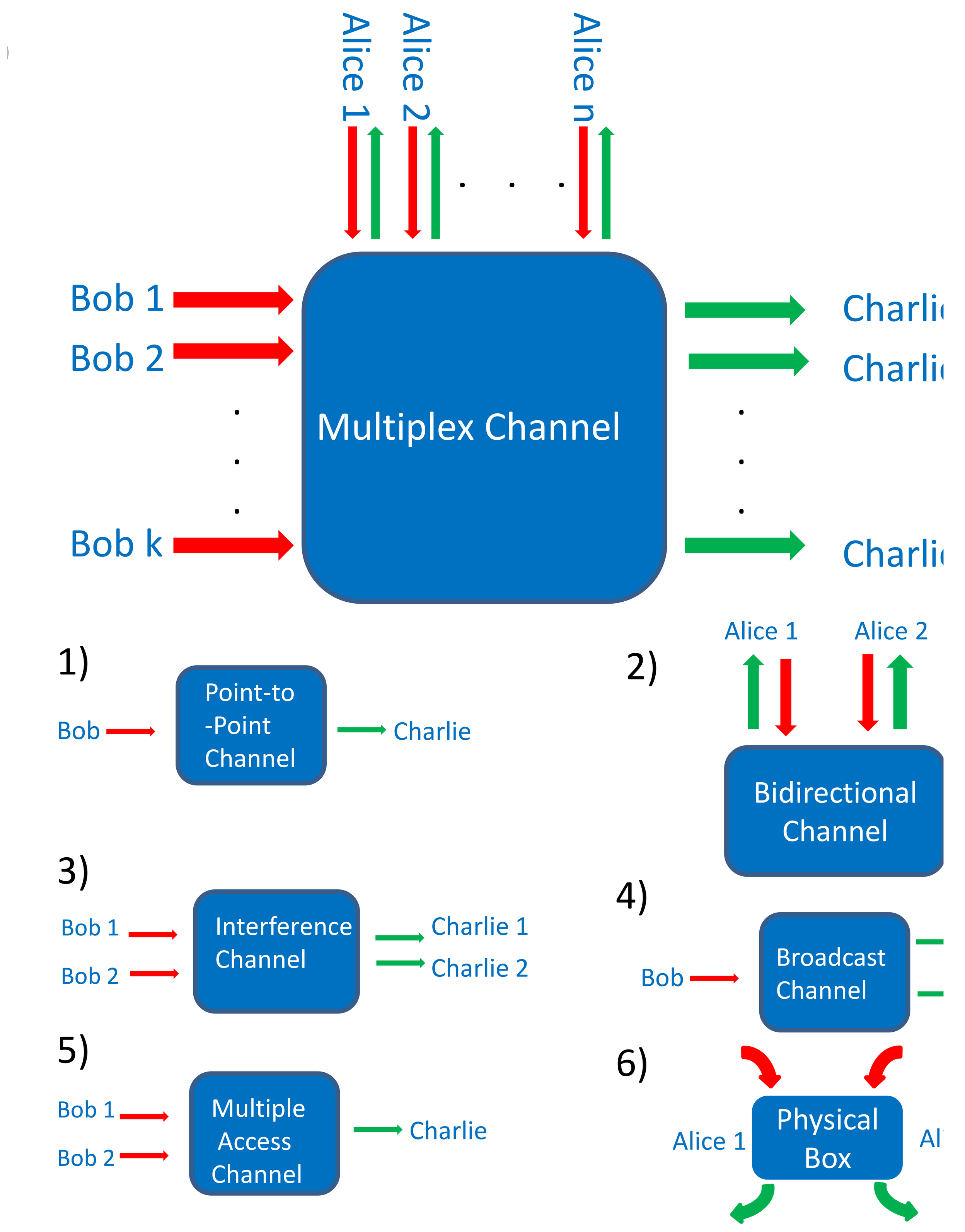
Universal limitations on quantum key distribution over a network

Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki

arXiv:1912.03646

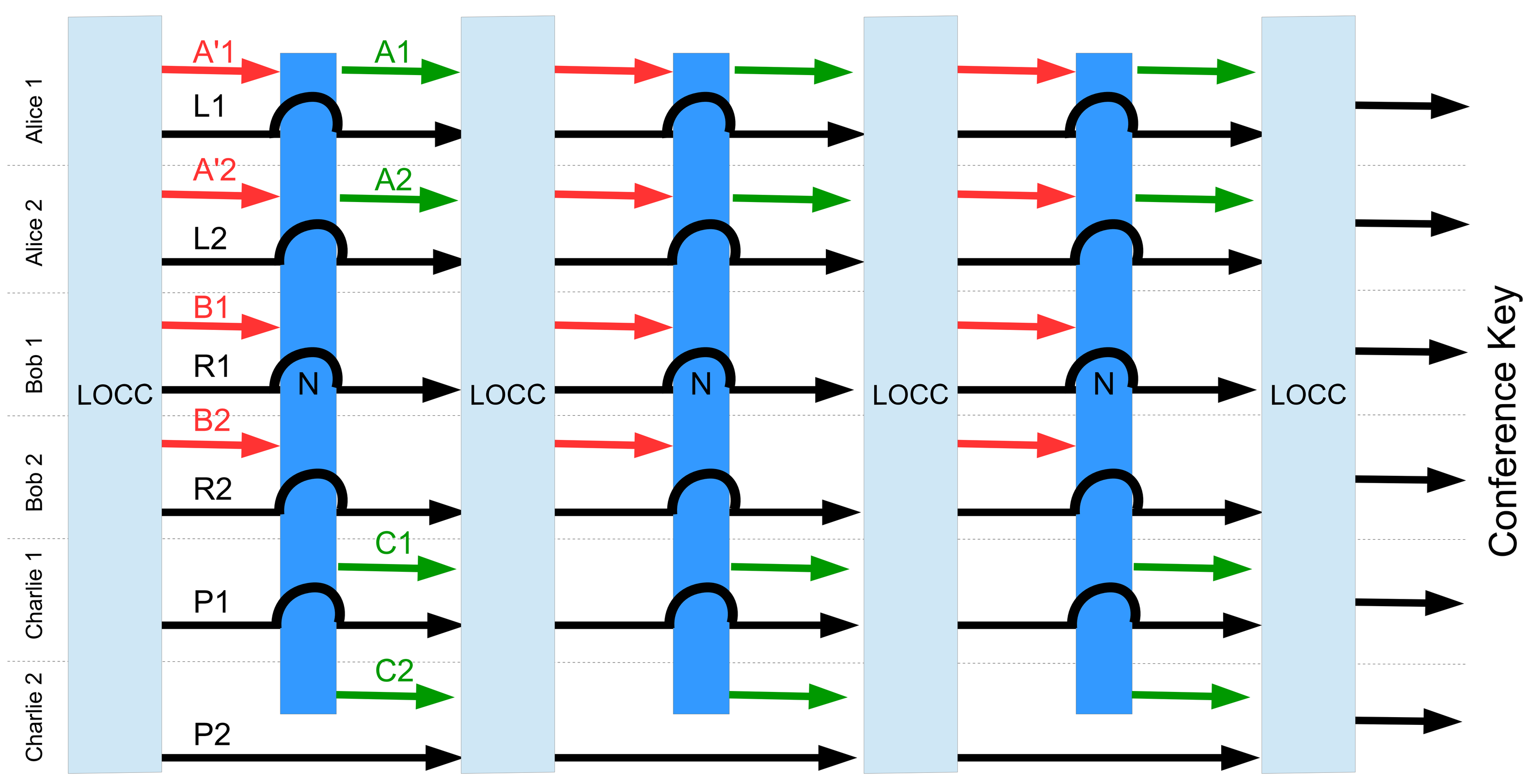
Quantum Multiplex Channels

- Consider multipartite quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$
- Including point-to-point channels, broadcast channels, multiple access channels, interference channels, bipartite interactions.



Adaptive LOCC protocol

- Goal: Conference key among all parties.
- N uses of quantum multiplex channel, interleaved by free LOCC among all parties.



Multipartite Entanglement

- Assume n parties. Let $2 \leq k \leq n$.
- k-separability:

$$\sigma_{k-sep} = \sum_i p_i \left|\psi^i_{A_1}\right\rangle\left\langle\psi^i_{A_1}\right| \otimes \left|\psi^i_{A_2}\right\rangle\left\langle\psi^i_{A_2}\right| \otimes \ldots \otimes \left|\psi^i_{A_k}\right\rangle\left\langle\psi^i_{A_k}\right|.$$

  If $k < n$, subsystems with respect to which the elements of the decomposition have to be product can differ!

- Set of k-separable states is convex for all k. Can use divergence based measures. $k = 2$: 'biseparable', $k = n$: 'fully separable'.
- Genuinely multipartite entangled (GME): Not biseparable.
- Biseparable states can be distilled to GME. Definition not tensor stable.

Quantum Conference Key Generation

- First option: Distill GHZ states

$$\left|\Phi^{\mathrm{GHZ,d}}\right\rangle_{A_1,\ldots,A_n} = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1} |i,\ldots,i\rangle_{A_1,\ldots,A_n}$$

- Second option: Distill n-partite private states [Augusiak, R., Horodecki, P. (2009). PRA, 80(4), 042307.]:

$$\gamma^d_{A_1,A_1',\ldots,A_n,A_n'} = \frac{1}{d}\sum_{ij} |i,\ldots,i\rangle\langle j,\ldots,j|_{A_1,\ldots,A_n} \otimes U^{(i)}\sigma_{A_1',\ldots,A_n'}U^{(j)\dagger}$$

Privacy from single-use multiplex channe[ls]

Theorem 1 *For any fixed $\varepsilon \in (0,1)$, the achievable region of cppp-assisted conference key agreement over a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ satisfies*

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(1,\varepsilon) \leq E^{\varepsilon}_{h,GE}(\mathcal{N}), \tag{1}$$

where

$$E^{\varepsilon}_{h,GE}(\mathcal{N}) = \sup_{\psi\in FS(:\vec{LA'}:\vec{RB}:)} \inf_{\sigma\in BS(:\vec{LA}:\vec{R}:\vec{C}:)} D^{\varepsilon}_h(\mathcal{N}(\psi)\|\sigma) \tag{2}$$

is the ε-hypothesis testing relative entropy of genuine entanglement of the multiplex channel $\mathcal{N}$. It suffices to optimize over pure input states $\psi \in FS(:\vec{LA'}:\vec{RB}:)$.

Strong converse bounds on LOCC-assiste[d]

Theorem 2 *For a fixed n, $K \in \mathbb{N}$, $\varepsilon \in (0,1)$, the following bound holds for an (n,K,ε) protocol for LOCC-assisted conference key agreement over a multiplex $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$:*

$$\frac{1}{n}\log_2 K \leq E_{\max,E}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right), \tag{3}$$

where the max-relative entropy of entanglement $E_{\max,E}(\mathcal{N})$ of the multiplex channel $\mathcal{N}$ is

$$E_{\max,E}(\mathcal{N}) = \sup_{\psi\in FS(:\vec{LA'}:\vec{RB}:)} \inf_{\sigma\in FS(:\vec{LA}:\vec{R}:\vec{C}:)} D_{\max}(\mathcal{N}(\psi)\|\sigma)$$

and it suffices to optimize over pure states ψ.

Corollary 3 *The strong converse LOCC-assisted conference-key-agreement capacity of a multiplex channel $\mathcal{N}$ is bounded from above by its max-relative entropy of entanglement:*

$$\widetilde{P}_{LOCC}(\mathcal{N}) \leq E_{\max,E}(\mathcal{N}). \tag{4}$$

Theorem 4 *For finite Hilbert space dimensions the asymptotic LOCC assisted private capacity of a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is bounded by its regularised relative entropy of entanglement:*

$$\widetilde{\mathcal{P}}_{LOCC}(\mathcal{N}) \leq E^{\infty}_{E}(\mathcal{N}). \tag{5}$$

Applications

- **Measurement-Device-Independent QKD:** Alice and Bob locally prepare states which they send to a relay station using channels $\mathcal{N}^1_{A'\to A}$ and $\mathcal{N}^2_{B'\to B}$. At the relay station, a joint measurement of the systems AB is performed. Define multiplex channel $\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B} := \mathcal{B}_{X\to Z_A Z_B}\circ\mathcal{M}_{AB\to X}\circ\mathcal{N}^1_{A'\to A}\otimes\mathcal{N}^2_{B'\to B}$
- Other applications: **Measurement-Device-Independent Conference Key Agreement**, **Quantum Key Repeater**, **Quantum Networks.**