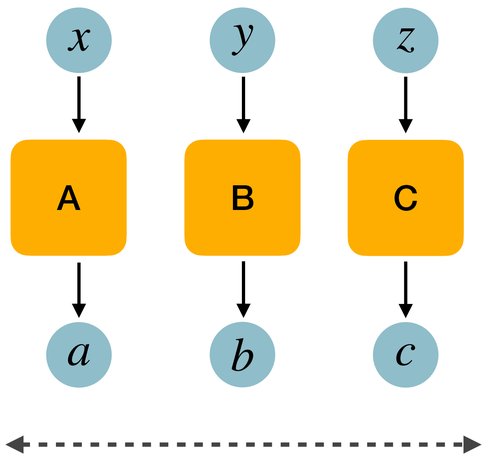
Quantitative quantum soundness for all multipartite compiled nonlocal games

Matilde Baroni[1], Igor Klep[2], Dominik Leichtle[3], Marc-Olivier Renou[4], Ivan Šupić[5], Lucas Tendick[4], **Xiangling Xu (许湘灵)[4]**

xu.xiangling@inria.fr

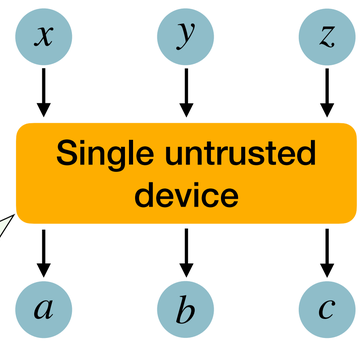
[1]Sorbonne Université, CNRS, LIP6, France
[2]University of Ljubljana, University of Primorska, and Institute of Mathematics, Physics and Mechanics, Slovenia
[3]School of Informatics, University of Edinburgh, United Kingdom
[4]Inria, CPHT, LIX, CNRS, École polytechnique, Institut Polytechnique de Paris, France
[5]Université Grenoble Alpes, CNRS, Grenoble INP, LIG, France

1 Bell nonlocal games and space-like



- A central tool for testing quantum nonlocality
- Foundations of device-independent (DI) quantum information
- Players cannot communicate with each other during the game
- For this, standard experimental implementations require space-like separated devices

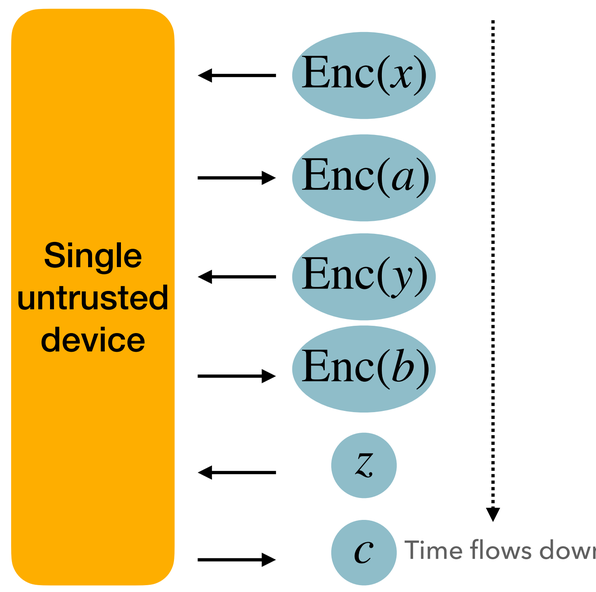
- *For many parties over large-distance, this is experimentally difficult!*
- *Can we perform nonlocal experiments on a single untrusted device?*



- Naive one device does not work: e.g., can learn x, y, a, b to cheat for (z, c)

2 Cryptography replaces space-like separation -- the KLVY compiler

- Any multipartite game is transformed into a **sequential game** on a single device
- Use cryptography to hide x, y, a, b from the device so it cannot cheat
- Encryption scheme: quantum homomorphic encryption (QHE)
- **Compiled nonlocal game**



Yes on a single device, but can we trust the results of compiled nonlocal game?

That is, do they faithfully represent the corresponding nonlocal games?

3 Quest for faithfulness of compiled games

Faithfulness needs two properties

- *Classical/quantum completeness*: honest classical/quantum strategies for the original game remain achievable after compilation
- *Classical/quantum soundness*: an efficient cheating device cannot substantially exceed the relevant nonlocal classical/quantum benchmarks

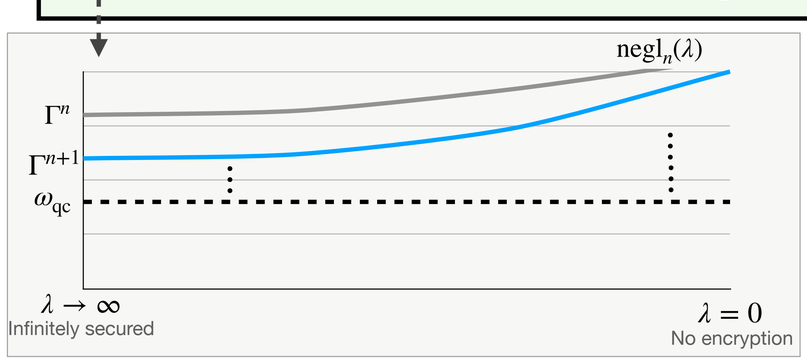
- Classical completeness & soundness, and classical soundness are proven
- Quantum soundness is only fully resolved for bipartite case; in multipartite case it is only sound assuming infinite cryptographic security
- But we don't have infinitely cryptographic security: need a **quantitative characterization of multipartite quantum soundness**
- Important for e.g., *compiled quantum key distributions* and *compiled random number generation*

4 Our result

Main result:

For all multipartite compiled games, at any cryptographic security level, we can systematically upper-bound their quantum score; establishing quantum soundness for a large class of games

- For every nonlocal game, the maximum winning probability with all (commuting) quantum strategies is the quantum score ω_{qc}
- We have a computable game-dependent monotone sequence $\omega^1 \geq \omega^2 \geq \cdots \geq \omega_{\mathrm{qc}}$, such that $\omega^n \searrow \omega_{\mathrm{qc}}$
- The security parameter $\lambda \in \mathbb{N}$: both the untrusted device and the encryption are due to quantum circuits of $\mathrm{poly}(\lambda)$-many gates
- **For every n, there exists a negligible function $\mathrm{negl}_n(\lambda)$ such that the compiled score $\leq \omega^n + \mathrm{negl}_n(\lambda)$**
- **For games (e.g., XOR) whose ω^n converge at finite n, they are quantum sound for a single negligible function: compiled score $\leq \omega_{\mathrm{qc}} + \mathrm{negl}(\lambda)$**



5 Technique for quantum soundness: sequential NPA hierarchy for quantum instruments

A novel generalized Navascués-Pironio-Acín (NPA) hierarchy for characterizing sequential applications of *quantum instruments*

- The sequence convergent $\{\omega^n\}$ are due to this hierarchy, computable due to semidefinite programs (SDPs)
- Very flexible framework to characterize *completely positive maps*, may be of independent interests

Back to compiled games

- Compiled strategies can be described by sequential instruments computationally non-signaling due to cryptographic constraints
- We prove they are negligibly close to feasible solutions of our sequential hierarchy of non-signaling quantum instruments at every n

- **Take-home message:** Cryptography can replace space-like separation, and the resulting multipartite compiled games now have quantitative finite-security guarantees
- **Open**: Self-testing for compiled games; applications of sequential NPA hierarchies; weaker computational assumptions

arXiv:2509.25145