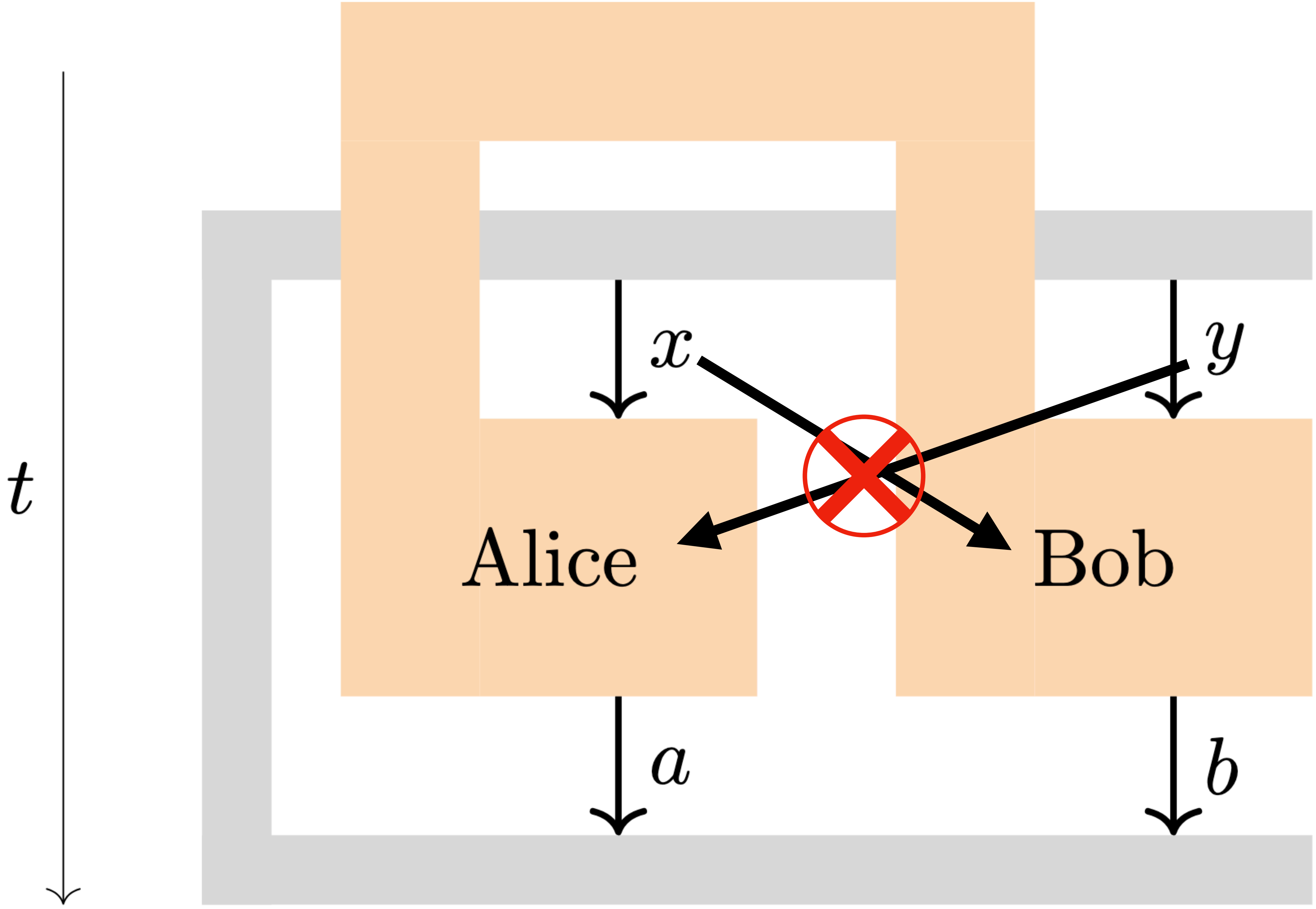
A Generalized NPA Moment-SOS Hierarchy and Its Application to Quantum Information Theory

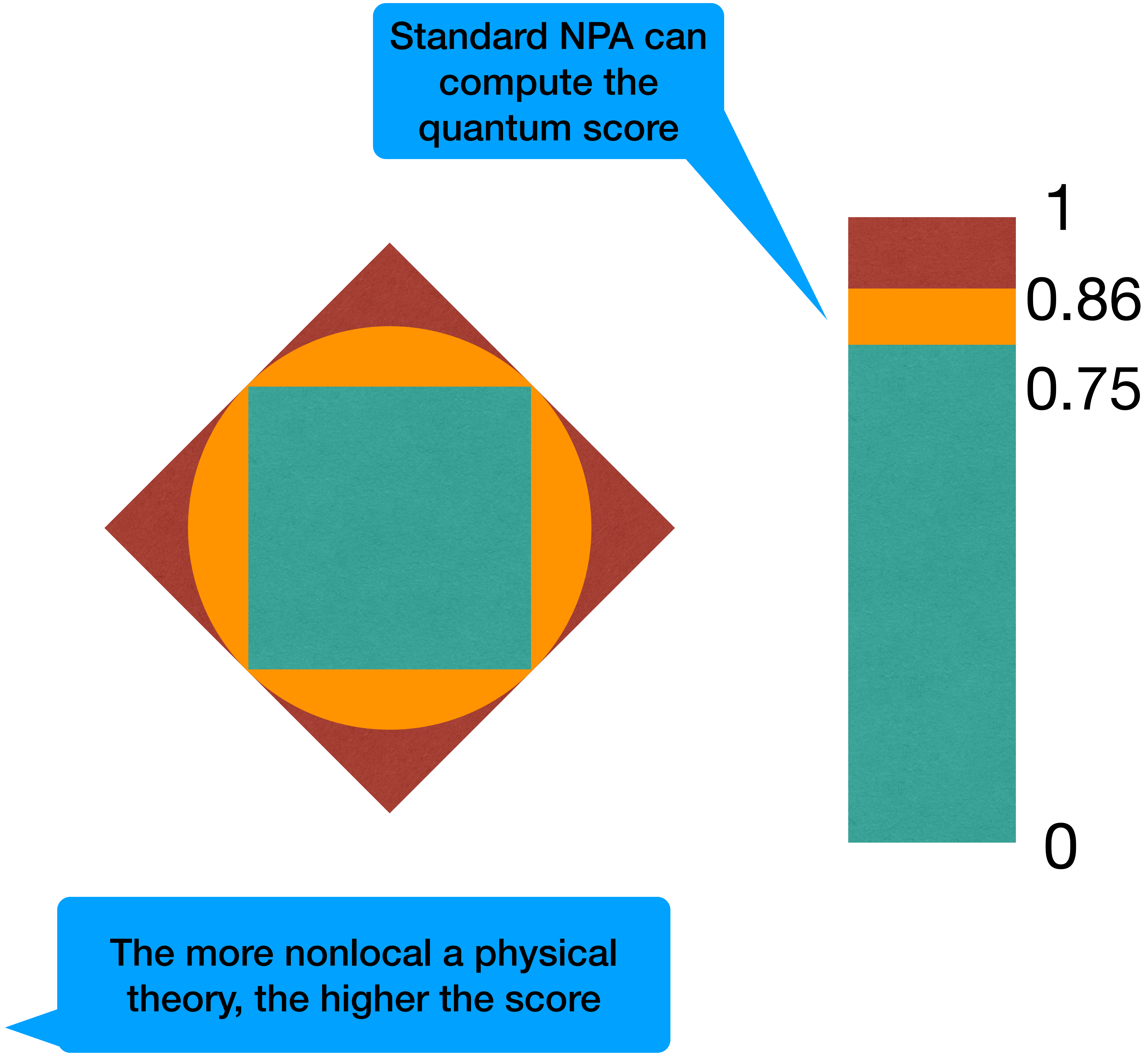
Xiangling Xu 许湘灵, Team PhIQuS, Inria Saclay

Based on arXiv:2507.17006 & arXiv:2509.25145
with Matilde Baroni, Igor Klep, Dominik Leichtle, Connor Paddock, Marc-Olivier Renou, Simon Schmidt, Ivan Šupić, Lucas Tendick, and Yuming Zhao

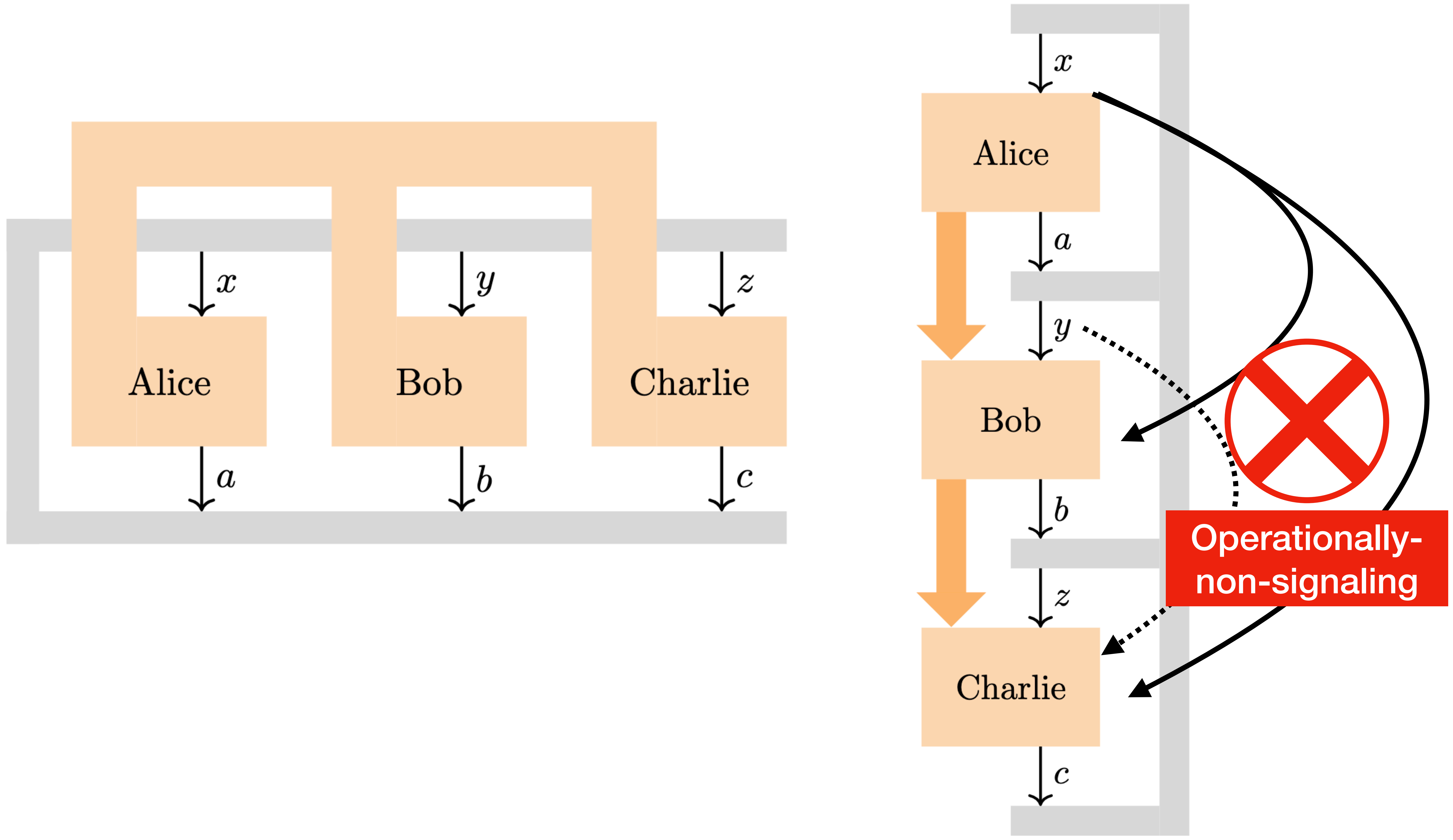
Device-independent non-locality 101



CHSH: $a \oplus b = x \cdot y$

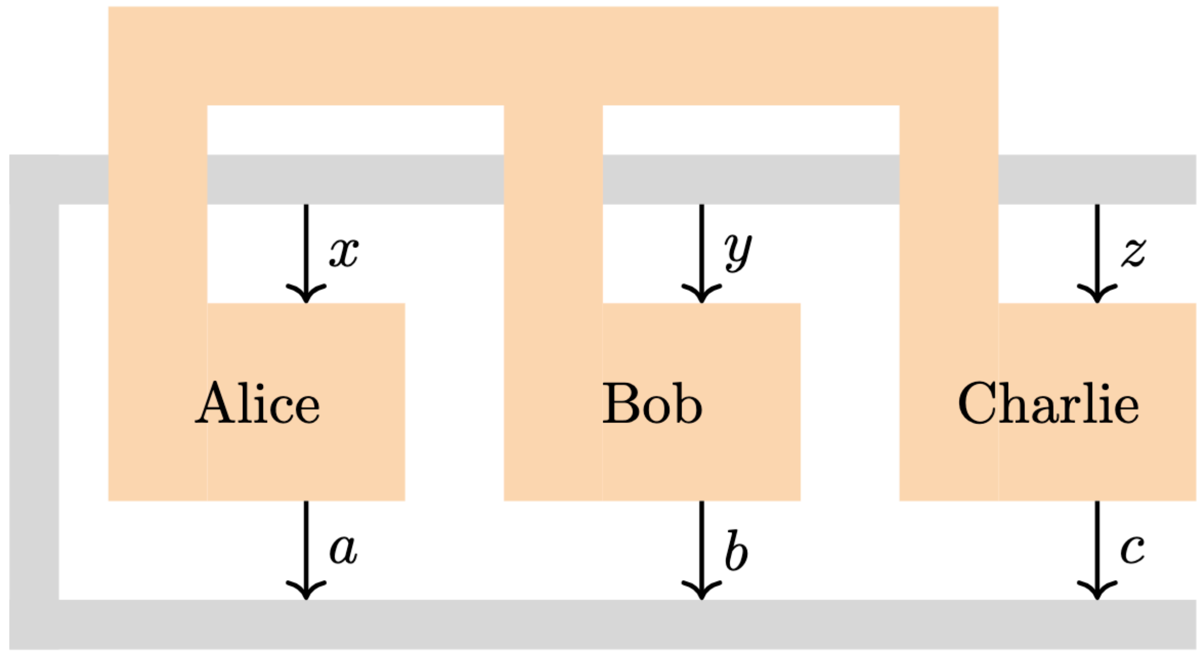


QIT allows for the sequential scenarios



- Standard NPA only applies to the left
- Goal of the talk: a NPA Moment-SOS hierarchy for the sequential scenario
- Application: open questions in quantum cryptography and QIT

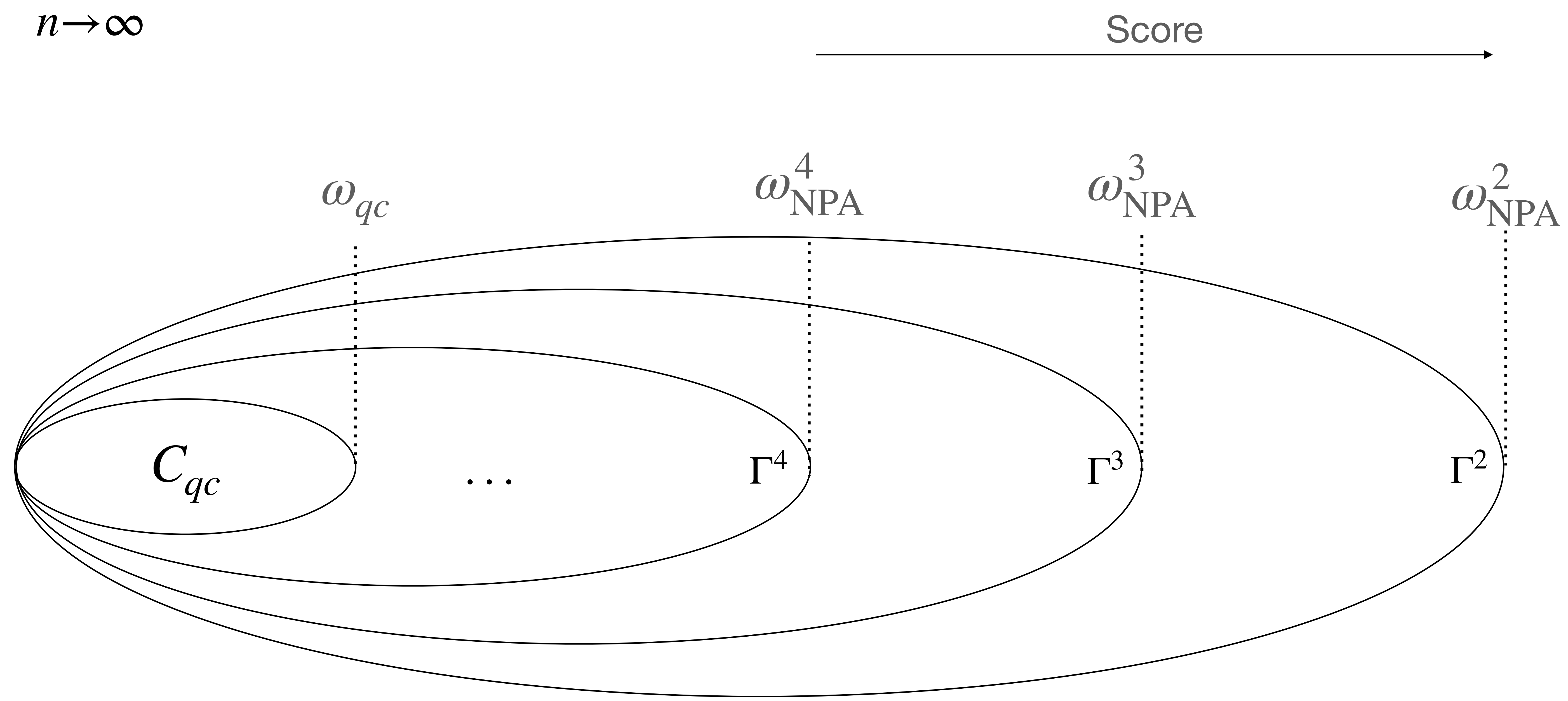
Commuting quantum strategies C_{qc}



- State σ and PVMs $\{A_{a|x}\}, \{B_{b|y}\}, \{C_{c|z}\}$
- Strategy: $p(abc\,|\,xyz) = \mathrm{Tr}(\sigma \cdot A_{a|x}B_{b|y}C_{c|z}) \in C_{qc}$
- ω_{qc} = Commuting quantum score = max winning probability with C_{qc}
- Lower bound of ω_{qc}: just try all quantum strategies!
- Upper bound: outer approximation of C_{qc} with NPA hierarchy [NPA08]

A hierarchy of pseudo-quantum strategies

- Will sketch, have sets of pseudo-quantum strategies $\Gamma^n, n \geq 2$, such that $p \in C_{qc} = \lim_{n\to\infty} \Gamma^n \subset \cdots \subset \Gamma^4 \subset \Gamma^3 \subset \Gamma^2$



- Characterizing C_{qc} from the outside

- Computable sequence of upper bounds $\omega^2_{\mathrm{NPA}} \geq \omega^3_{\mathrm{NPA}} \geq \omega^4_{\mathrm{NPA}} \geq \cdots \searrow \omega_{qc}$

NPA hierarchy: moment matrix Γ^2

- Suppose we do state/PVMs s.t. have $p(abc \mid xyz) = \mathrm{Tr}(\sigma A_{a|x} B_{b|y} C_{c|z})$, easy to calculate expectation values: $\mathrm{Tr}(\sigma A_{a|x}), \mathrm{Tr}(\sigma A^*_{a|x} C_{c|z}), \ldots$

- Put them into a moment matrix Γ^2, indexed by $1, A_{a|x}, A_{a|x} A_{a'|x'}, \ldots$ (up to length 2).

$$
\begin{array}{cc}
 & \begin{array}{ccccc} \mathbb{1} & A_{a|x} & B_{b|y} & C_{c|z} & \cdots \end{array} \\
\begin{array}{c} \mathbb{1} \\ (A_{a|x})^\dagger \\ (B_{b|y})^\dagger \\ (C_{c|z})^\dagger \\ \cdots \end{array} &
\begin{bmatrix}
1 & \mathrm{Tr}\left(\sigma A_{a|x}\right) & \mathrm{Tr}\left(\sigma B_{b|y}\right) & \mathrm{Tr}\left(\sigma C_{c|z}\right) & \\
 & \mathrm{Tr}\left(\sigma A_{a|x}\right) & \mathrm{Tr}\left(\sigma A_{a|x} B_{b|y}\right) & \mathrm{Tr}\left(\sigma A_{a|x} C_{c|z}\right) & \\
 & & \mathrm{Tr}\left(\sigma B_{b|y}\right) & \mathrm{Tr}\left(\sigma B_{b|y} C_{c|z}\right) & \\
 & & & \mathrm{Tr}\left(\sigma C_{c|z}\right) & \\
 & & & &
\end{bmatrix}
\end{array}
$$

- Rule: $\Gamma_{B_{b|y}, B_{b|y}} = \mathrm{Tr}(\sigma B^*_{b|y} B_{b|y}) = \mathrm{Tr}(\sigma B_{b|y}) = \mathrm{Tr}(\sigma \mathrm{Id}^* \cdot B_{b|y}) = \Gamma_{1, B_{b|y}}$

NPA hierarchy: moment matrix Γ^2

- Zoom out to length 2

$$\Gamma_{A_{a|x}B_{b|y},C_{c|z}} = \mathrm{Tr}(\sigma(A_{a|x}B_{b|y})^{*}C_{c|z}) = \mathrm{Tr}(\sigma A_{a|x}B_{b|y}C_{c|z}) = p(abc\,|\,xyz)$$

$$\begin{array}{cc}
 & \begin{array}{cccccc} \mathbb{1} & A_{a|x} & B_{b|y} & C_{c|z} & A_{a|x}A_{a'|x'} & \cdots \end{array} \\
\begin{array}{c} \mathbb{1} \\ (A_{a|x})^{\dagger} \\ (B_{b|y})^{\dagger} \\ (C_{c|z})^{\dagger} \\ (A_{a|x}A_{a'|x'})^{\dagger} \\ (A_{a|x}B_{b|y})^{\dagger} \\ \cdots \end{array} &
\begin{bmatrix}
1 & & & & & \\
 & & & & & \\
 & & \mathrm{Tr}(\sigma B_{b|y}) & & & \\
 & & & & & \\
 & & & \mathrm{Tr}(\sigma A_{a'|x'}A_{a|x}C_{c|z}) & & \\
 & & & p(abc|xyz) & & \\
 & & & & &
\end{bmatrix}
\end{array}$$

- Γ^2 is positive semidefinite, symmetric, satisfies many linear constraints…

- $p \in \Gamma^2$ pseudo-quantum strategy if such a matrix exists

NPA hierarchy: moment matrix Γ^3 and more

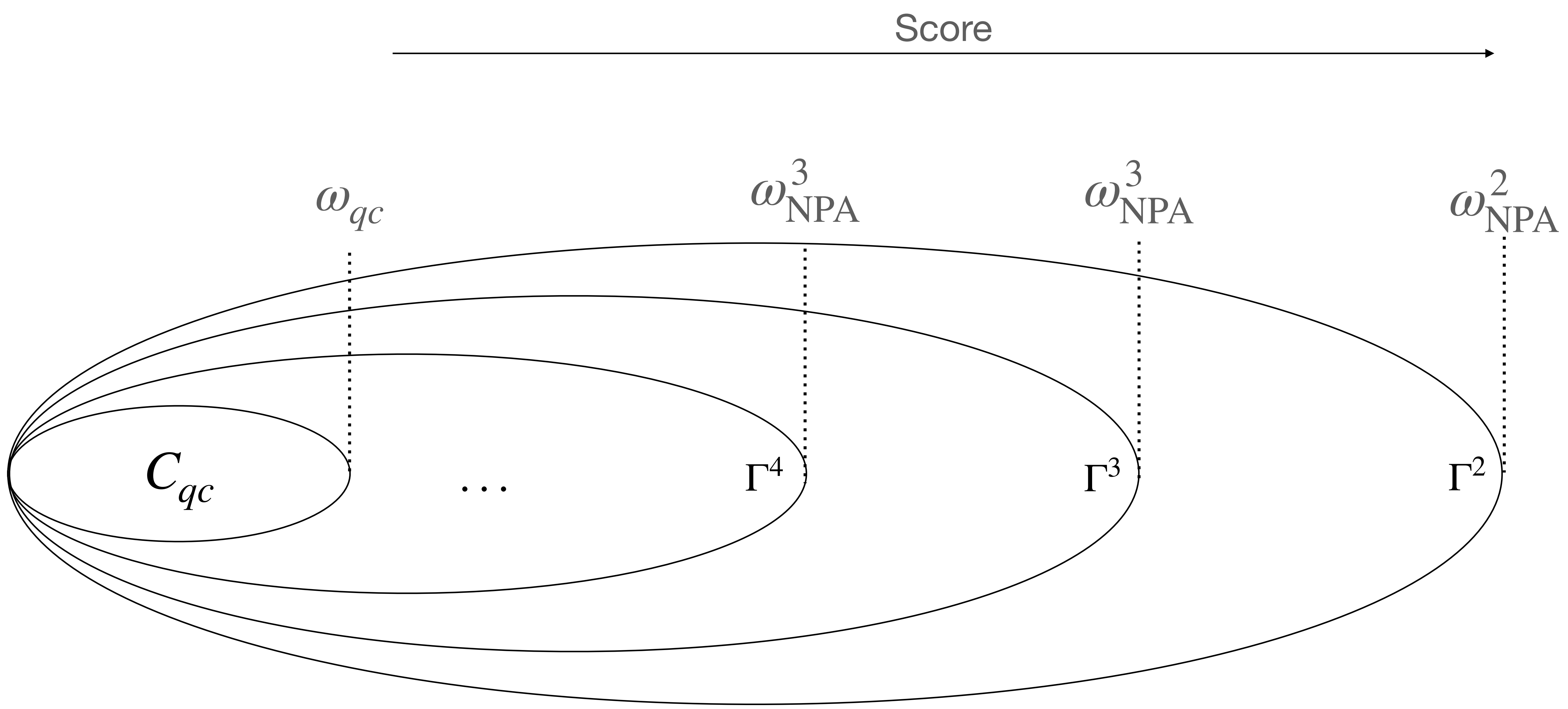
- Longer indices, such as $A_{a|x}B_{b|y}C_{c|z}$, of length 3, to get a bigger matrix Γ^3

$$\begin{array}{c|c} & \begin{array}{ccccc} \mathbb{1} & A_{a|x} & B_{b|y} & C_{c|z} & \cdots \end{array} \\ \begin{array}{c} \mathbb{1} \\ (A_{a|x})^\dagger \\ (B_{b|y})^\dagger \\ (C_{c|z})^\dagger \\ (A_{a|x}A_{a'|x'})^\dagger \\ (A_{a|x}B_{b|y})^\dagger \\ \cdots \\ (A_{a|x}B_{b|y}C_{c|z})^\dagger \\ \cdots \end{array} & \begin{bmatrix} 1 & & & & \\ & & & & \\ & & \mathrm{Tr}\left(\sigma B_{b|y}\right) & & \\ & & & & \\ & & & \mathrm{Tr}\left(\sigma A_{a'|x'} A_{a|x} C_{c|z}\right) & \\ & & & p(abc|xyz) & \\ & & & & \\ & \mathrm{Tr}\left(\sigma A_{a|x} B_{b|y} C_{c|z}\right) & & & \\ & & & & \end{bmatrix} \end{array}$$

- Containing Γ^2 as a submatrix, i.e., Γ^3-pseudo strategy is also in Γ^2

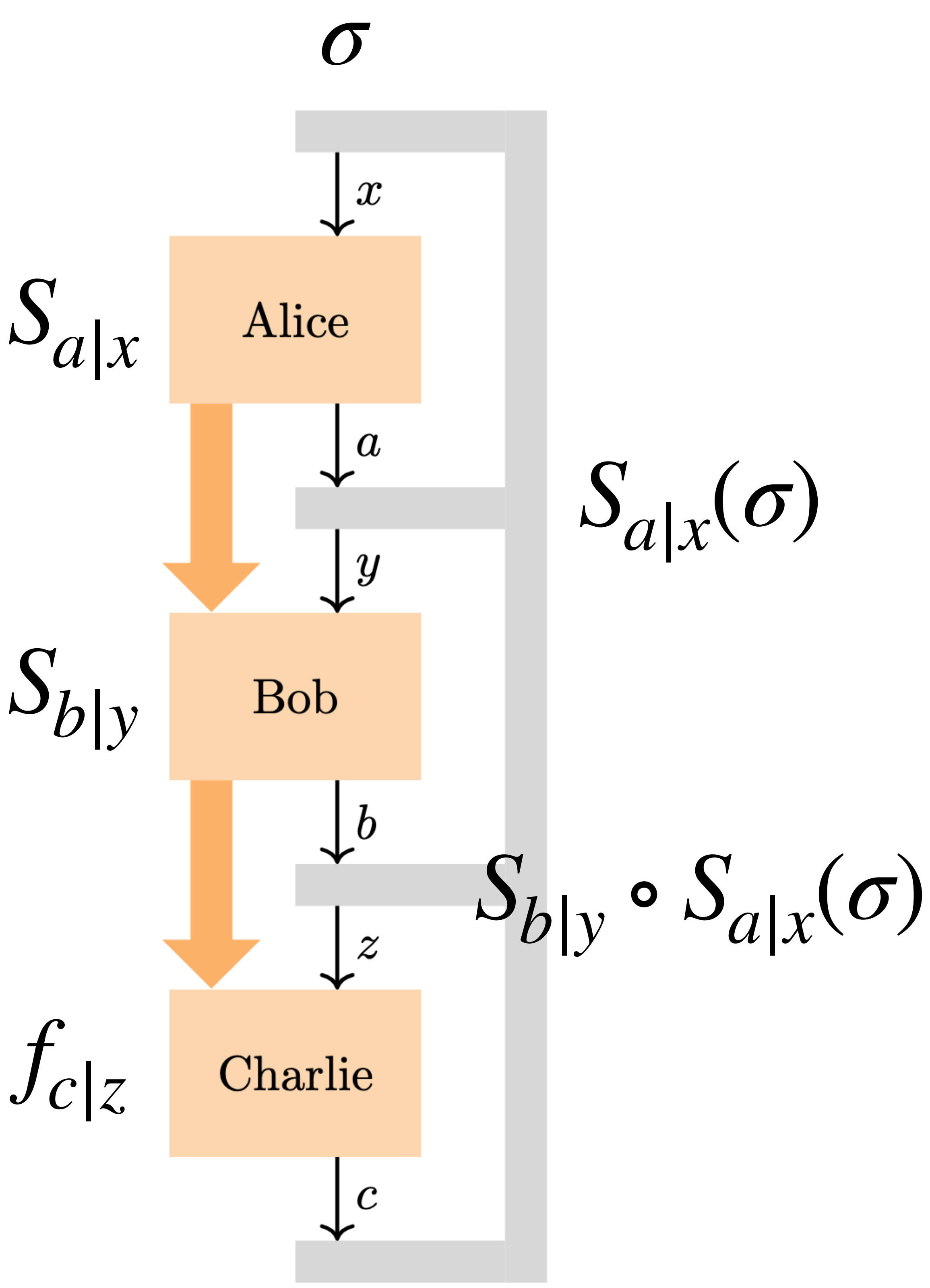
- Repeat to get $\Gamma^2, \Gamma^3, \Gamma^4 \ldots$ A hierarchy of moment matrices for pseudo-quantum strategies

A hierarchy of pseudo-quantum strategies



- Finding Γ^n and optimization can be done with semidefinite programs (SDPs)
- Computable sequence of upper bounds $\omega^2_{\mathrm{NPA}} \geq \omega^3_{\mathrm{NPA}} \geq \omega^4_{\mathrm{NPA}} \geq \cdots \searrow \omega_{qc}$

Sequential quantum scenarios C_{seq}



- $p(abc\,|\,xyz) = \mathrm{Tr}(S_{b|y} \circ S_{a|x}(\sigma) \cdot f_{c|z}) \in C_{\text{seq}}$

Sequential quantum scenarios C_{seq}: the Heisenberg picture

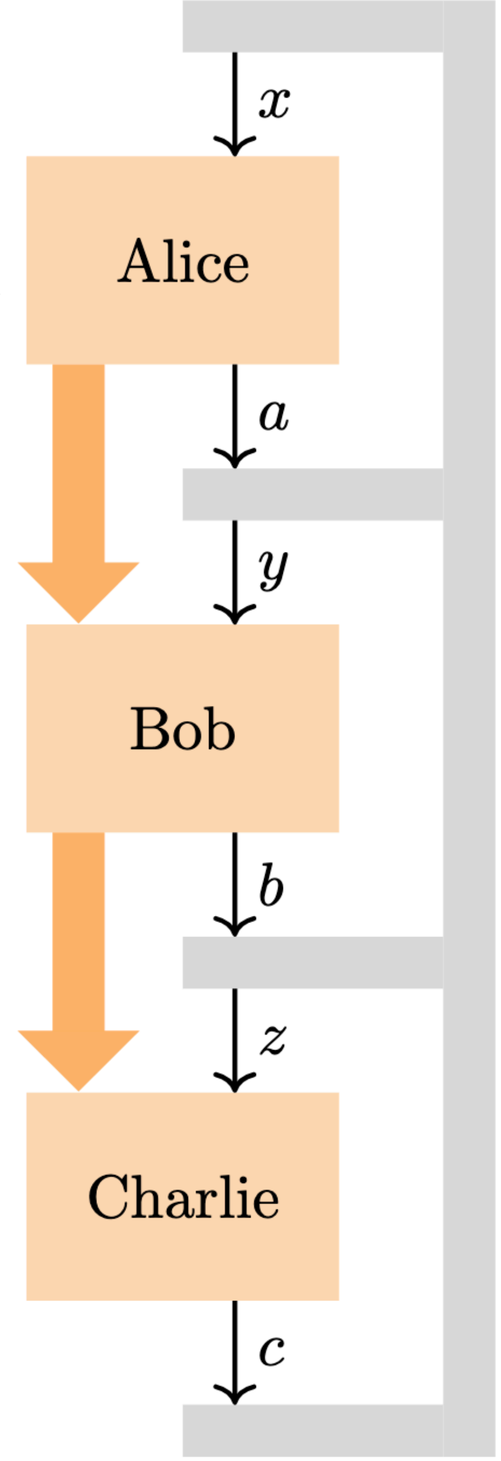
- $p(abc \,|\, xyz) = \mathrm{Tr}(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z})) \in C_{\text{seq}}$
- Operationally-non-signaling: $\sum_a T_{a|x} = \mathrm{id}, \sum_b T_{b|y} = \mathrm{id}$

σ

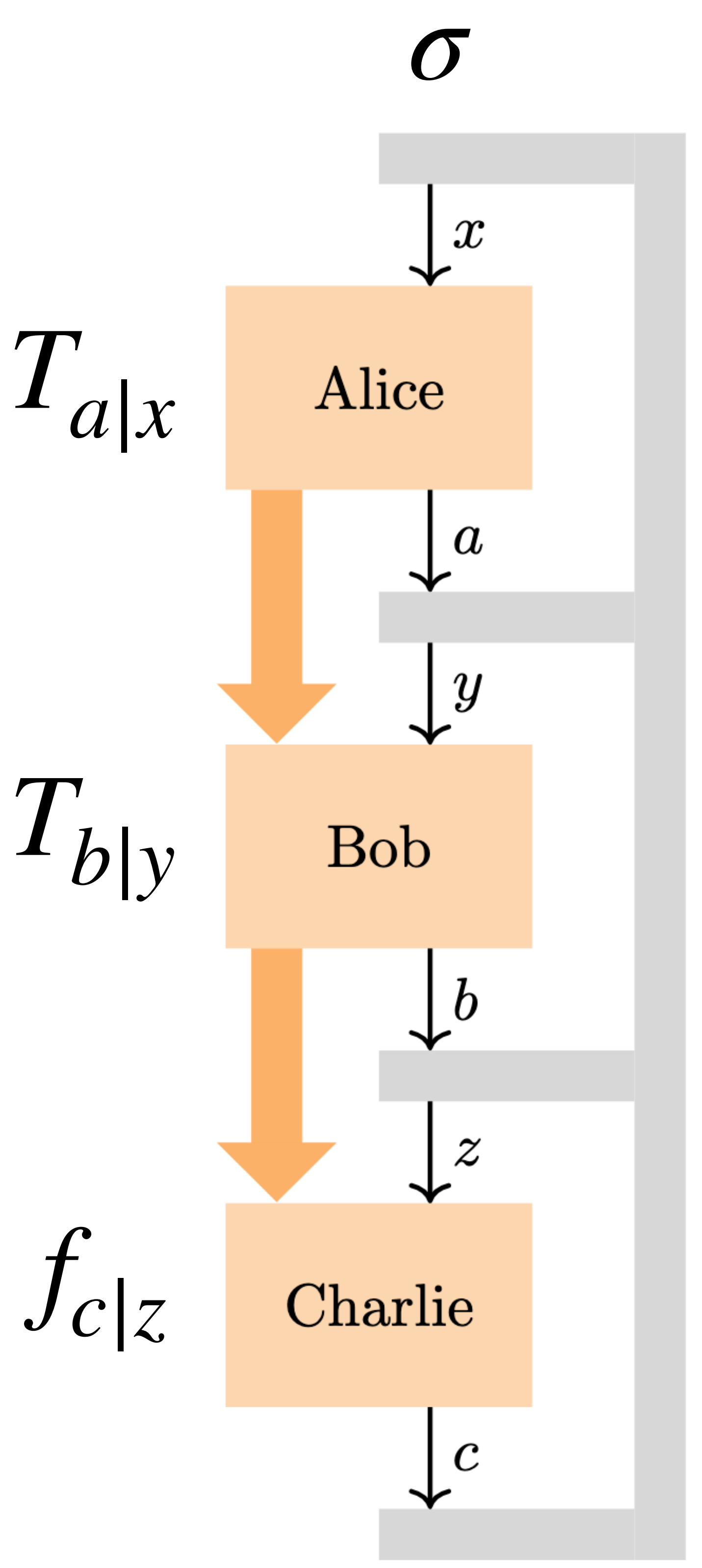
$T_{a|x} = S^*_{a|x}$

$T_{b|y} = S^*_{b|y}$

$f_{c|z}$



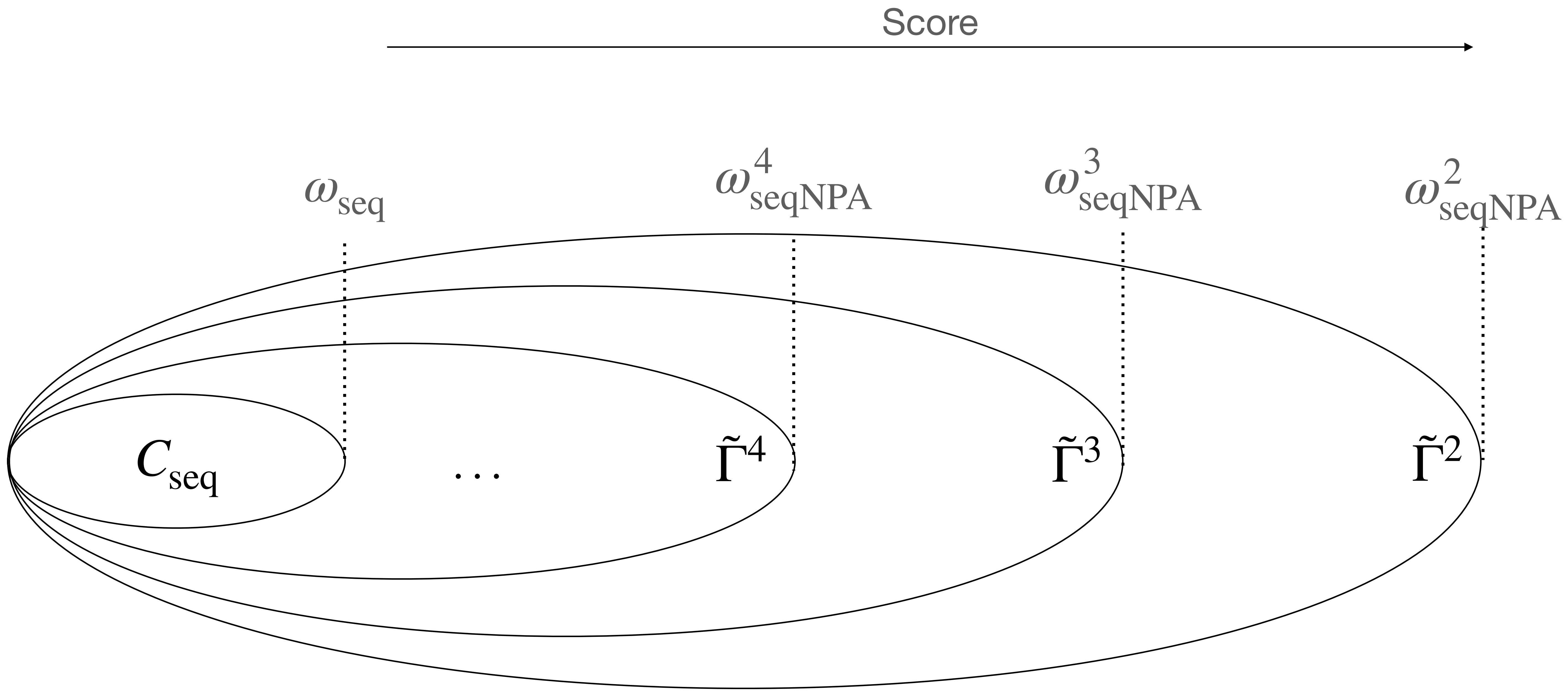
Sequential NPA hierarchy



- Suppose $\exists\, p(abc\,|\,xyz) = \mathrm{Tr}(T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot \sigma)$ s.t. $T_{a|x}, T_{b|y}$ operationally-non-signaling, $f_{c|z}$ PVMs
- Expectations values and arrange them into moment matrices $\tilde{\Gamma}^n$, satisfying many constraints

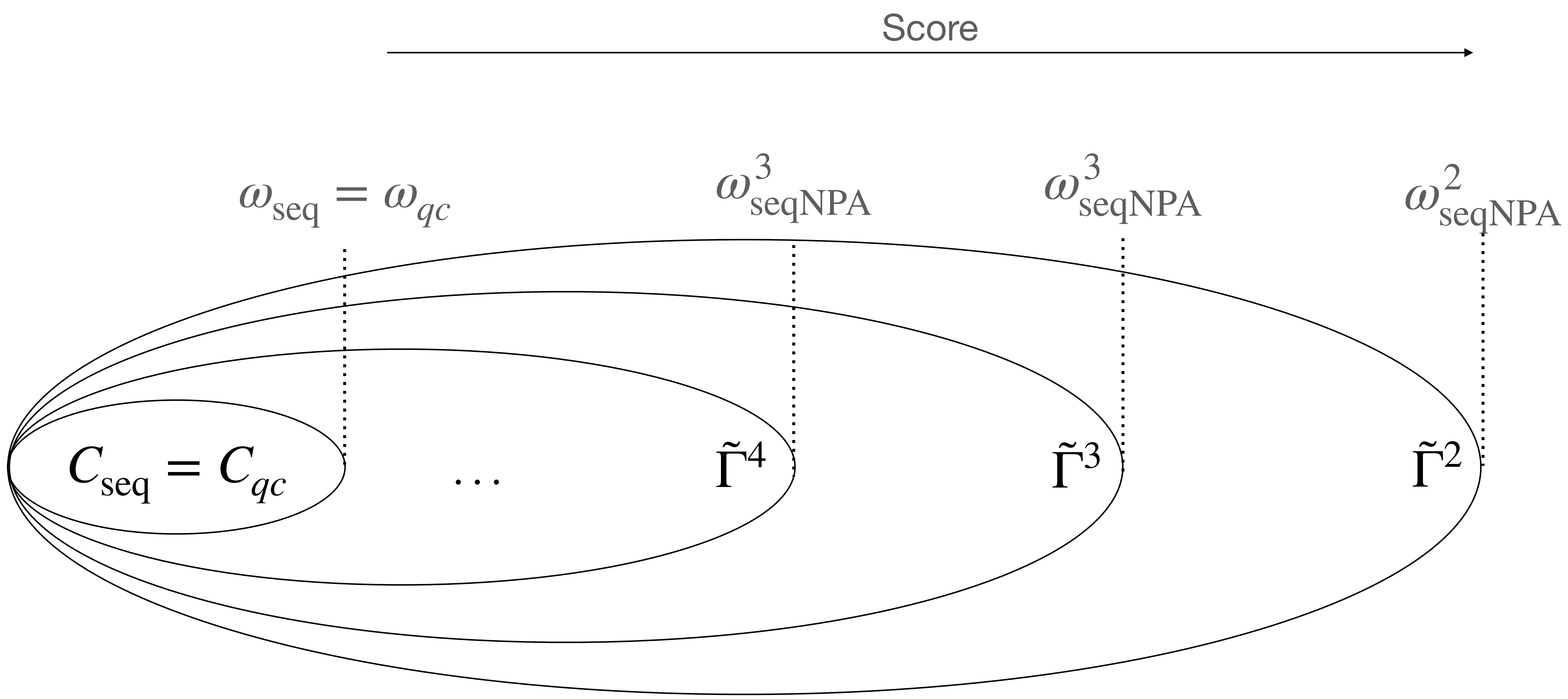
$$
\begin{bmatrix}
1 & p(abc|xyz) & & \mathrm{Tr}\big(\sigma \cdot T_{a|x}\big(T_{b|y}(f_{c|z}) \cdot T_{b'|y'}(f_{c'|z'})\big)\big) & \cdots \\
& & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z} \cdot f_{c'|z'})\big) & & \\
& \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot T_{a'|x'} \circ T_{b'|y'}(f_{c'|z'})\big) & & & \\
& & \vdots & &
\end{bmatrix}
$$

Sequential NPA hierarchy of pseudo sequential quantum strategies



- Finding $\tilde{\Gamma}^n$ and optimization can be done with SDPs
- Computable sequence of upper bounds $\omega^2_{\mathrm{seqNPA}} \geq \omega^3_{\mathrm{seqNPA}} \geq \omega^4_{\mathrm{seqNPA}} \geq \cdots \searrow \omega_{\mathrm{seq}}$

Sequential NPA hierarchy to C_{qc}



- Multipartite S-G-HJW theorem [BLJŠ25]: $C_{\text{seq}} = C_{qc}$ with operationally-non-signaling
- SDP-computable sequence of upper bounds $\omega^2_{\text{seqNPA}} \geq \omega^3_{\text{seqNPA}} \geq \omega^4_{\text{seqNPA}} \geq \cdots \searrow \omega_{qc}$

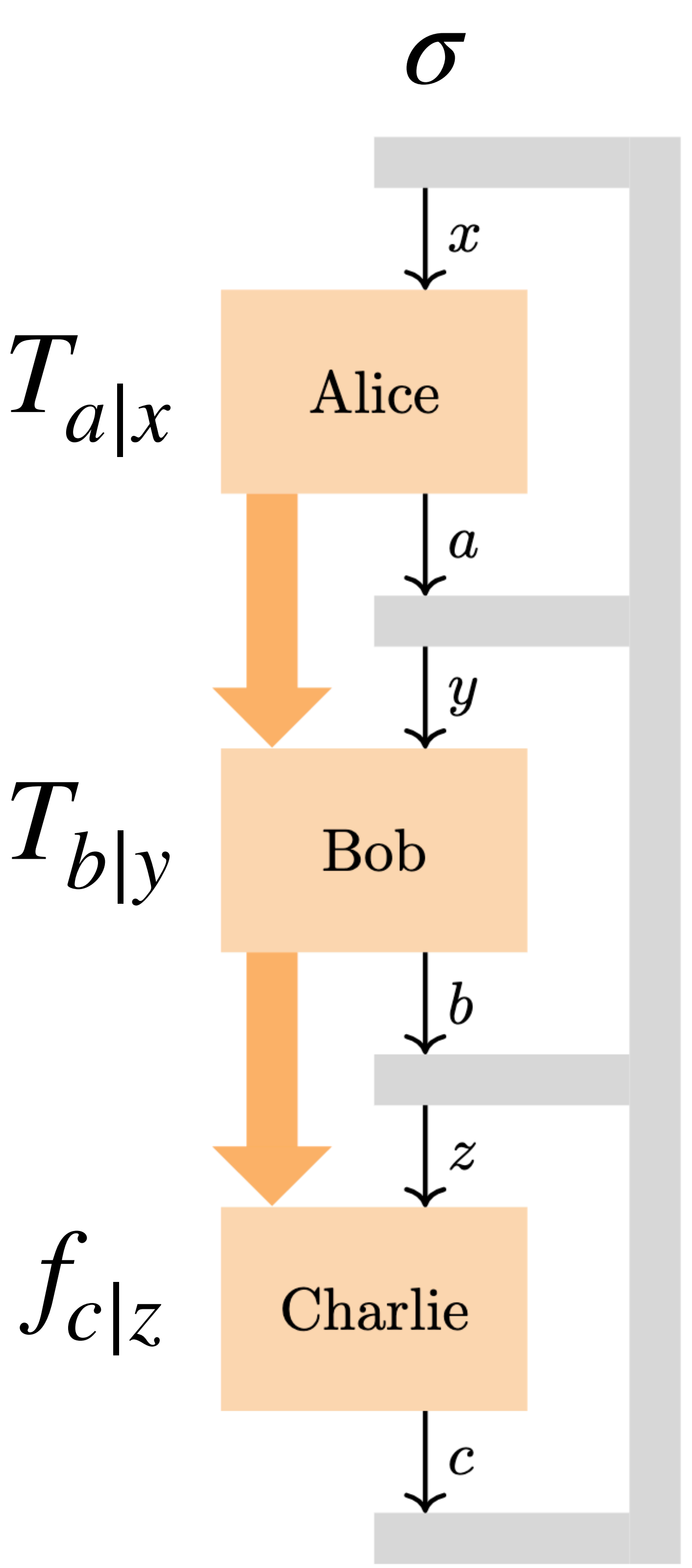
Conclusion

- Generalized NPA moment-SOS hierarchy that can describe sequentiality and quantum instruments/completely positive maps
- When convergent, recover completely positive maps satisfying map-level constraints
- More sparse while the constraints are more complicated
- Flexible, and could be useful to other problems?
- An application: quantitive quantum soundness to compiled games

Sequential NPA hierarchy

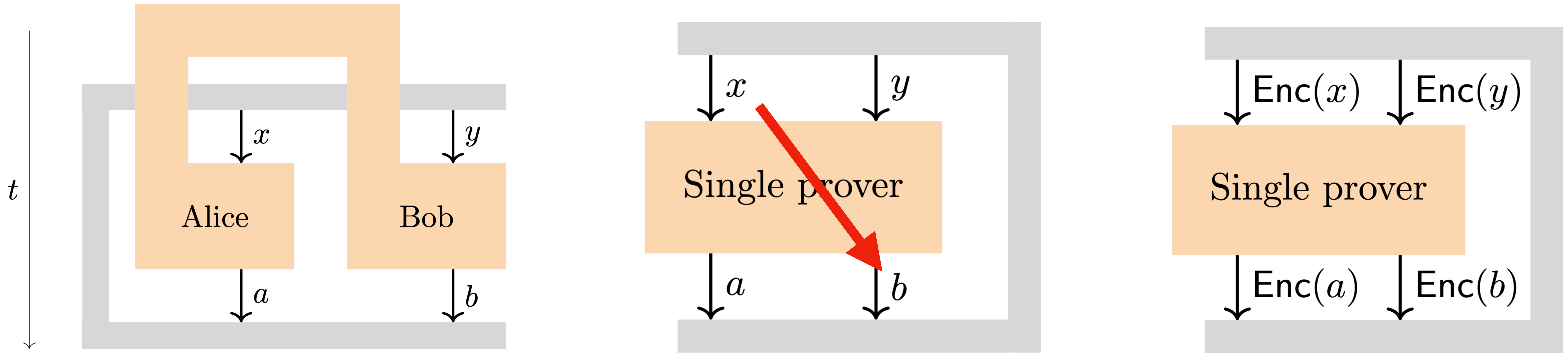
$$\begin{bmatrix} 1 & p(abc|xyz) & & \mathrm{Tr}\big(\sigma \cdot T_{a|x}\big(T_{b|y}(f_{c|z}) \cdot T_{b'|y'}(f_{c'|z'})\big)\big) & \cdots \\ & & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z} \cdot f_{c'|z'})\big) & & \\ & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot T_{a'|x'} \circ T_{b'|y'}(f_{c'|z'})\big) & & & \\ & & \vdots & & \end{bmatrix}$$

$$\begin{aligned} \omega^n_{\mathrm{3seqNPA}}(\mathcal{G}) \;:=\; \max \quad & \sum_{a,b,c,x,y,z} \beta_{abcxyz}\, \Gamma^{(n)}_{\mathbb{1}, f_{abc|xyz}} \\ \text{s.t.} \quad & \Gamma^{(n)} \succeq 0, \quad \Gamma^{(n)}_{\mathbb{1},\mathbb{1}} = 1, \quad \text{(PSD and normalization)} \\ & \Gamma^{(n)}_{w,w'} = \Gamma^{(n)}_{v,v'} \quad \text{whenever } w^* w' = v^* v', \quad \text{(Hankel condition)} \\ & L^{2n}\Big(w^* \sum_a \big(T_{a|x}(r^* s) - T_{a|x'}(r^* s)\big) v\Big) \underset{\substack{\forall x,x',\, \forall w,v \in \mathcal{W}^n_{ABC}, \\ r,s \in \mathcal{W}^n_{BC}, \\ \deg w + \deg v + \deg r + \deg s \leq 2n}}{= 0} \quad \text{(Alice operationally-non-signaling)} \\ & L^{2n}\Big(T_{a|x}\Big(r^* \sum_b \big(T_{b|y}(t^* u) - T_{b|y'}(t^* u)\big) s\Big)\Big) \underset{\substack{\forall\, a,x,y,y', \\ r,s \in \mathcal{W}^n_{BC}, \\ t,u \in \mathcal{W}^n_C, \\ \deg r + \deg s + \deg t + \deg u \leq 2n}}{= 0} \quad \text{(Bob operationally-non-signaling).} \end{aligned}$$



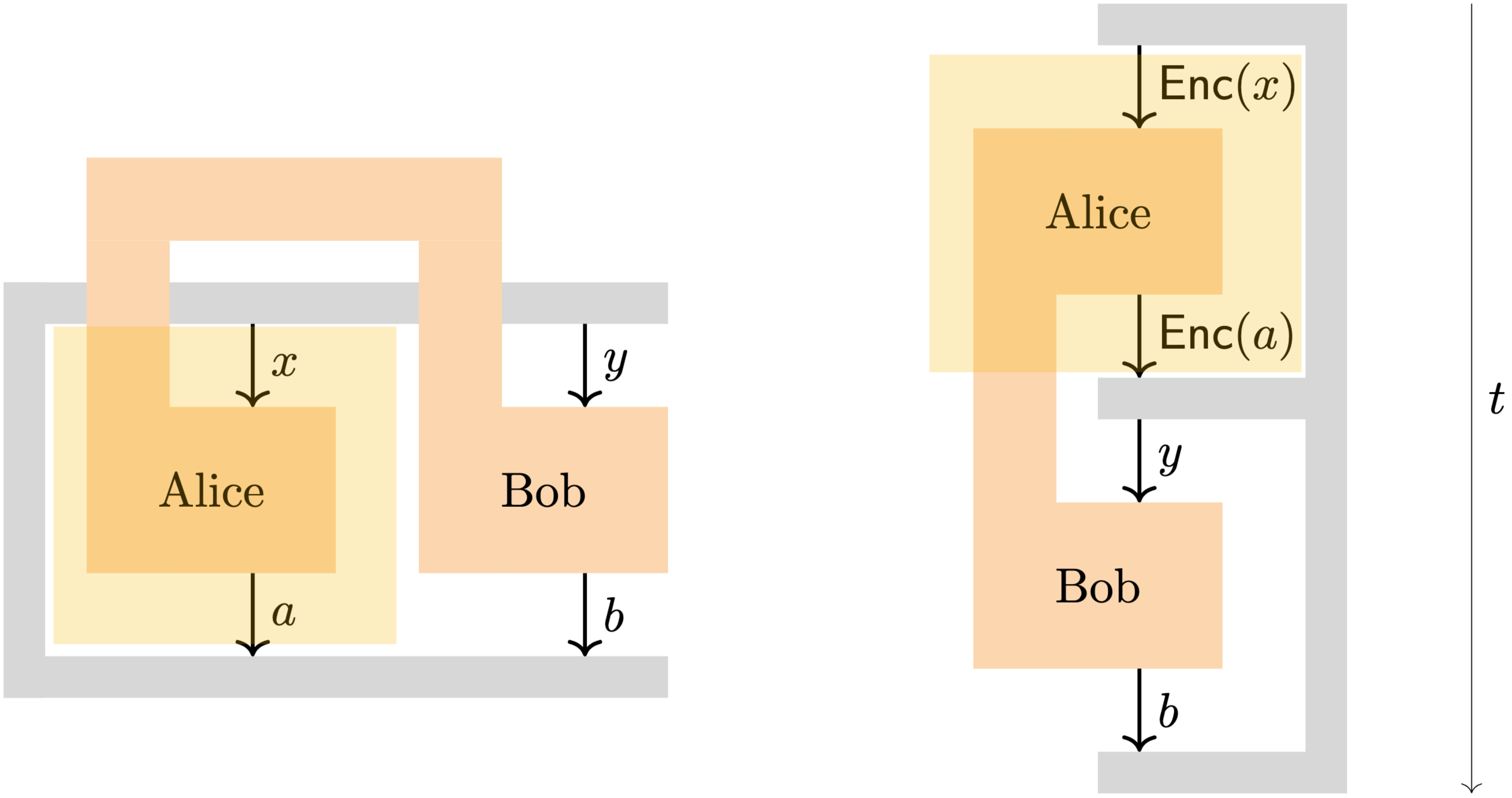
Application to compiled nonlocal games

Removing space-like separation using cryptography



- Goal: performing Bell test on a single untrusted device?
- Idea: Encryption acts as a barrier

KLVY compiler: encryption & sequentiality

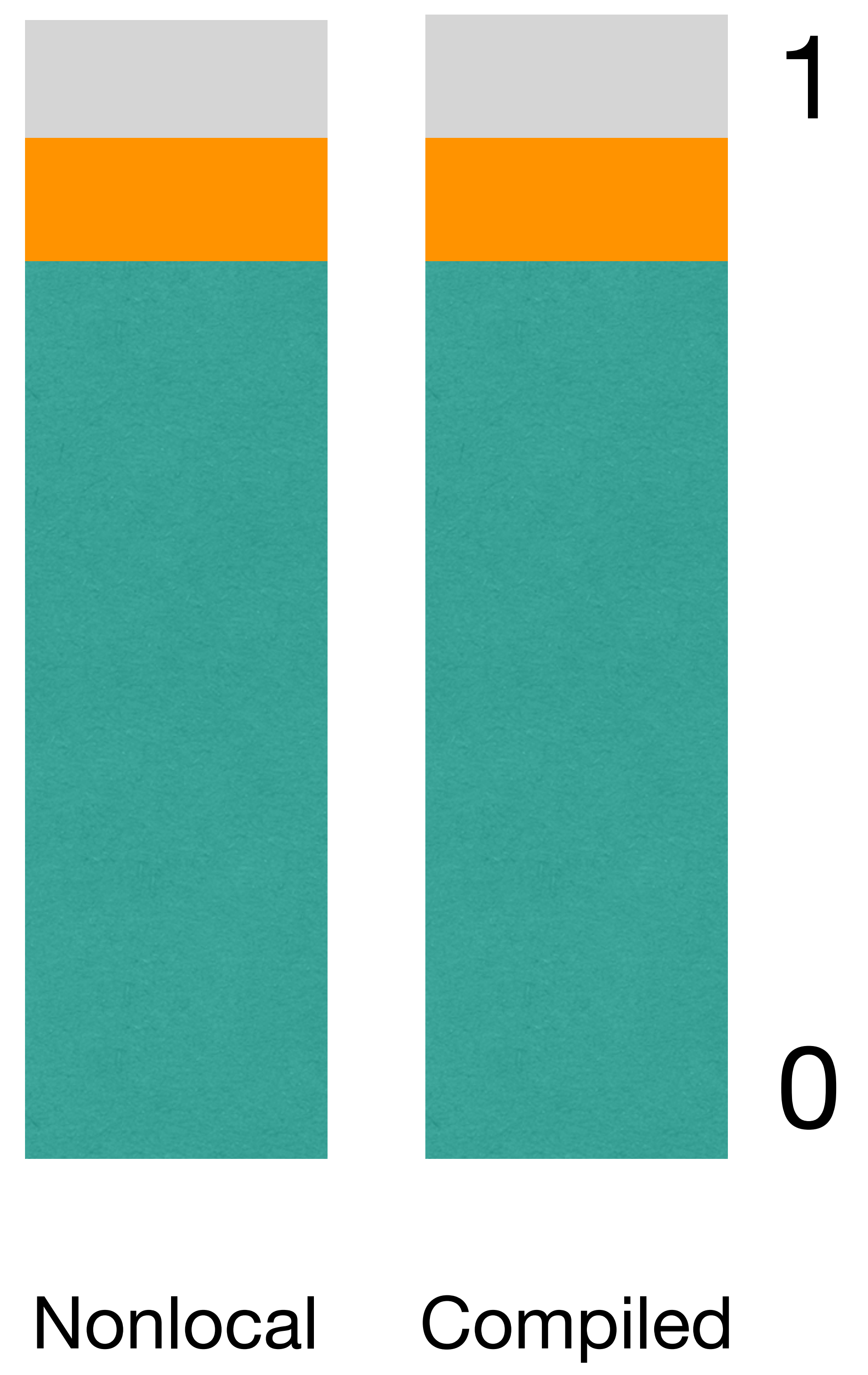


Works for all k players games!

Properties of KLVY compiler

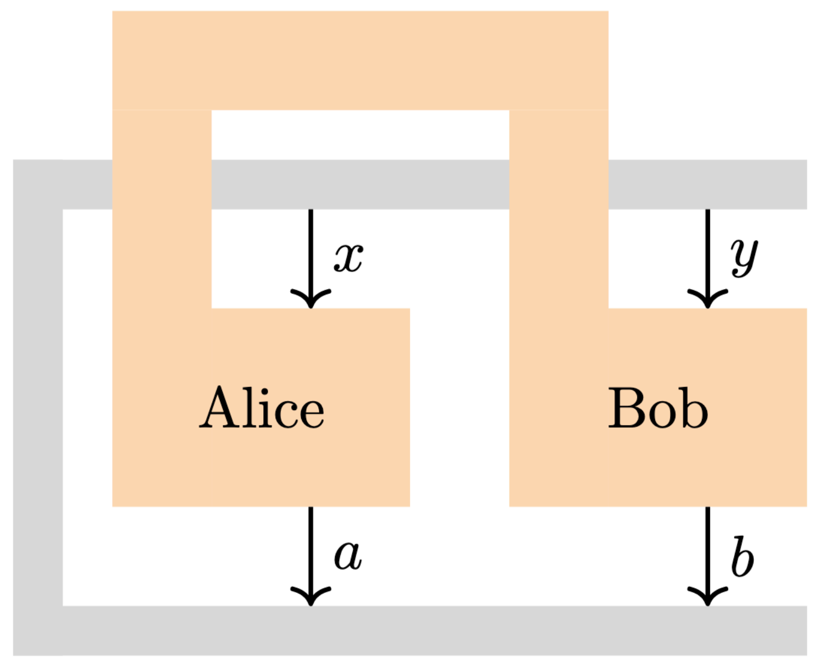
- Are compiled games trustworthy?
- Completeness: honest strategies reaches the ideal score
- Soundness: cheating strategies cannot exceed physical limits

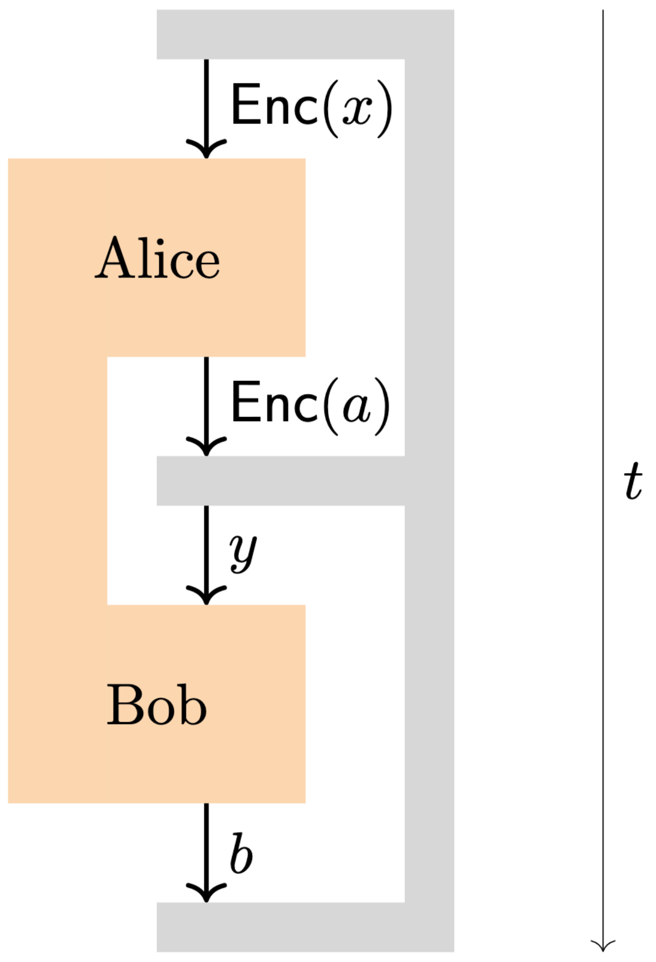
1. Classical soundness for all games [KLVY22]
2. Quantum completeness for all games [KLVY22]
3. Quantum soundness was opened, only partially understood for bipartite cases
4. With [KPRSTXZ25, BKLRŠTX25]: Quantitative upper bounds of compiled scores for <u>all</u> multipartite games



[KLVY22] arXiv: 2203.15877

Security parameter λ

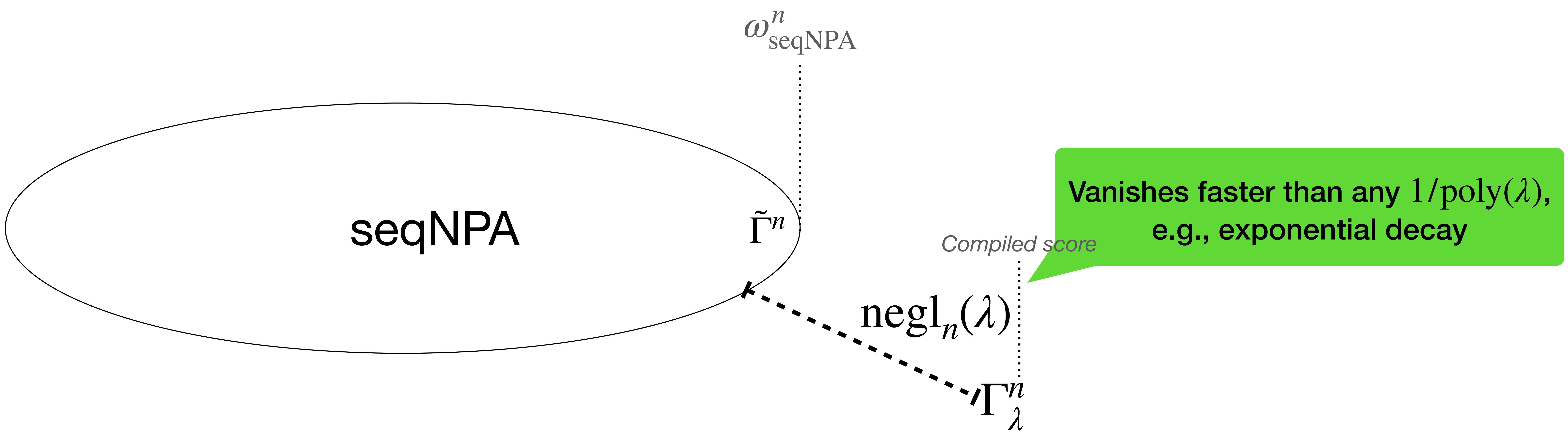




- Models both computational power and encryption strength
- A λ-efficient prover can run circuits with poly(λ) quantum gates
- λ-secure encryption safe against all λ-efficient provers' attacks

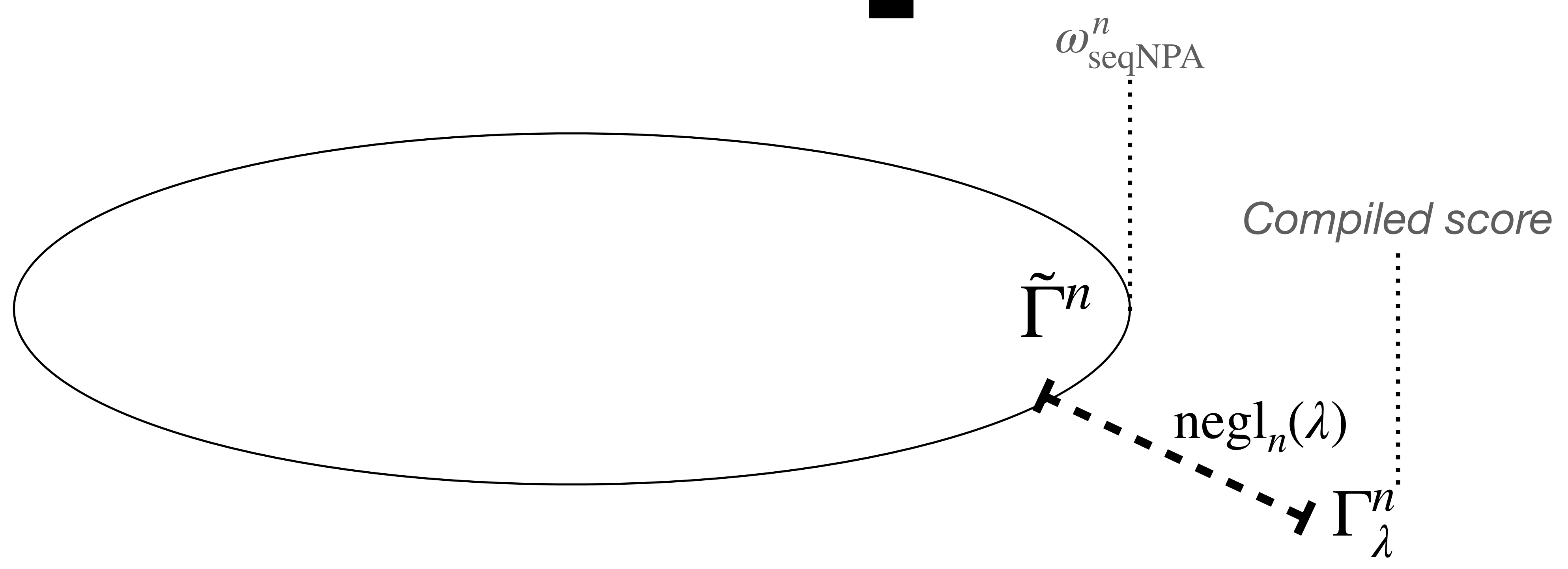
Efficient prover and the sequential hierarchy

- Quantum strategy of a λ-efficient prover is a sequential strategy that is "almost" operationally-non-signaling
- For every λ and n, it gives moment matrix Γ_λ^n
- Theorem: it is almost a solution of the sequential hierarchy

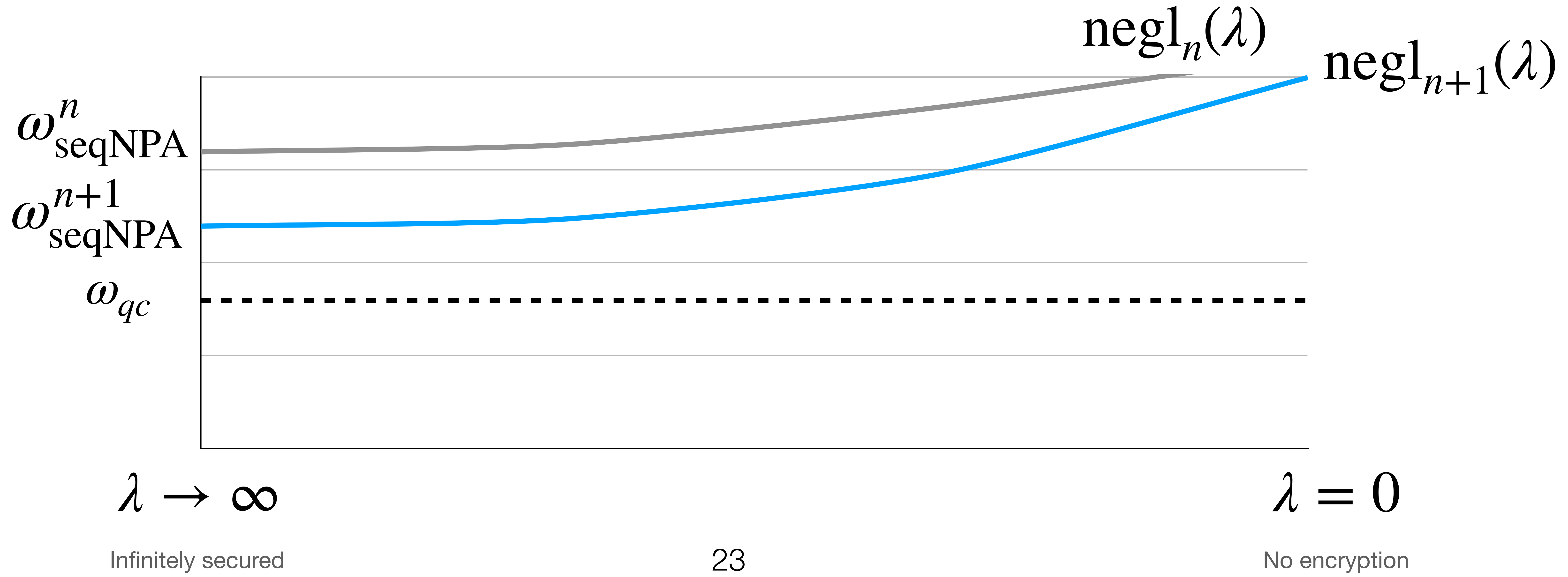


Main results: [BKLRŠTX25]

- Theorem: λ-efficient strategy



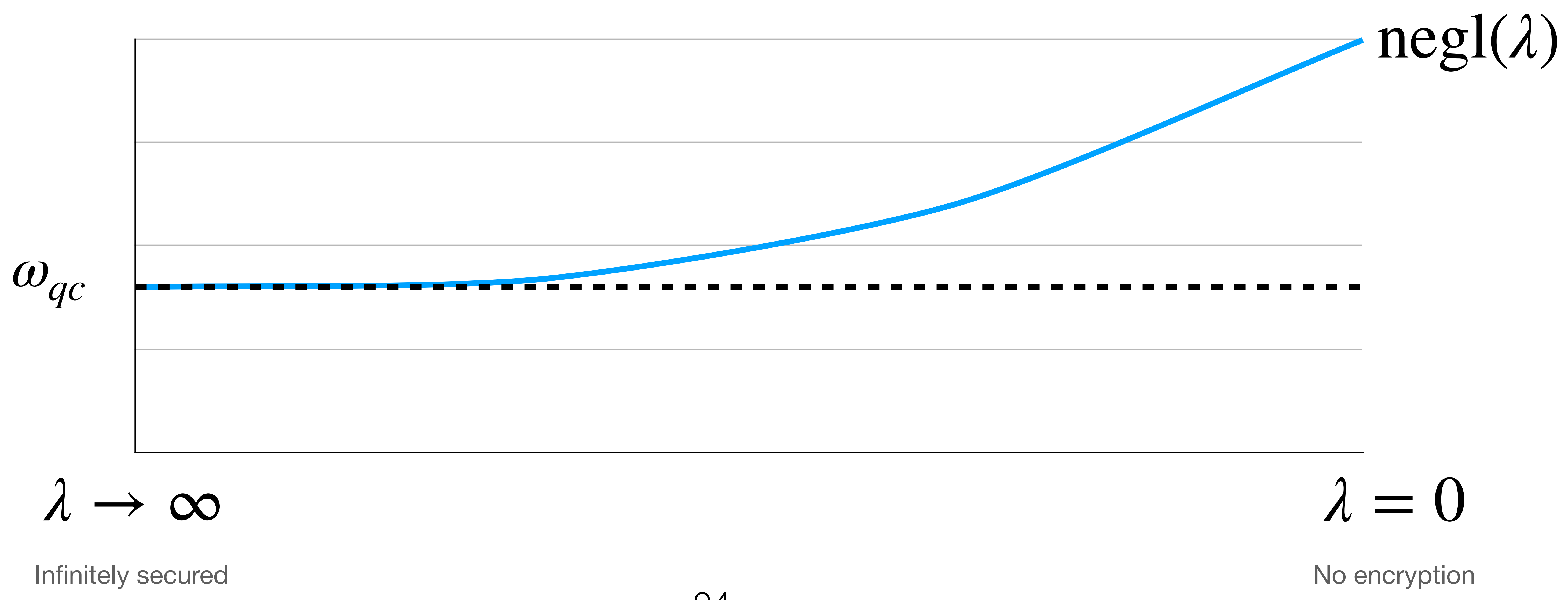
- The larger the n the tighter the bound



Main results: [BKLRŠTX25]

- If game admits a flat optimal solution, then finite NPA convergence, thus remove n-dependence

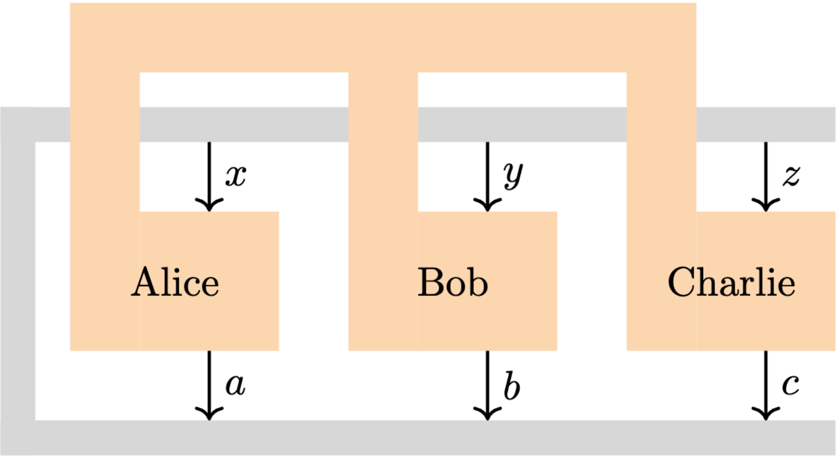
- At finite λ, compiled score of an efficient prover can only beat the nonlocal quantum score by a negligible amount



Conclusion

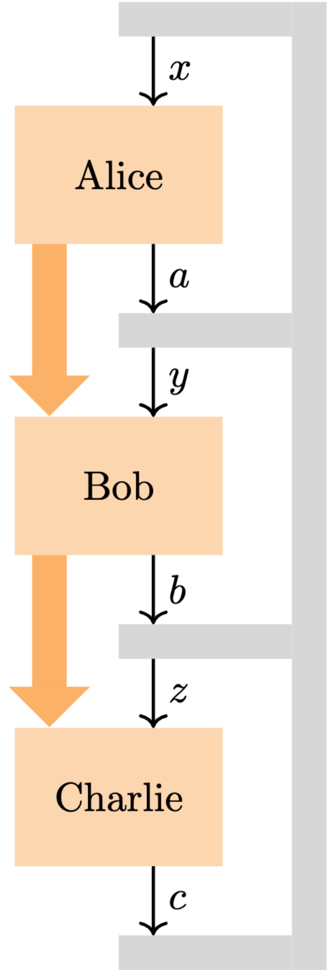
- Generalized NPA moment-SOS hierarchy that can describe sequentiality and quantum instruments/completely positive maps
- Flexible in the constraints, and could be useful to other problems?
- Application: quantitative quantum soundness for compiled nonlocal game
- $\Longrightarrow$ making compiled nonlocal game a practical venue to test Bell nonlocality with a single untrusted quantum computer

Asymptotic to quantitative: [KPRSTXZ25, BKLRŠTX25]



Non-local game

$\omega^1_{\mathrm{seqNPA}} \geq \omega^2_{\mathrm{seqNPA}} \geq \cdots \geq \omega_{\mathrm{qc}}$



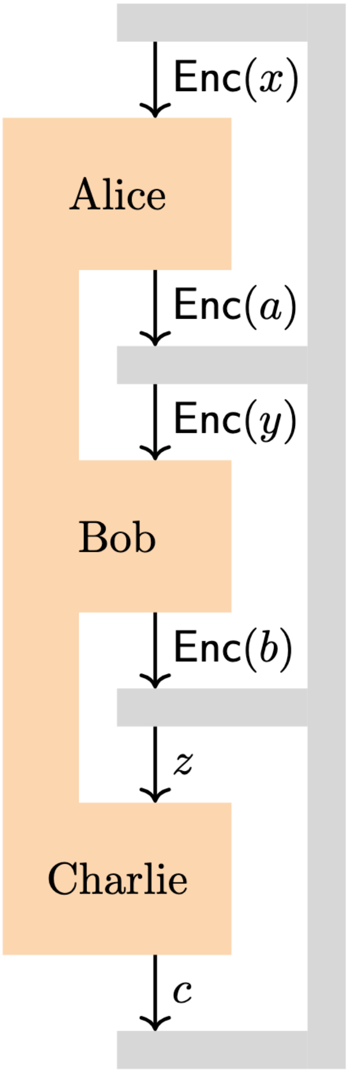
New NPA-like hierarchy for the quantum instruments

+ Solution of the sequential NPA hierarchy at every n
+ Operationally-non-signaling

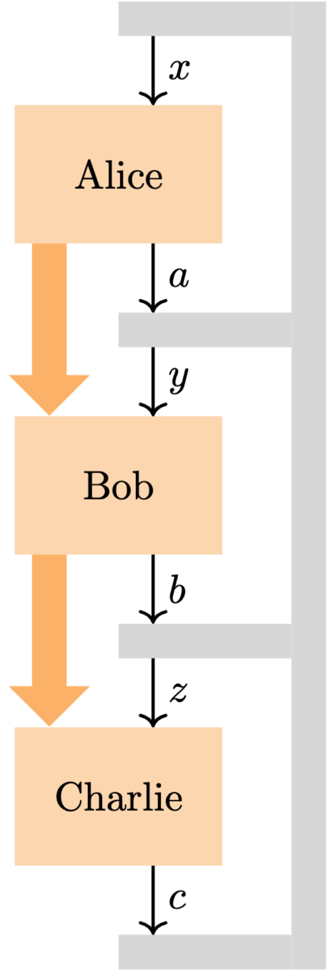
KLVY compiler

For all games, compiles score $\leq \omega^n_{\mathrm{seqNPA}} + \mathrm{negl}_n(\lambda)$

Novel geometric argument: $\mathrm{negl}_n(\lambda)$-close

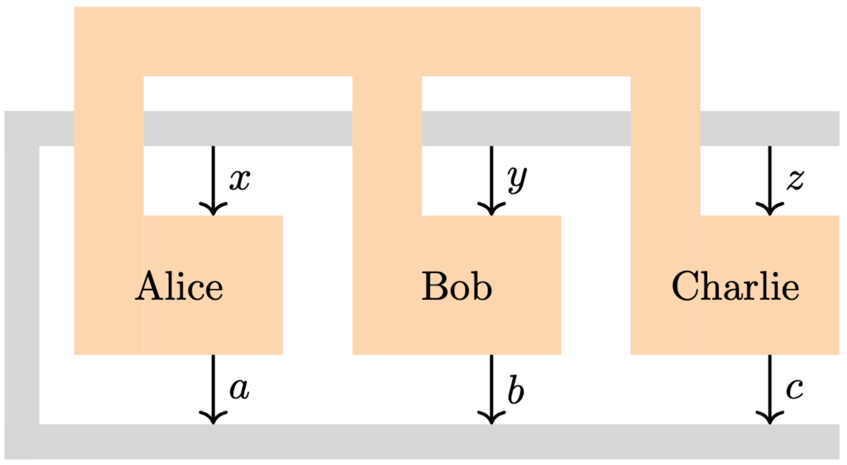


Sequential game



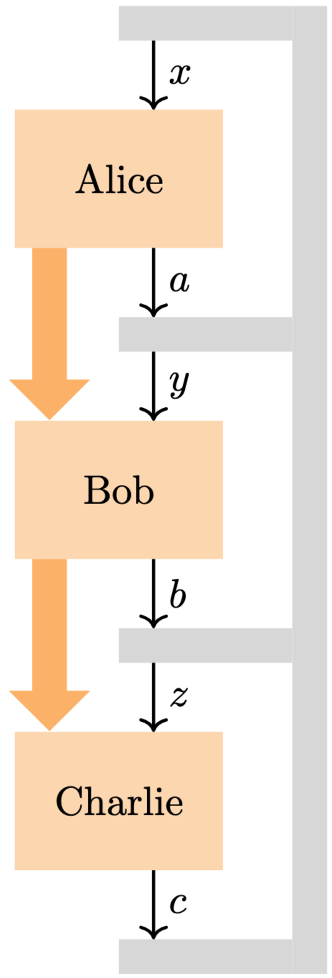
+ Almost non-signaling condition from security against efficient provers
+ Almost-solution of the sequential NPA hierarchy at every n

Outline for multipartite asymptotic soundness [BLJŠ25]



Non-local game

New operator algebraic theorem

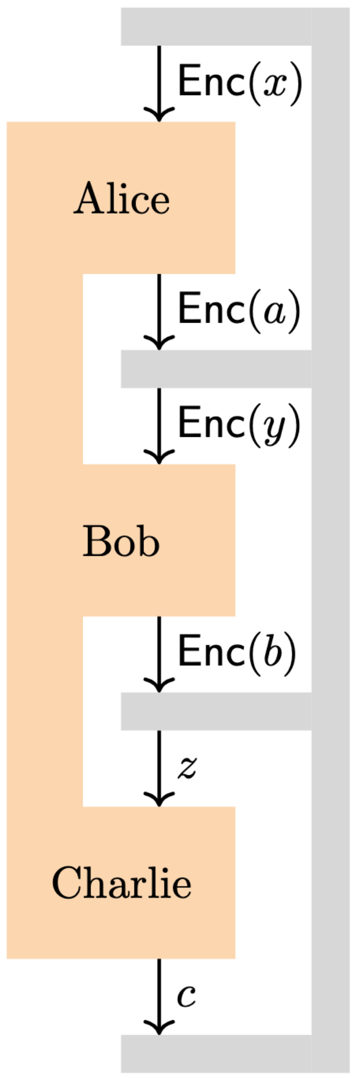


\+ Operationally-non-signaling

KLVY compiler

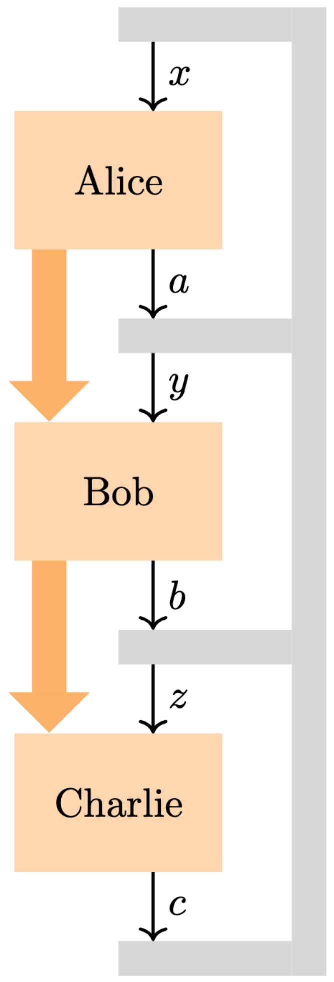
Operator algebraic: Sequential scenarios with quantum instruments

$\lambda \to \infty$



Sequential game

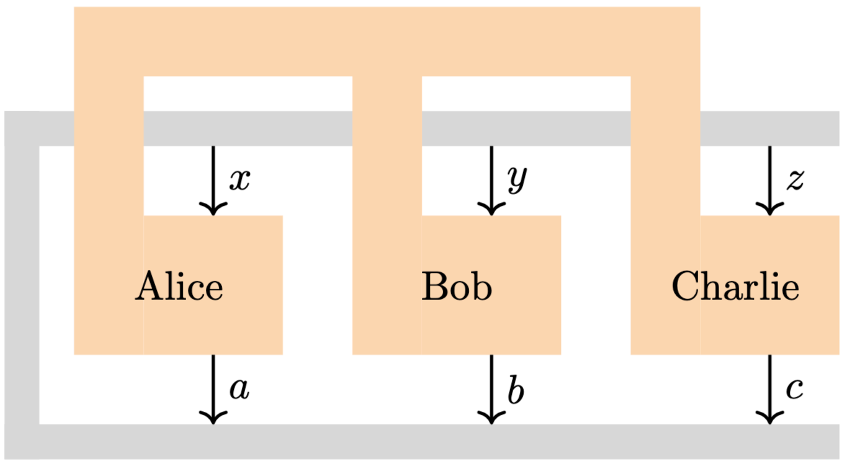
A mapping to unravel compiled games



\+ λ-security against λ-efficient provers

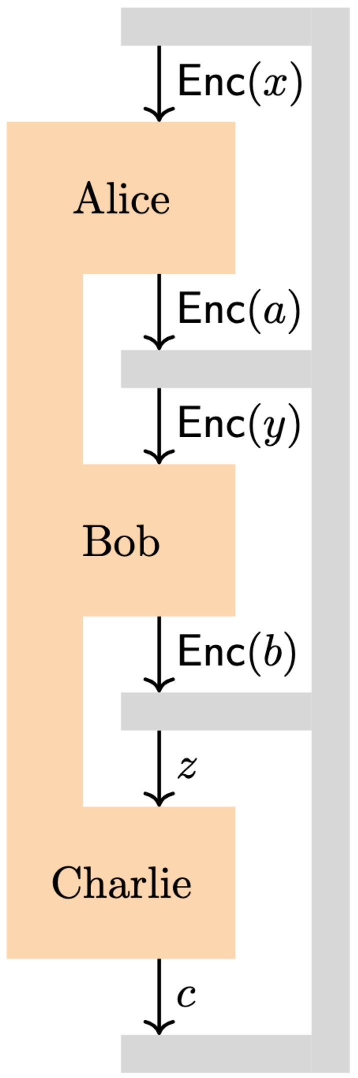
\+ Almost non-signaling condition

Asymptotic to quantitative: [KPRSTXZ25, BKLRŠTX25]



Non-local game

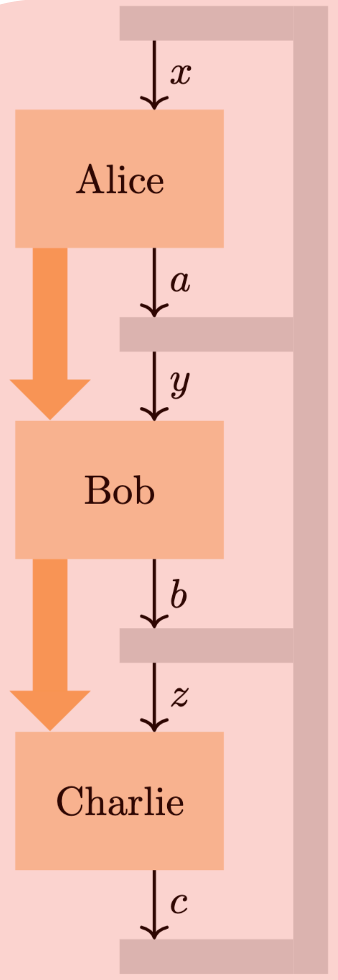
KLVY compiler



Sequential game

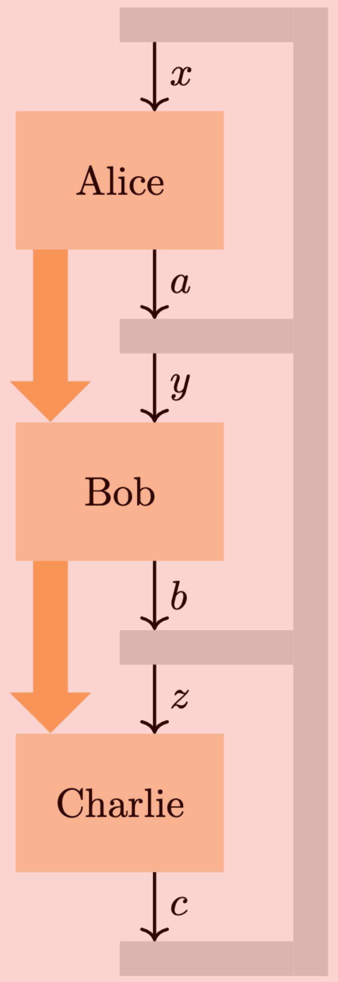
NPA hierarchy for sequential scenarios!

Sequential scenarios formulated with quantum instruments



+ Operationally-non-signaling

$\lambda \to \infty$



+ Almost non-signaling condition from security against efficient provers