Proof using PT invariance of $K_{A\leftrightarrow C\leftrightarrow B}$, LOCC monotonicity of the key as well as fact that E_R^∞ and E_{sq} upper bound key.

Example: PPT state close to p-bit

- PPT state with high key and transpose close to separable state.
- Idea: Mix private state with separable state to get PPT state.

$$\rho_d = \frac{1}{2}\begin{bmatrix} (1-p)\sqrt{XX^\dagger} & 0 & 0 & (1-p)X \\ 0 & p\sqrt{YY^\dagger} & 0 & 0 \\ 0 & 0 & p\sqrt{Y^\dagger Y} & 0 \\ (1-p)X^\dagger & 0 & 0 & (1-p)\sqrt{X^\dagger X} \end{bmatrix}$$

with $p = \frac{1}{\sqrt{d}+1}$, $X = \frac{1}{d\sqrt{d}}\sum_{i,j=1}^{d} u_{ij}|ij\rangle\langle ji|$ and $Y = \sqrt{d}X^\Gamma$.

$$\rho_d^\Gamma = \frac{1}{2}\begin{bmatrix} (1-p)\sqrt{XX^\dagger} & 0 & 0 & 0 \\ 0 & p\sqrt{YY^\dagger} & pY & 0 \\ 0 & pY^\dagger & p\sqrt{Y^\dagger Y} & 0 \\ 0 & 0 & 0 & (1-p)\sqrt{X^\dagger X} \end{bmatrix} \geq 0,$$

since $\sqrt{XX^\dagger} \geq 0$ and $\sqrt{X^\dagger X} \geq 0$ and middle block private bit.

Example: PPT state close to p-bit

- Dephase first qubit of Alice's system $\Rightarrow$ separable state.

$$\sigma_d = \frac{1}{2}\begin{bmatrix} (1-p)\sqrt{XX^\dagger} & 0 & 0 & 0 \\ 0 & p\sqrt{YY^\dagger} & 0 & 0 \\ 0 & 0 & p\sqrt{Y^\dagger Y} & 0 \\ 0 & 0 & 0 & (1-p)\sqrt{X^\dagger X} \end{bmatrix},$$

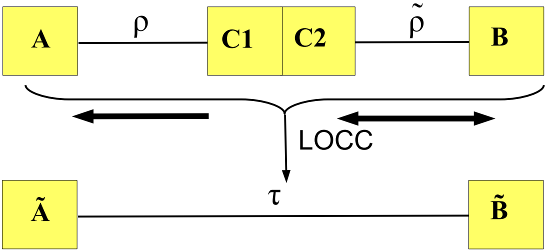
$$\|\rho_d^\Gamma - \sigma_d\|_1 = \frac{1}{\sqrt{d}+1}.$$

- Hence,

$$1 \approx K_D(\rho) > K_{A\leftrightarrow C\leftrightarrow B}(\rho\otimes\rho) \approx 0.$$

- Demonstrated experimentally with $X = \text{SWAP}$ and $d = 2$ (Dobek et al, PRL 106, 030501).

Second Result

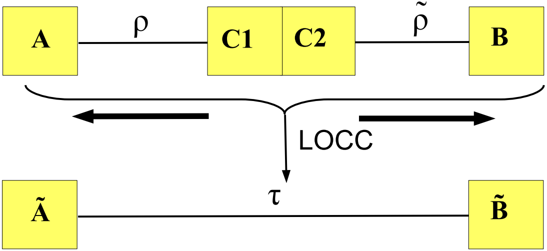


Theorem

For input states ρ_{AC_1} and $\tilde{\rho}_{C_2B}$ it holds

$$K_{A\leftarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})\leq\frac{1}{2}E_D(\tilde{\rho}_{C_2B})+\frac{1}{2}E_C(\rho_{AC_1}).$$

Second Result



Theorem

For input states ρ_{AC_1} and $\tilde{\rho}_{C_2B}$ it holds

$$K_{A\leftarrow C\rightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})\leq\frac{1}{2}E_D^{C_2\rightarrow B}(\tilde{\rho}_{C_2B})+\frac{1}{2}E_C(\rho_{AC_1}).$$

Second Result

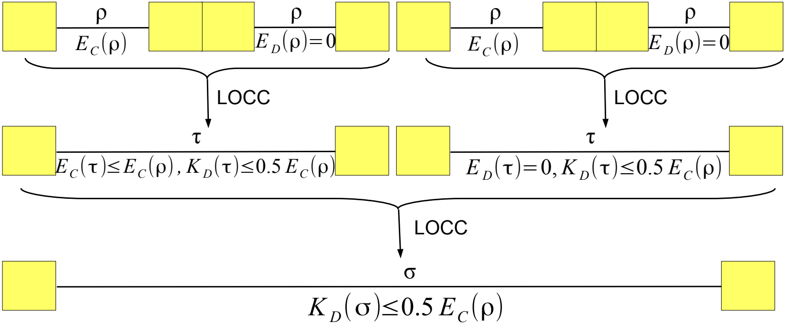
Theorem

For input states ρ_{AC_1} and $\tilde{\rho}_{C_2B}$ it holds

$$K_{A\leftarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \le \frac{1}{2}E_D(\tilde{\rho}_{C_2B}) + \frac{1}{2}E_C(\rho_{AC_1}),$$
$$K_{A\leftarrow C\rightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \le \frac{1}{2}E_D^{C_2\rightarrow B}(\tilde{\rho}_{C_2B}) + \frac{1}{2}E_C(\rho_{AC_1}).$$

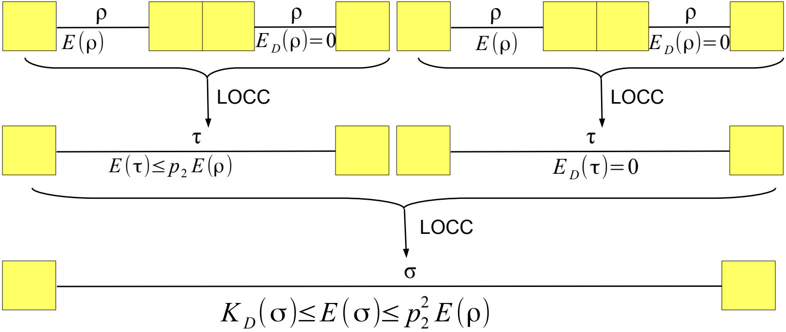
- Nontrivial bound if $\tilde{\rho}$ bound entangled.
- For $\rho = \tilde{\rho} = \rho^{\text{flag}}$, $E_D \approx 0$ and $E_C \le 1 \Rightarrow K_D$ reduced significantly by swapping.
- Also applicable for NPT states, e.g. possible NPT bound entanglement.
- Nontrivial results for PPT invariant entangled states, where first result does not work.
- Proof idea: First show result for $E_{sq} \ge K_D$ and E_F.

Improvable?


ρ
$E_C(\rho)$
ρ
$E_D(\rho)=0$
ρ
$E_C(\rho)$
ρ
$E_D(\rho)=0$
LOCC
LOCC
τ
$E_C(\tau)\leq E_C(\rho), K_D(\tau)\leq 0.5\,E_C(\rho)$
τ
$E_D(\tau)=0, K_D(\tau)\leq 0.5\,E_C(\rho)$
LOCC
σ
$K_D(\sigma)\leq 0.5\,E_C(\rho)$

Improvable?

- Can we get a better bound?
- Assume $K_D(\tau) \leq E(\tau) \leq p_1 E_D(\tilde{\rho}) + p_2 E(\rho)$



Counterexample for E_C and E_F

- Maximally correlated states $\rho_{AB} = \sum_{ik=0}^{d-1} a_{ik} |ii\rangle\langle kk|$.
- Purification $|\Psi\rangle_{ABE} = \frac{1}{\sqrt{d}} \sum_i |ii\rangle \otimes |u_i\rangle$.
- $E_D(\rho_{AB}) = E_R(\rho_{AB}) = S(A)_\rho - S(AB)_\rho$.
- $E_C(\rho_{AB}) = E_F(\rho_{AB}) = S(A)_\rho - I_{\text{acc}}\left(\left\{\frac{1}{d}, |u_i\rangle\right\}\right)$, where $I_{\text{acc}}\left(\left\{\frac{1}{d}, |u_i\rangle\right\}\right) = \sup_{\{A_j\}\ \text{POVM}} I(i:j)$.
- ρ and $\tilde{\rho}$ maximally correlated $\Rightarrow$ τ maximally correlated for standard swapping protocol.
- For every outcome μ, resulting state purified by state with ensemble $\left\{\frac{1}{d}, |u_i^{(1)}\rangle \otimes |u_{i+\mu}^{(2)}\rangle\right\}$.
- $E_F(\tau) \leq pE_D(\rho^2) + (1-p)E_F(\rho^1)$ implies

$$\frac{1}{d} \sum_\mu I_{\text{acc}}\left(\left\{\frac{1}{d}, |u_i^{(1)}\rangle \otimes |u_{i+\mu}^{(2)}\rangle\right\}\right) \geq pS(\tilde{\rho}).$$

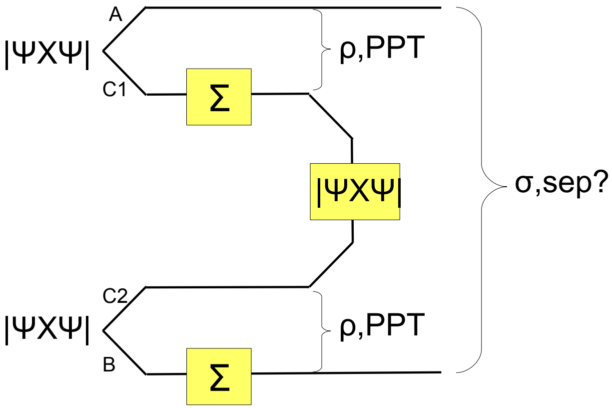
- Counterexample by random construction.

Summary

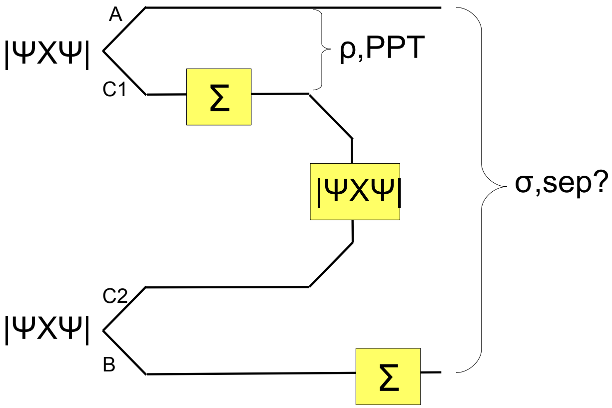
- Limitations on the entanglement of the output state of a quantum key repeater protocol.
- Upper bounds on the key rate achievable from the output. Depend on entanglement measures of input states or their transpose.
- Examples of bound entangled or nearly bound entangled input states where key is lost or significantly reduced in the repeater protocol.
- Support of the PPT^2 Conjecture: $\Sigma^{\mathrm{PPT}} \circ \Sigma^{\mathrm{PPT}} = \Sigma^{\mathrm{EB}}$.

The PPT^2 Conjecture

Different interpretation of PPT entanglement swapping for locally maximally mixed states using Jamiolkowski isomorphism:

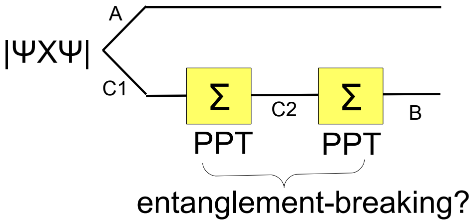


Different interpretation of PPT entanglement swapping for locally maximally mixed states using Jamiolkowski isomorphism:



The PPT^2 Conjecture

Teleport C_1-part of ρ_{AC_1} to B via $|\Psi\rangle\langle\Psi|_{C_2 B}$:



If Conjecture true, PPT entanglement useless in repeater.

Open Problems

- Only distillable entanglement preserved in a quantum repeater?
- Other inequalities between entanglement measures of in- and output states (c.f. results by Gour, Sanders and Lee)?
- $E(\tau) \leq p_1 E_D(\rho) + p_2 E(\tilde{\rho})$ for entanglement measure E other than E_C or E_F?
- Results for smaller shield dimensions as realised in experiments?
- Possibility of different kind of quantum key repeater protocols beyond distillation?

Thank you for your attention!

arXiv:1402.5927