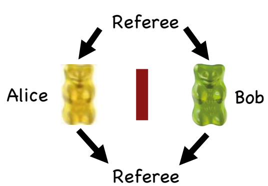
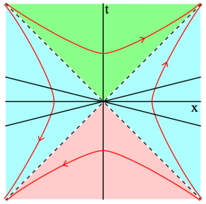
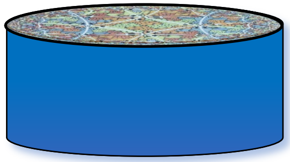
Trading Space for Time in Nonlocal Games

Michael Walter







Quantum Extreme Universe Workshop, Okinawa, Oct 2024

RUHR UNIVERSITÄT BOCHUM RUB

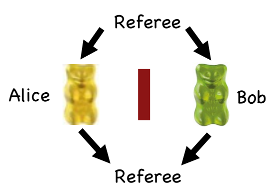
European Research Council
Established by the European Commission

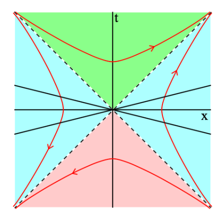
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

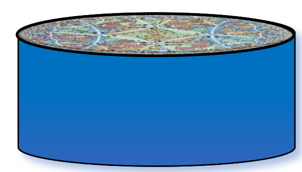
Trading Space for Time in Nonlocal Games

or: Playing Games with Locality

Michael Walter



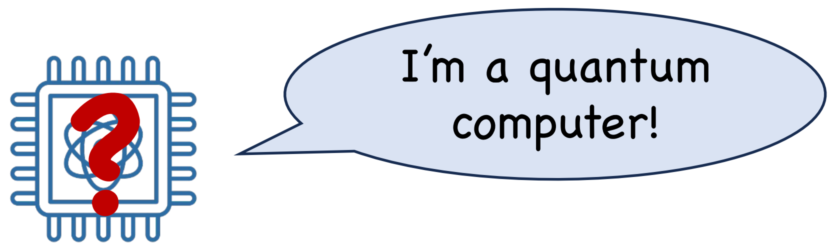




Quantum Extreme Universe Workshop, Okinawa, Oct 2024

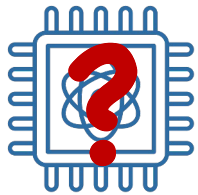
RUHR UNIVERSITÄT BOCHUM RUB
European Research Council
Established by the European Commission
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Can one trust a quantum computer?



Can a classical "verifier" convince themselves that they are indeed interacting with a quantum computer?

Can one trust a quantum computer?



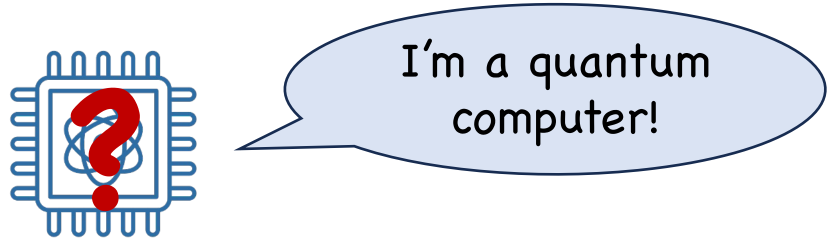
I’m a quantum computer!

Can a classical “verifier” convince themselves that they are indeed interacting with a quantum computer?

Idea: Violate a Bell inequality.

[TU Delft]

Can one trust a quantum computer?



Can a classical "verifier" convince themselves that they are indeed interacting with a quantum computer?

[TU Delft]

Idea: Violate a Bell inequality.

Easy to verify. Remarkably, can be extended to verify arbitrary quantum computation!

[Reichardt et al, ..., Grilo]

☹ need two devices
☹ need to ensure they are spacelike

Can one trust a quantum computer?

Can a classical “verifier” interacting with single device do the job?

Possibly! Any quantum computation can be simulated classically, but in general only *inefficiently* *(or so we believe)...*

Can one trust a quantum computer?

Can a classical "verifier" interacting with single device do the job?

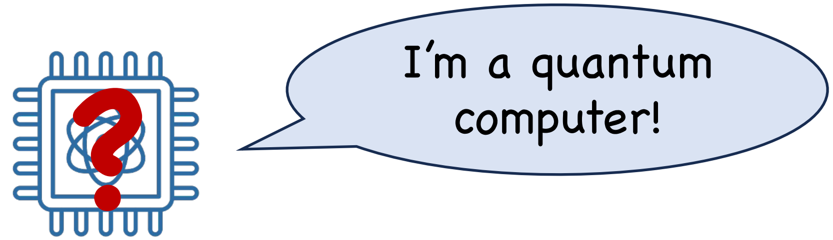
Possibly! Any quantum computation can be simulated classically, but in general only *inefficiently (or so we believe)...*

Idea: Ask it to factor a number.

☺ easy to verify
☹ not universal – only certifies that we can factor

Can one trust a quantum computer?

Can a classical "verifier" interacting with single device do the job?



Possibly! Any quantum computation can be simulated classically, but in general only *inefficiently* *(or so we believe)...*

Idea: Ask it to factor a number.

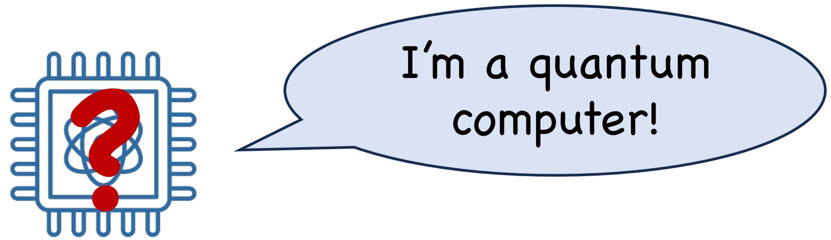
☺ easy to verify
☹ not universal – only certifies that we can factor

Better idea: Ask it to solve universal (BQP-complete) problem.

Can be made to work. Breakthrough gave first classical verification protocol for single device *under computational assumptions*. [Mahadev]

namely that device is efficient & some computational problem is hard

How can one trust a quantum computer?



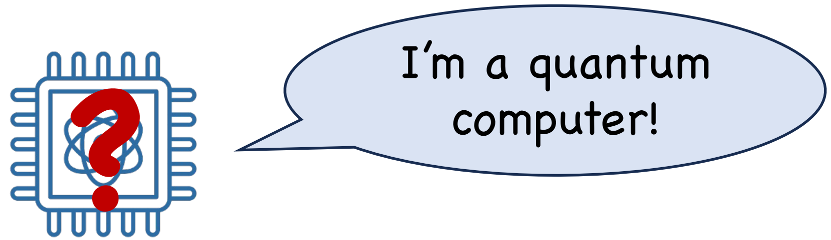
Nonlocal Approach

- need two <u>spacelike</u> devices
- no assumption on inner workings

Computational Approach

- a single device is enough
- need to assume device is <u>efficient</u> (polynomial-time)

How can one trust a quantum computer?



Nonlocal Approach

- need two <u>spacelike</u> devices
- no assumption on inner workings

???

Computational Approach

- a single device is enough
- need to assume device is <u>efficient</u> (polynomial-time)

Question: Is there a systematic link between these two worlds?

Cf. how can locality emerge for bounded complexity observers?

Nonlocal games

[Bell, Clauser-Horne
-Shimony-Holt, ...]

Two non-communicating players play against a referee:

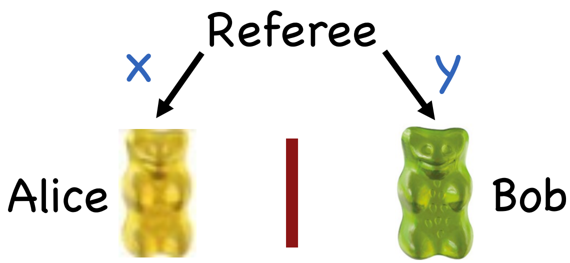
Referee

Alice   Bob

Nonlocal games

[Bell, Clauser-Horne -Shimony-Holt, ...]

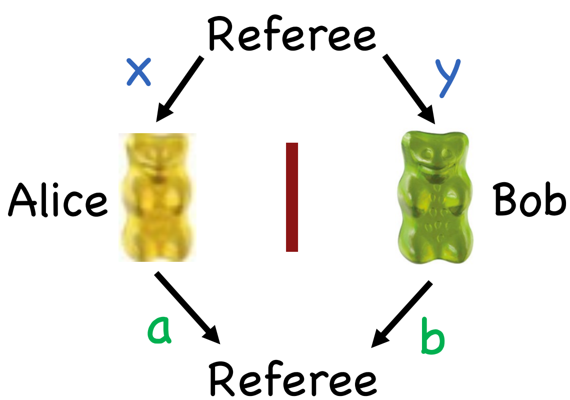
Two non-communicating players play against a referee:



Nonlocal games

[Bell, Clauser-Horne -Shimony-Holt, ...]

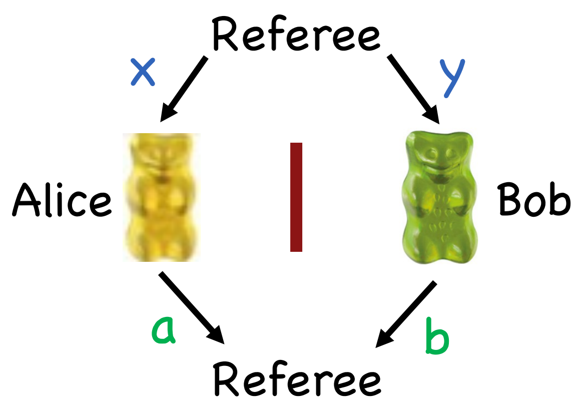
Two non-communicating players play against a referee:



Nonlocal games

[Bell, Clauser-Horne -Shimony-Holt, ...]

Two non-communicating players play against a referee:



Winning Condition (**CHSH Game**)

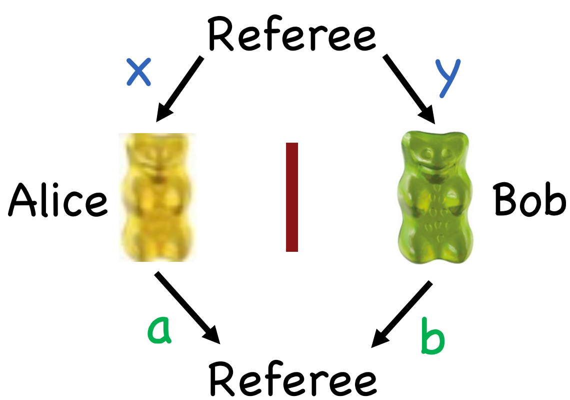
x	y	a + b
0	0	even
0	1	even
1	0	even
1	1	odd

Question: Can classical players win this game?

Nonlocal games

[Bell, Clauser-Horne -Shimony-Holt, ...]

Two non-communicating players play against a referee:



Winning Condition (**CHSH Game**)

x	y	$a(x) + b(y)$
0	0	even
0	1	even
1	0	even
1	1	odd

Are there suitable "answer functions" $a(x)$, $b(y)$? If so, then...

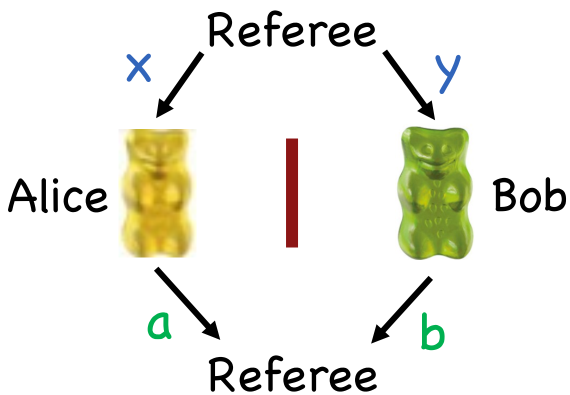
$$\big(a(0) + b(0)\big) + \big(a(0) + b(1)\big) + \big(a(1) + b(0)\big) + \big(a(1) + b(1)\big)$$

...would be **odd**. But each answer appears **twice**. **Contradiction!**

Nonlocal games

[Bell, Clauser-Horne -Shimony-Holt, ...]

Two non-communicating players play against a referee:



Winning Condition (**CHSH Game**)

x	y	a(x) + b(y)
0	0	even
0	1	even
1	0	even
1	1	odd

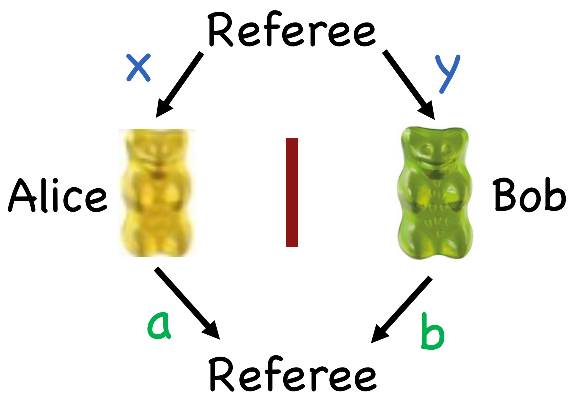
There is no "classical" way to win CHSH game: $p_{\text{win}}^{\text{classical}} \leq \frac{3}{4}$

This is a Bell inequality!

Nonlocal games

[Bell, Clauser-Horne
-Sh]

Two non-communicating players play against a referee:



Winning Condition (**CHSH Game**)

x	y	a + b
0	0	even
0	1	even
1	0	even
1	1	odd

There is no "classical" way to win CHSH game: $p_{\text{win}}^{\text{classical}} \leq \frac{3}{4}$

This is a Bell inequality!

[TU Delft]

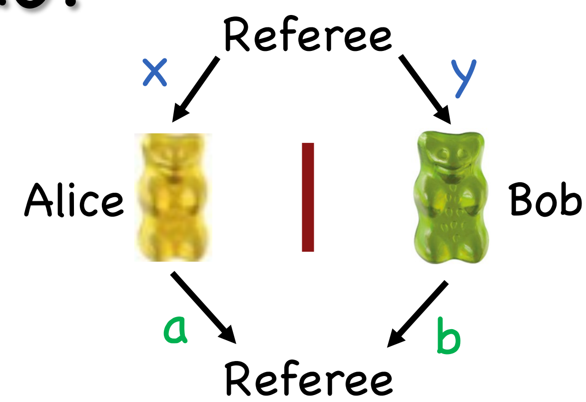
If the players share quantum entanglement they can do better!

How well can quantum players do?

If they share EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and use complementary measurements, can achieve:

$$p_{\text{win}}^{\text{quantum}} \approx \mathbf{85\%}$$

and this is optimal [Tsirelson]

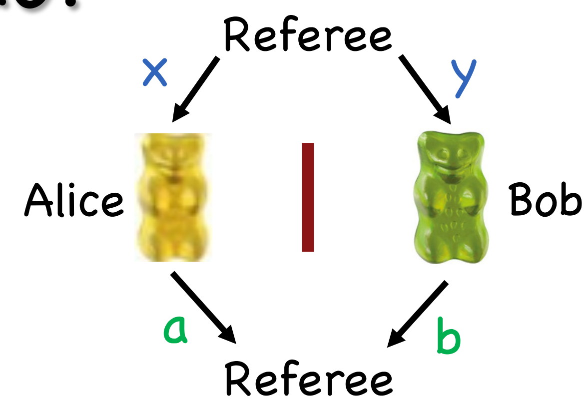


How well can quantum players do?

If they share EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and use complementary measurements, can achieve:

$$p_{\text{win}}^{\text{quantum}} \approx \mathbf{85\%}$$

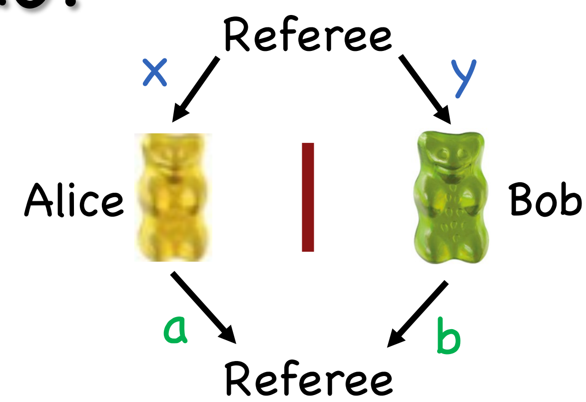
and this is optimal [Tsirelson]



Amazingly, optimal quantum strategy is "unique" and "rigid"!

"Operational" characterization of entanglement!

How well can quantum players do?



If they share EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and use complementary measurements, can achieve:

$$p_{\text{win}}^{\text{quantum}} \approx 85\%$$

and this is optimal [Tsirelson]

Amazingly, optimal quantum strategy is "unique" and "rigid"!

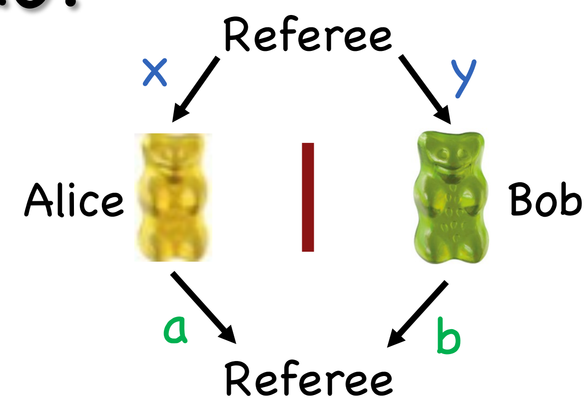
"Operational" characterization of entanglement!

Classical verifier can verify & control untrusted pair of quantum devices [Reichard-Unger-Vazirani, ...]

→ *device-independent cryptography*

Reason: Hidden symmetry! Roughly, ϵ-optimal strategy ⇔ ϵ-representation of G = <X,Z>, and there is a nearby exact representation [Gowers-Hatami] ☺

How well can quantum players do?



If they share EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and use complementary measurements, can achieve:

$$p_{\text{win}}^{\text{quantum}} \approx 85\%$$

and this is optimal [Tsirelson]

Amazingly, optimal quantum strategy is "unique" and "rigid"!

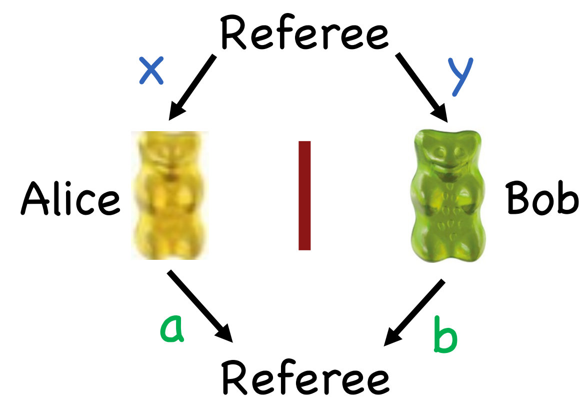
"Operational" characterization of entanglement!

Classical verifier can verify & control untrusted pair of quantum devices

So long they can't communicate (are spacelike)!

Reason: Hidden symmetry! Roughly, ϵ-optimal strategy ⇔ ϵ-representation of G = <X,Z>, and there is a nearby exact representation [Gowers-Hatami] ☺

Nonlocal games and their values

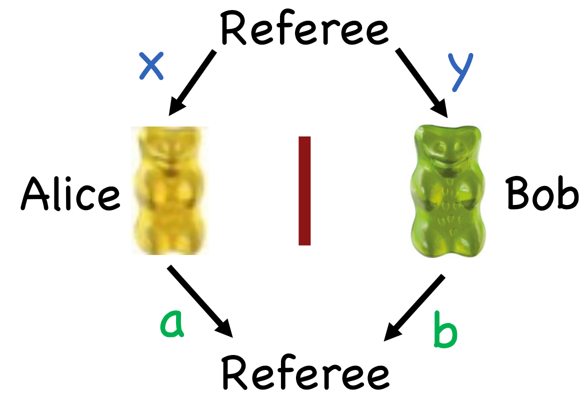


The players' strategy determines their winning probability.

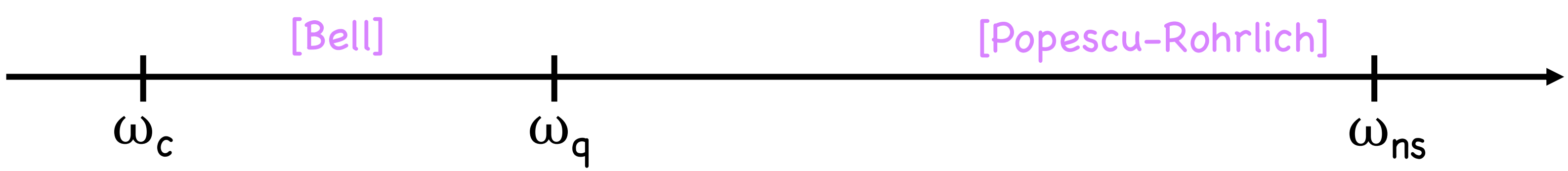
> The optimal winning probability for some class of strategies is called a **"value"**:

Nonlocal games and their values

The players' strategy determines their winning probability.



The optimal winning probability for some class of strategies is called a **"value"**:



Classical value

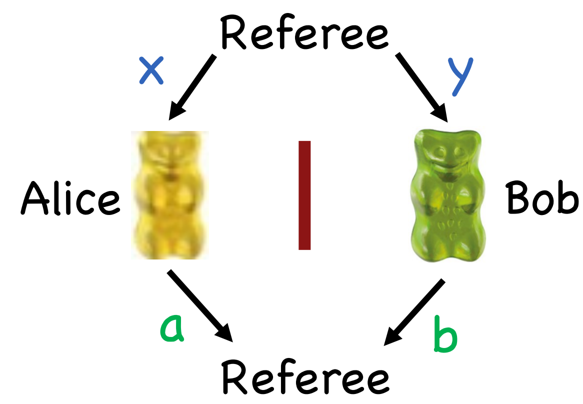
Quantum value

Non-signaling value

$p(a|xy) = p(a|x)$
$P(b|xy) = p(b|y)$

Nonlocal games and their values

The players' strategy determines their winning probability.



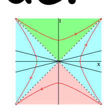
> The optimal winning probability for some class of strategies is called a **"value"**:

[Bell] [MIP*=RE] [Popescu-Rohrlich]

ω_c ω_q ω_{qc} ω_{ns}

Classical value

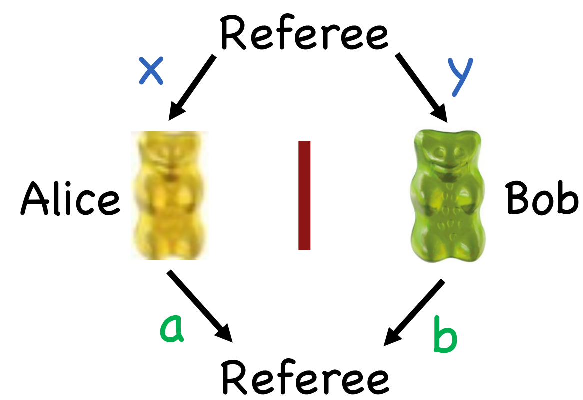
Quantum value
$H_A \otimes H_B$

Quantum commuting operator value:
$[A,B] = 0$ 

Non-signaling value
$p(a|xy) = p(a|x)$
$P(b|xy) = p(b|y)$

Nonlocal games and their values

The players' strategy determines their winning probability.



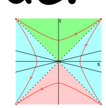
The optimal winning probability for some class of strategies is called a **"value"**:

[Bell] [MIP*=RE] [Popescu-Rohrlich]

ω_c ω_q ω_{qc} ω_{ns}

Classical value

Quantum value
$H_A \otimes H_B$

Quantum commuting operator value:
$[A,B] = 0$ 

Non-signaling value
$p(a|xy) = p(a|x)$
$P(b|xy) = p(b|y)$

In general **all distinct**!

Crucially, <u>no</u> assumption about the player's efficiency!

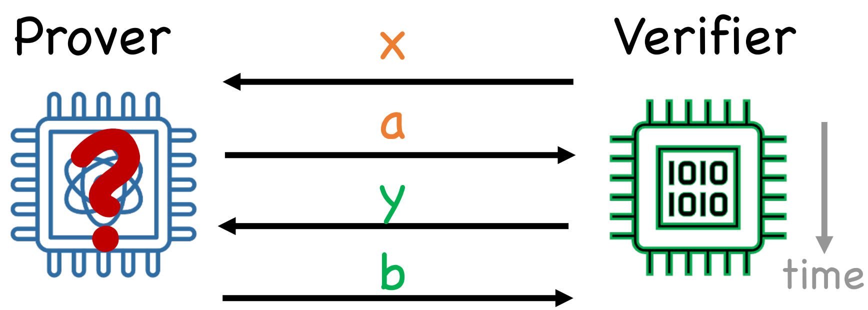
Trading space for (polynomial) time

Question: Can we get rid of spacelike separation and play a nonlocal game with a **single** efficient player (“prover”)?

Trading space for (polynomial) time

Question: Can we get rid of spacelike separation and play a nonlocal game with a **single** efficient player ("prover")?

Naïve attempt: Just play sequentially.

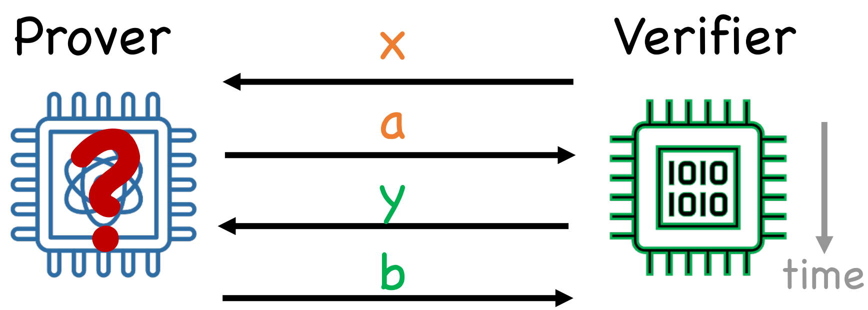


This cannot work because it even allows forward signaling!

Trading space for (polynomial) time

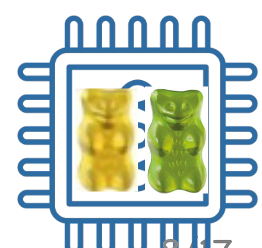
Question: Can we get rid of spacelike separation and play a nonlocal game with a **single** efficient player ("prover")?

Naïve attempt: Just play sequentially.



This cannot work because it even allows forward signaling!

Idea: Use cryptography to force prover to "simulate" two spacelike players **(as long as they are unable to break the cryptography)**!

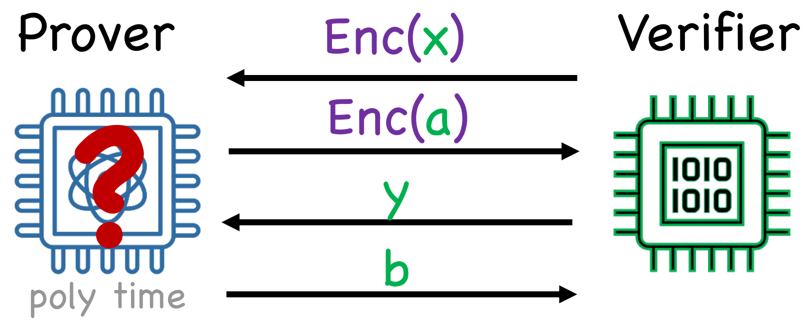


long history in crypto

Trading space for time – the KLVY way

Kalai-Lombardi-Vaikuntanathan-Yang:

Encrypt Alice's question x, while sending Bob's question y in plain.

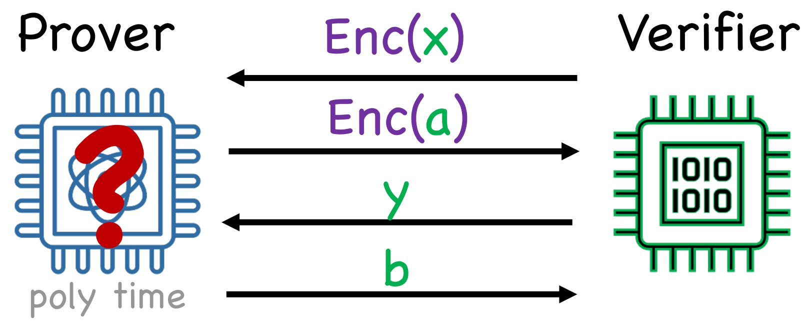


Intuition: Since prover does not know secret key, encrypted messages cannot usefully be "combined" with plain ones (as if they were spacelike)?

Trading space for time – the KLVY way

Kalai-Lombardi-Vaikuntanathan-Yang:

Encrypt Alice's question x, while sending Bob's question y in plain.



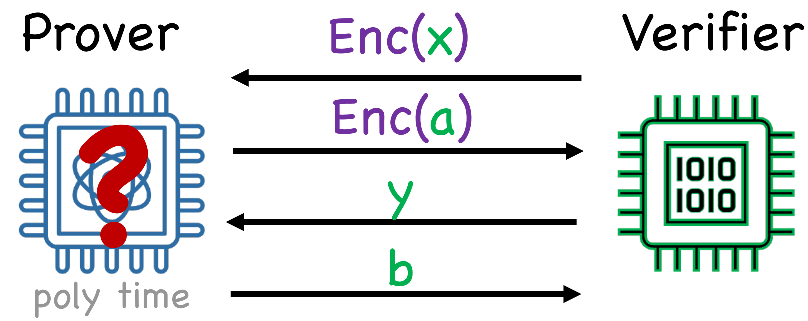
Intuition: Since prover does not know secret key, encrypted messages cannot usefully be "combined" with plain ones (as if they were spacelike)?

Problem: Since prover does not know key, how can they do *anything?*

Trading space for time – the KLVY way

Kalai-Lombardi-Vaikuntanathan-Yang:

Encrypt Alice's question x, while sending Bob's question y in plain.

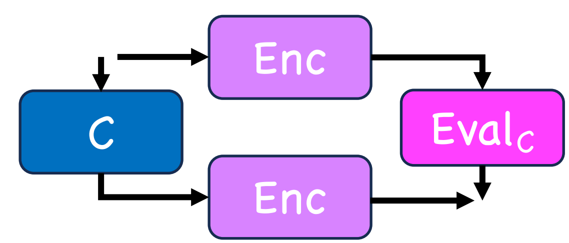


Intuition: Since prover does not know secret key, encrypted messages cannot usefully be "combined" with plain ones (as if they were spacelike)?

Problem: Since prover does not know key, how can they do *anything?*

Solution: Use "homomorphic" encryption scheme!

= allows computing on encrypted data

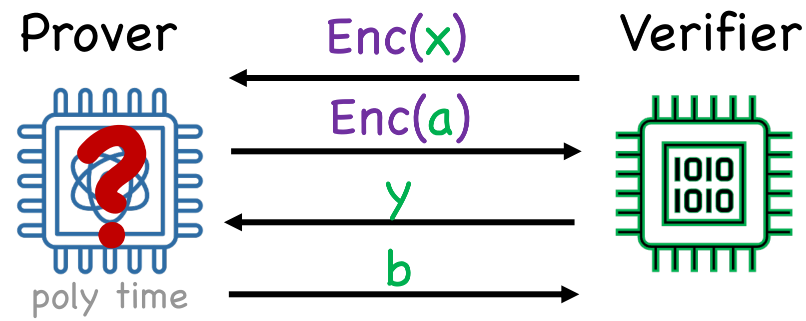


for circuit C

Trading space for time – the KLVY way

Kalai-Lombardi-Vaikuntanathan-Yang:

Encrypt Alice's question x, while sending Bob's question y in plain.

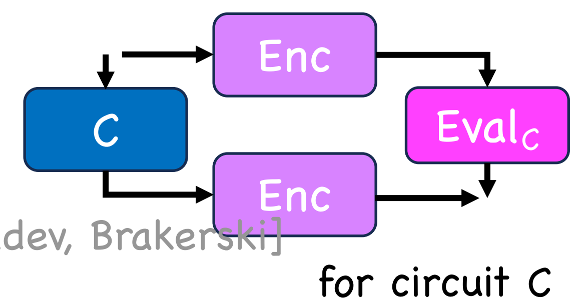


Intuition: Since prover does not know secret key, encrypted messages cannot usefully be "combined" with plain ones (as if they were spacelike)?

Problem: Since prover does not know key, how can they do *anything?*

Solution: Use "homomorphic" encryption scheme!

= allows computing on encrypted data

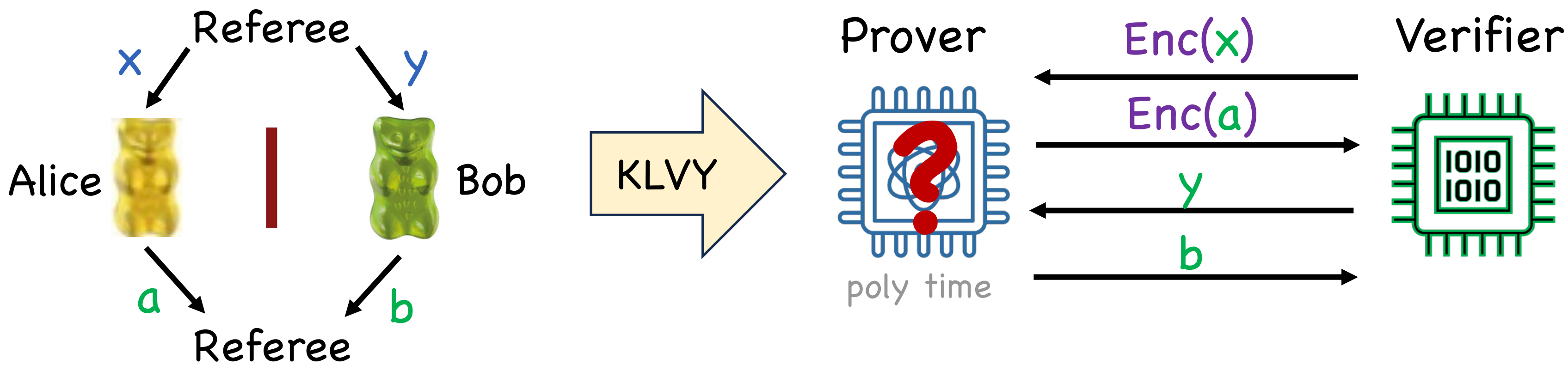


These exist under computational assumptions. [Mahadev, Brakerski]

→ General "compiler" that applies to any nonlocal game ☺

Trading space for time – the KLVY way

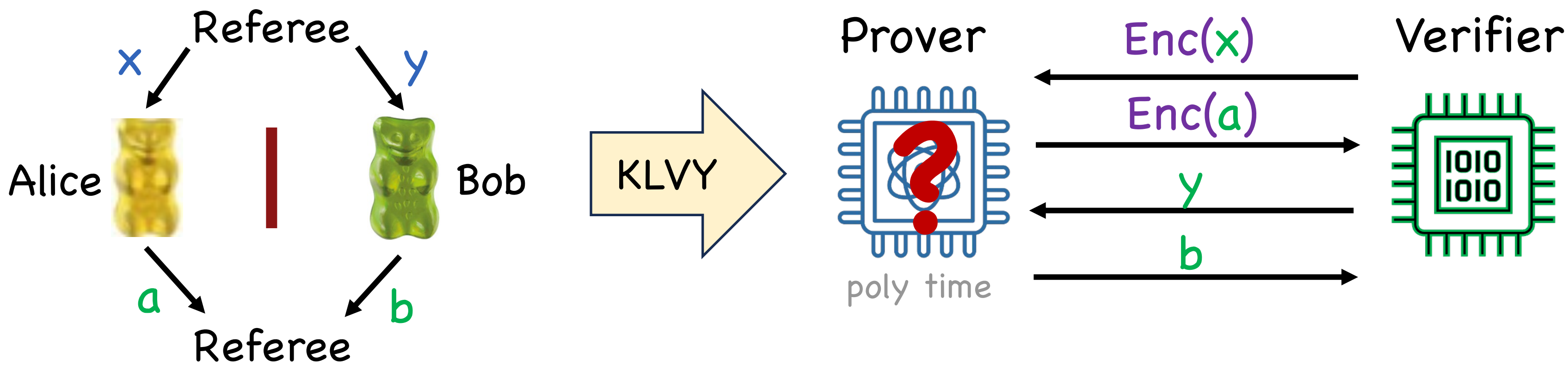
Given any nonlocal game, can "compile" into a single-prover protocol:



Key question: What properties of the nonlocal game are preserved?

Trading space for time – the KLVY way

Given any nonlocal game, can "compile" into a single-prover protocol:



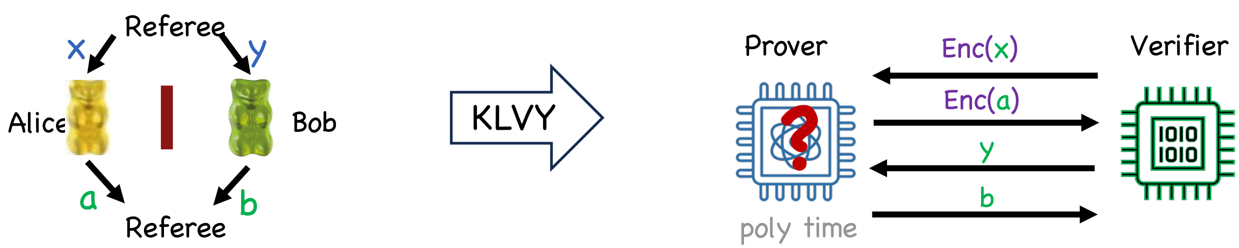
Key question: What properties of the nonlocal game are preserved?

As discussed, provers can do at least as well as in nonlocal game. $\omega_{\text{compiled}} \geq \omega$

But why can't they do better? Not obvious!

- At first glance, cryptography only ensures "non-signaling".
- But this is **not** enough!
- Natural variations do **not** work ("spooky" encryption)!

What we know: Trading space for time



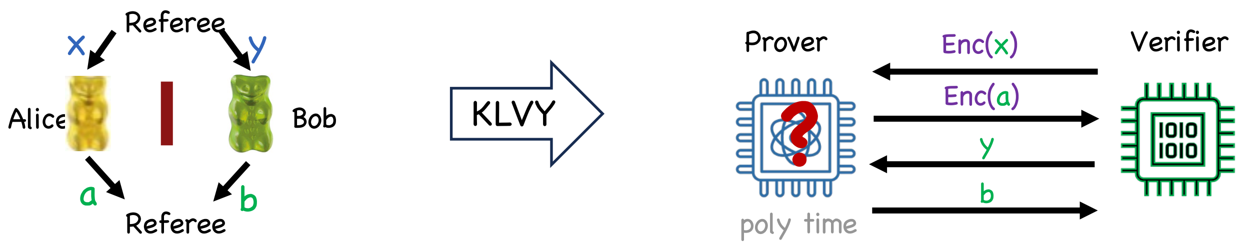
Classical Soundness (KLVY): Efficient classical provers cannot cheat, i.e. exceed classical value of nonlocal game.

$\omega_{c,\text{compiled}} \leq \omega_c$

Thus, if observe $p_{win} > \omega_c$ this constitutes proof of non-classicality! ☺

All results hold for large security parameter ("key length").

What we know: Trading space for time



Classical Soundness (KLVY): Efficient classical provers cannot cheat, i.e. exceed classical value of nonlocal game.

$\omega_{c,\text{compiled}} \leq \omega_c$

Thus, if observe $p_{win} > \omega_c$ this constitutes proof of non-classicality! ☺

Computational Tsirelson Theorem (Natarajan-Zhang, Cui-…-W):

- For "XOR games", quantum provers cannot exceed q. value.
- Near optimal strategies yield "logical qubits" inside prover!

$\omega_{q,\text{compiled}} \leq \omega_q$

$$B_0 B_1 \approx -B_1 B_0$$

This is good enough to verify q. computations. ☺

All results hold for large security parameter ("key length").

What we know: Trading space for time for <u>all</u> nonlocal games

[Kulpe-Malavolta-Paddock-Schmidt-W]

XOR games are *special* - they don't probe full power & complexity of spacelike quantum correlations. What can we say about *general* games?

All results hold for large security parameter ("key length").

What we know: Trading space for time for <u>all</u> nonlocal games

[Kulpe-Malavolta-Paddock-Schmidt-W]

XOR games are *special* - they don't probe full power & complexity of spacelike quantum correlations. What can we say about *general* games?

Quantum Soundness Theorem: Quantum provers cannot exceed quantum *commuting* operator value of nonlocal game.

$\omega_{q,\text{compiled}} \leq \omega_{qc}$

This generalizes prior works for CHSH and XOR games, where $\omega_{qc} = \omega_q$.

All results hold for large security parameter ("key length").

What we know: Trading space for time for all nonlocal games

[Kulpe-Malavolta-Paddock-Schmidt-W]

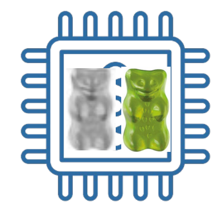
XOR games are *special* – they don't probe full power & complexity of spacelike quantum correlations. What can we say about *general* games?

Quantum Soundness Theorem: Quantum provers cannot exceed quantum *commuting* operator value of nonlocal game.

$\omega_{q,\text{compiled}} \leq \omega_{qc}$

This generalizes prior works for CHSH and XOR games, where $\omega_{qc} = \omega_q$.

Rigidity Theorem: For optimal quantum provers, "Bob" observables satisfy same relations as in nonlocal game.



All results hold for large security parameter ("key length").

What we know: Trading space for time for all nonlocal games

[Kulpe-Malavolta-Paddock-Schmidt-W]

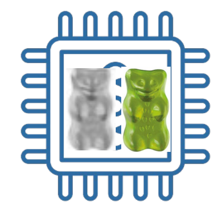
XOR games are *special* – they don't probe full power & complexity of spacelike quantum correlations. What can we say about *general* games?

Quantum Soundness Theorem: Quantum provers cannot exceed quantum *commuting* operator value of nonlocal game.

$\omega_{q,\text{compiled}} \leq \omega_{qc}$

This generalizes prior works for CHSH and XOR games, where $\omega_{qc} = \omega_q$.

Rigidity Theorem: For optimal quantum provers, "Bob" observables satisfy same relations as in nonlocal game.



To prove these, we connect notions that are usually treated separately:

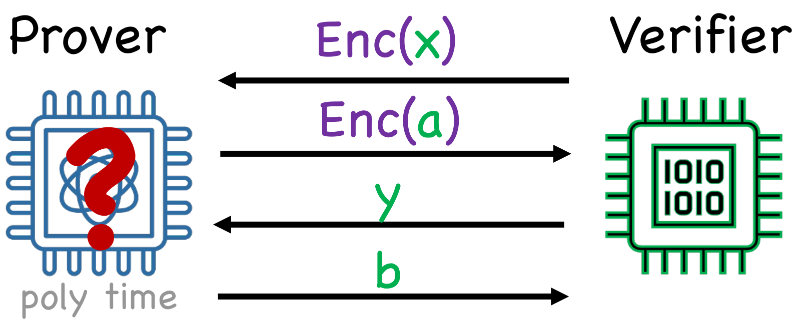
(1) *Timelike* characterization of *spacelike* correlations.
(2) *Computational* security → *info-theoretic* security.

Of independent interest?

How does it work?

Task: Given a quantum prover for the compiled game, wish to construct quantum strategy for the two-player game.

Let's analyze the situation:



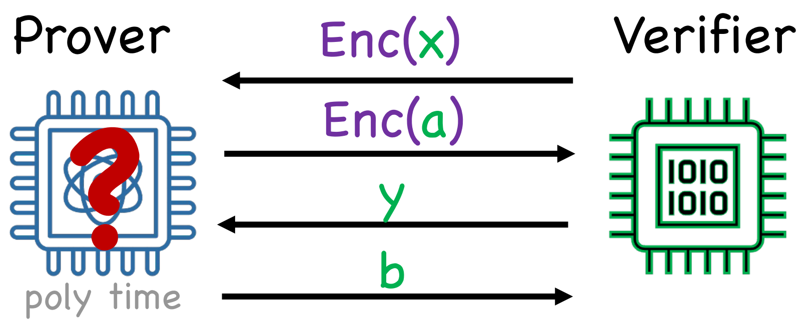
How does it work?

λ = security parameter
(key length)

Task: Given a quantum prover for the compiled game, wish to construct quantum strategy for the two-player game.

Let's analyze the situation:

Prover
= Algorithm
= Family of circuits
(one for each λ)



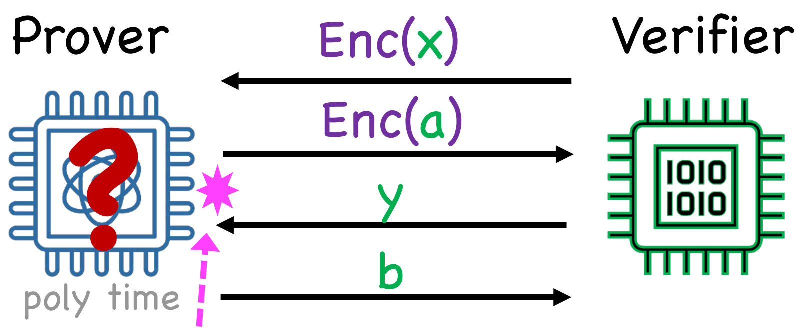
How does it work?

λ = security parameter
(key length)

Task: Given a quantum prover for the compiled game, wish to construct quantum strategy for the two-player game.

Let's analyze the situation:

Prover
= Algorithm
= Family of circuits
(one for each λ)



$\rho_x^\lambda = \sum_a \rho_{x,a}^\lambda$ = state after 2nd round

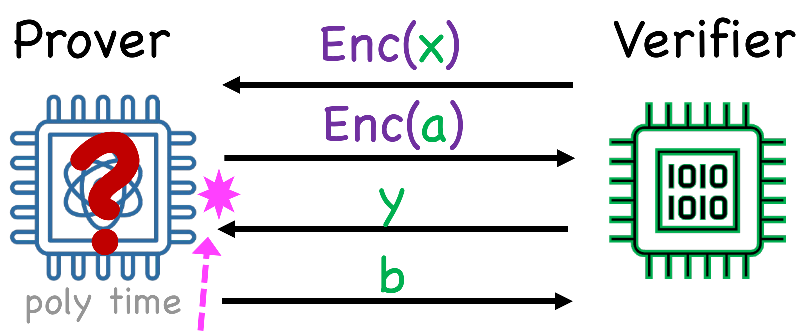
How does it work?

λ = security parameter
(key length)

Task: Given a quantum prover for the compiled game, wish to construct quantum strategy for the two-player game.

Let's analyze the situation:

Prover
= Algorithm
= Family of circuits
(one for each λ)



$\rho_x^\lambda = \sum_a \rho_{x,a}^\lambda$ = state after 2nd round

Observation: $\rho_x^\lambda \approx \rho_{x'}^\lambda$ are computationally indistinguishable!

no poly-time algo can tell the difference (otherwise could break crypto)

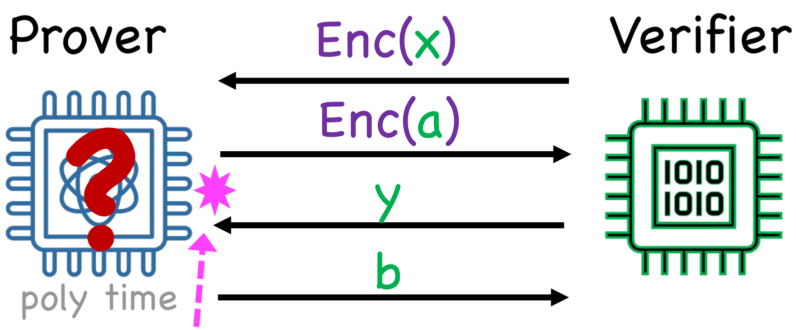
How does it work?

λ = security parameter
(key length)

Task: Given a quantum prover for the compiled game, wish to construct quantum strategy for the two-player game.

Let's analyze the situation:

Prover
= Algorithm
= Family of circuits
(one for each λ)



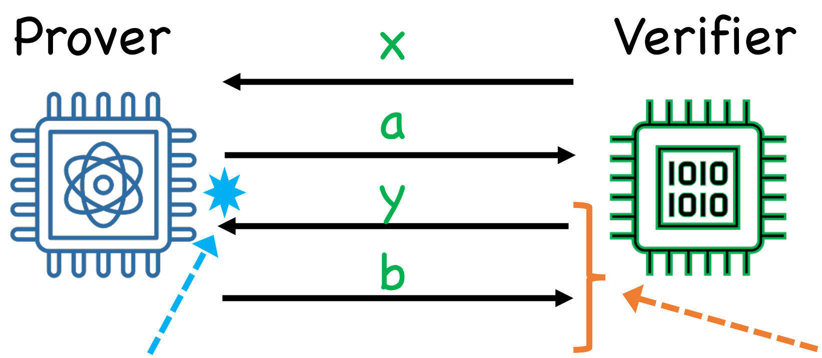
$\rho_x^\lambda = \sum_a \rho_{x,a}^\lambda$ = state after 2nd round

Observation: $\rho_x^\lambda \approx \rho_{x'}^\lambda$ are computationally indistinguishable!

no poly-time algo can tell the difference (otherwise could break crypto)

What if they were truly indistinguishable?

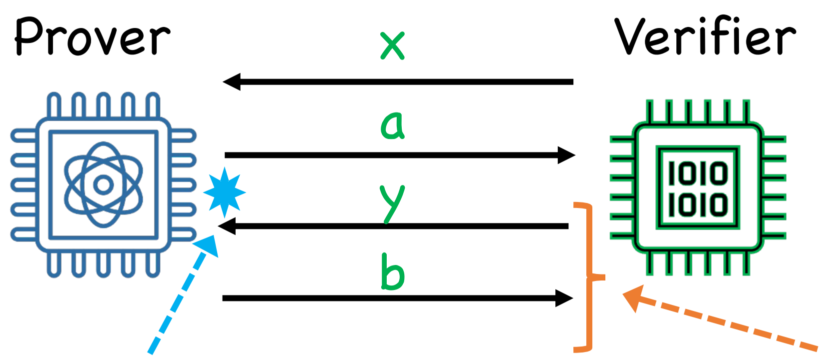
An information-theoretic toy model



States $\rho_x = \sum_a \rho_{x,a}$ on a C*-algebra $\mathcal{B}$

POVMs $\{B_{y,b}\}$ in $\mathcal{B}$

An information-theoretic toy model

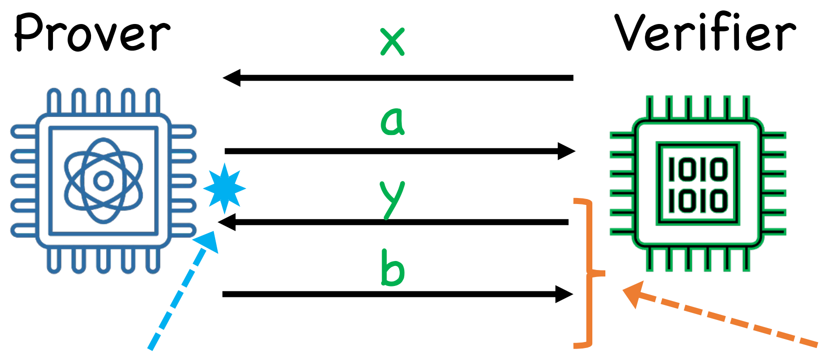


States $\rho_x = \sum_a \rho_{x,a}$ on a C*-algebra $\mathcal{B}$

POVMs $\{B_{y,b}\}$ in $\mathcal{B}$

Assume $\rho_x = \rho_{x'}$ are all the same. We call this **"strong non-signaling"** because it is equivalent to non-signaling for *any* POVM.

1st Ingredient: Timelike characterization of spacelike correlations



States $\rho_x = \sum_a \rho_{x,a}$ on a C*-algebra $\mathcal{B}$

POVMs $\{B_{y,b}\}$ in $\mathcal{B}$

Assume $\rho_x = \rho_{x'}$ are all the same. We call this **"strong non-signaling"** because it is equivalent to non-signaling for *any* POVM.

Theorem: p(a,b|x,y) = $\rho_{x,a}(B_{y,b})$ is **quantum commuting op. correlation.**

In type I, an older result by [Navascues et al] shows that condition implies quantum $\otimes$ correlations. For us this unfortunately does not apply...

Connecting computational and information-theoretic security

$\lim_{\lambda \to \infty}$

Challenge: Intuitively, in compiled game have "strong non-signaling" for poly-time observables – but these don't form an algebra.

Moreover, $\rho_{x,a}^{\lambda}$ & $B_{y,b}^{\lambda}$ live on different (larger and larger) Hilbert spaces…

Connecting computational and information-theoretic security

$\lim_{\lambda \to \infty}$

Challenge: Intuitively, in compiled game have "strong non-signaling" for poly-time observables – but these don't form an algebra.

Moreover, $\rho_{x,a}^{\lambda}$ & $B_{y,b}^{\lambda}$ live on different (larger and larger) Hilbert spaces...

Solution: Work with $\mathcal{B}$ = universal POVM algebra. This is an infinite dimensional C^*-algebra, but independent of security parameter!

Then we can define a sequence of states on the same algebra:

$$\varphi_{x,a}^{\lambda}\left(B_{y_1 b_1} B_{y_2 b_2} \ldots\right) := tr(\rho_{x,a}^{\lambda}\, B_{y_1 b_1}^{\lambda} B_{y_1 b_1}^{\lambda} \ \ldots)$$

2^{nd} Ingredient: Computational cryptography at infinite key length

$\lim_{\lambda\to\infty}$

Challenge: Intuitively, in compiled game have "strong non-signaling" for poly-time observables – but these don't form an algebra.

Moreover, $\rho_{x,a}^{\lambda}$ & $\mathrm{B}_{y,b}^{\lambda}$ live on different (larger and larger) Hilbert spaces...

Solution: Work with $\mathcal{B}$ = universal POVM algebra. This is an infinite dimensional C^*-algebra, but independent of security parameter!

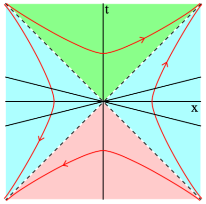
Then we can define a sequence of states on the same algebra:

$$\varphi_{x,a}^{\lambda}(B_{y_1 b_1} B_{y_2 b_2} \dots) := tr(\rho_{x,a}^{\lambda}\, \mathrm{B}_{y_1 b_1}^{\lambda} \mathrm{B}_{y_1 b_1}^{\lambda}\ \dots)$$

Theorem: For any quantum prover for the compiled game, limiting strategies at $\lambda = \infty$ exist and are strongly non-signaling! ☺

Proof uses quantum algorithmic techniques such as block encodings.

Open problems and speculations

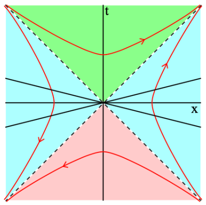


$\omega_q \leq \omega_{q,\text{compiled}} \leq \omega_{qc}$. What is the right answer?

Both plausible! Surprisingly, *not* absurd to approximate commuting operator correlations by finite-dim. objects…

cf. [Ozawa, Coudron-Vidick]

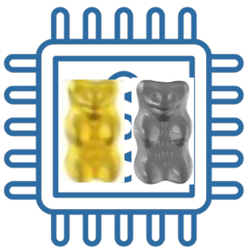
Open problems and speculations



$\omega_q \leq \omega_{q,\text{compiled}} \leq \omega_{qc}$. What is the right answer?

Both plausible! Surprisingly, *not* absurd to approximate commuting operator correlations by finite-dim. objects…

cf. [Ozawa, Coudron-Vidick]

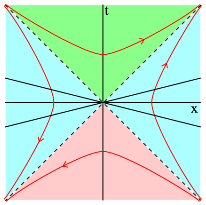


Rigidity inside the encrypted ("Alice") part of prover?

$$\lim_{\lambda \to \infty}$$

Other situations in which one can connect computational and information-theoretic security?

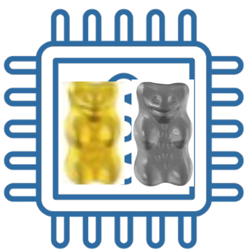
Open problems and speculations



$\omega_q \leq \omega_{q,\text{compiled}} \leq \omega_{qc}$. What is the right answer?

Both plausible! Surprisingly, *not* absurd to approximate commuting operator correlations by finite-dim. objects…

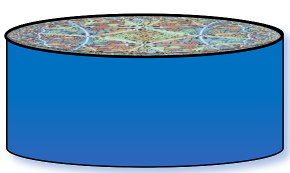
cf. [Ozawa, Coudron-Vidick]



Rigidity inside the encrypted ("Alice") part of prover?

$\lim_{\lambda \to \infty}$

Other situations in which one can connect computational and information-theoretic security?

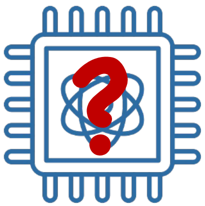


These results show rigorously how spacelike correlations can emerge from perspective of poly-time "observers". Anything to learn for quantum gravity?

Cf. works connecting complexity, pseudo-randomness, holography [Susskind-Maldacena, May, Bouland et al, …]

Summary

Nonlocal games are a foundational tool in quantum information and complexity.



Recent results establish links between the traditional space-like (information theoretic) and a time-like (computational) setting.

This gives new protocols to verify quantum advantage, computations, etc. It may also offer new insights into how locality can emerge in low-complexity effective theories.

Thank you for your attention!