Compiled Nonlocal Games

Sum of Squares Optimization Meets Cryptography?

Anand Natarajan & Tina Zhang

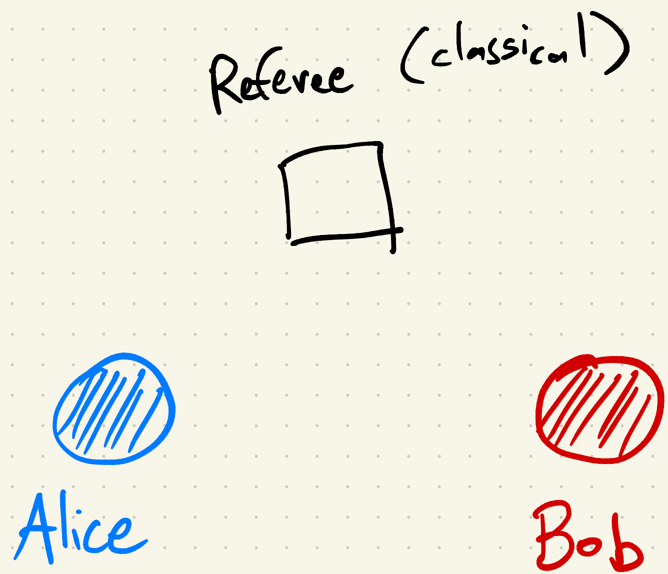
arXiv:2303.01545

Nonlocal Games

Invented by John Bell to test quantum mechanics

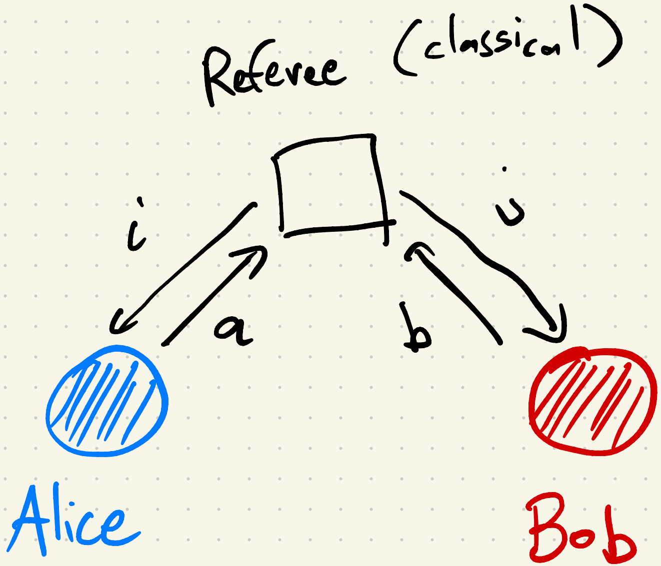
Nonlocal Games

Invented by John Bell to test quantum mechanics



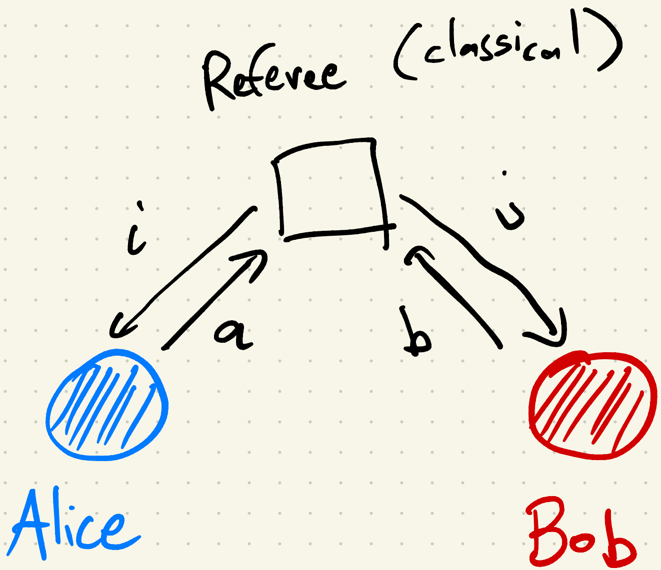
Nonlocal Games

Invented by John Bell to test quantum mechanics



Nonlocal Games

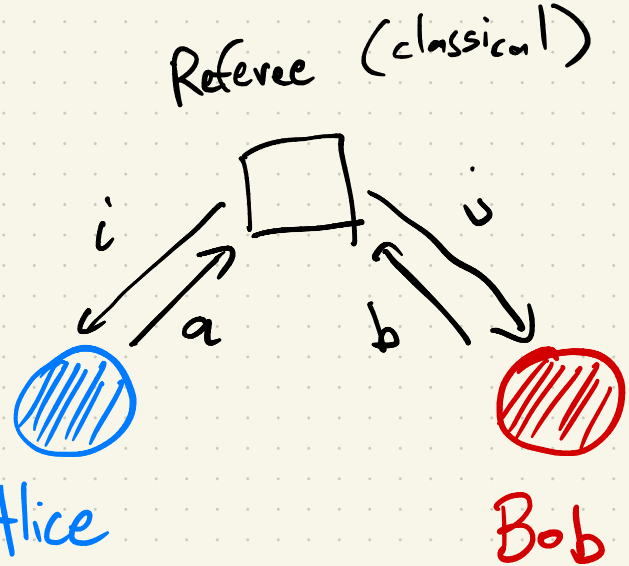
Invented by John Bell to test quantum mechanics



$$P_{win} = \Pr_{\substack{i,j \\ a \sim i \\ b \sim j}} \left[\text{Answers } a,b \text{ are "correct" for questions } i,j \right]$$

Nonlocal Games

Invented by John Bell to test quantum mechanics

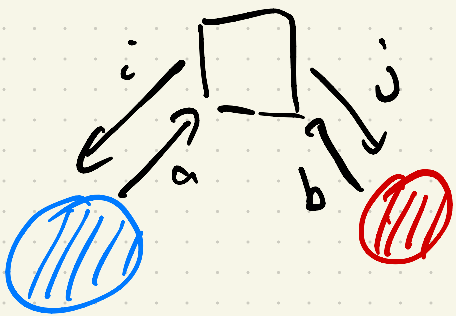


$$P_{win} = \Pr_{\substack{i,j \\ a \sim i \\ b \sim j}} \left[\text{Answers } a, b \text{ are "correct" for questions } i, j \right]$$

In general

$$P^{classical}_{win} \leq P^{quantum}_{win}$$

The CHSH Game



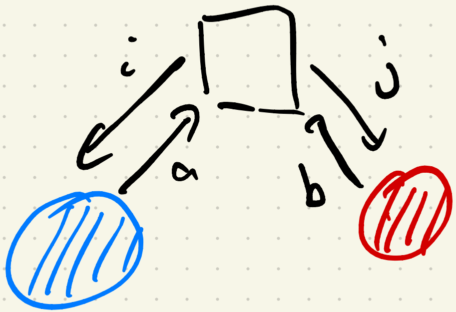
$i, j \in \{0, 1\}$

$a, b \in \{\pm 1\}$

Win if $ab = (-1)^{s_{ij}}$

i	j	$ab \stackrel{?}{=}$	s_{ij}
0	0	+1	0
0	1	+1	0
1	0	+1	0
1	1	−1	1

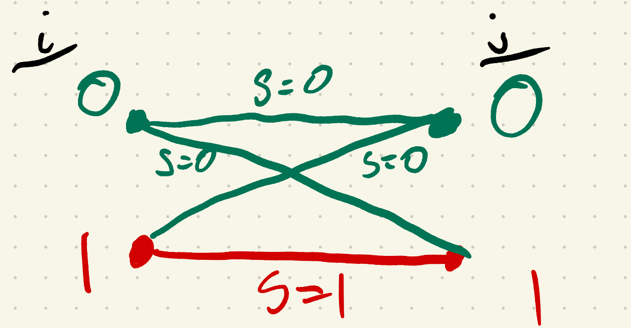
The CHSH Game



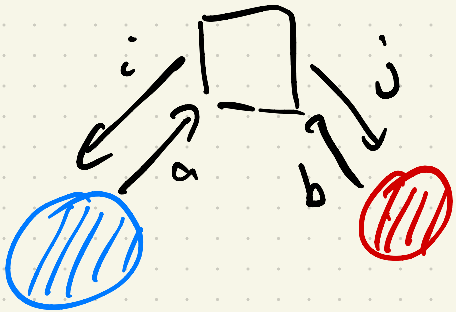
$i, j \in \{0, 1\}$

$a, b \in \{\pm 1\}$

Win if $ab = (-1)^{s_{ij}}$



The CHSH Game

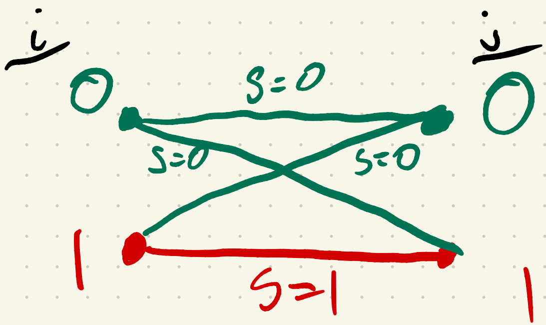


$$p_{win} = \frac{1}{2} + \frac{1}{2}\beta$$

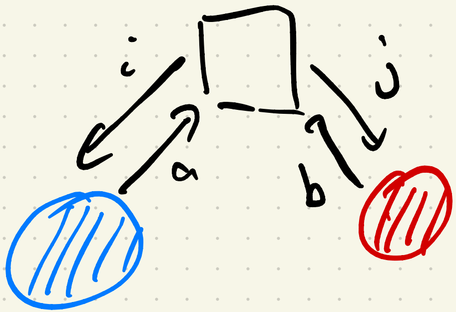
$$\beta^{\text{classical}} = \max \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} a_i b_j$$

$$\text{s.t.} \quad \forall i \quad a_i^2 = I$$

$$\forall j \quad b_j^2 = I$$



The CHSH Game

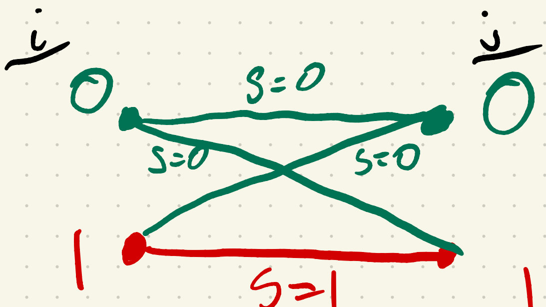


$$P_{win} = \frac{1}{2} + \frac{1}{2}\beta$$

$$\beta^{classical} = \max \mathbb{E}_{ij} (-1)^{s_{ij}} a_i b_j$$

s.t. $\forall i \quad a_i^2 = 1$

$\forall j \quad b_j^2 = 1$



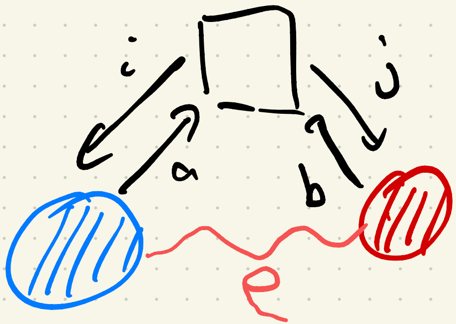
$$\beta^{classical} = \frac{1}{2}$$

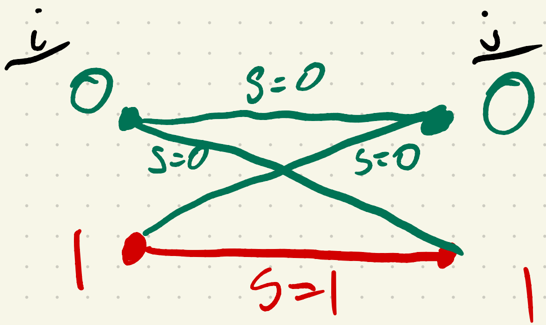
Set $a_0 = a_1 = 1$

$b_0 = b_1 = 1$

$\Rightarrow P_{win}^{classical} = 3/4$

The CHSH Game





$$p_{win} = \frac{1}{2} + \frac{1}{2}\beta$$

matrices!

quantum

$$\beta = \max_{A_i, B_j, \rho} \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} \mathrm{tr}[A_i B_j \rho]$$

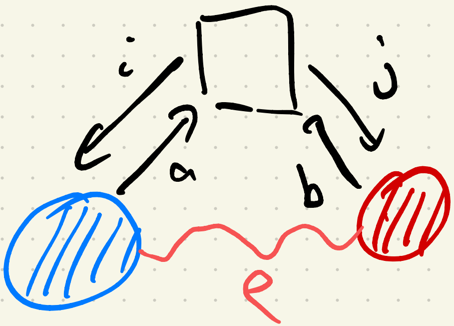
s.t. $\rho \succeq 0$, $\mathrm{tr}\,\rho = 1$

$\forall i,\ A_i^2 = I$

$\forall j\ \ B_j^2 = I$

$\forall i,j\ \ A_i B_j = B_j A_i$

The CHSH Game



$$p_{win} = \frac{1}{2} + \frac{1}{2}\beta$$

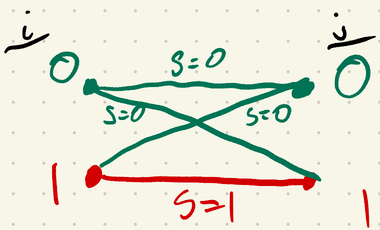
$$\beta^{quantum} = \max_{A_i, B_j, \rho} \mathbb{E}_{ij} (-1)^{s_{ij}} \operatorname{tr}[A_i B_j \rho]$$

s.t. $\rho \succeq 0$, $\operatorname{tr}\rho = 1$

$\forall i, \; A_i^2 = I$

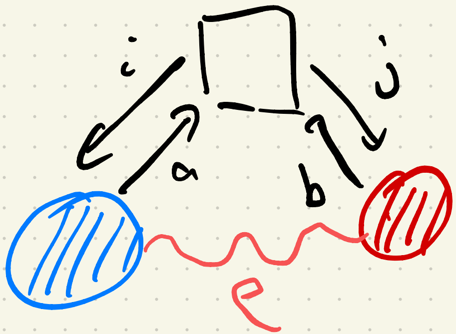
$\forall j \;\; B_j^2 = I$

$\forall i,j \;\; A_i B_j = B_j A_i$



$$\beta^{quantum} = \frac{1}{2} \cdot \sqrt{2} > \beta^{classical}$$

The CHSH Game



$$p_{win} = \frac{1}{2} + \frac{1}{2}\beta$$

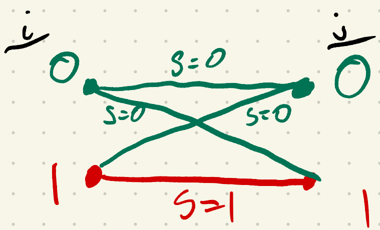
$$\beta^{\text{quantum}} = \max_{A_i, B_j, \rho} \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} \operatorname{tr}[A_i B_j \rho]$$

s.t. $\rho \succeq 0$, $\operatorname{tr}\rho = 1$

$\forall i,\ A_i^2 = I$

$\forall j\ \ B_j^2 = I$

$\forall i,j\ \ A_i B_j = B_j A_i$



$$\beta^{\text{quantum}} = \frac{1}{2} \cdot \sqrt{2}$$

$$p_{win}^{\text{quantum}} \approx 0.85 > \frac{3}{4}$$

The CHSH Game

- $P^{\text{quantum}}_{\text{win}} > P^{\text{classical}}_{\text{win}}$ demonstrated in lab [2022 Nobel Prize!]

- Q. optimizer is "rigid"

$$\beta^Q(A, B) \approx \tfrac{1}{2}\sqrt{2} \Rightarrow \underbrace{\begin{matrix} A_0 A_1 \approx -A_1 A_0 \\ B_0 B_1 \approx -B_1 B_0 \end{matrix}}$$

Anticommutation ⇒ "complementary measurements" in physics

The CHSH Game

- Q. optimizer is "rigid"

$$\beta^Q(A, B) \approx \tfrac{1}{2}\sqrt{2} \Rightarrow \underbrace{\begin{array}{l} A_0A_1 \approx -A_1A_0 \\ B_0B_1 \approx -B_1B_0 \end{array}}$$

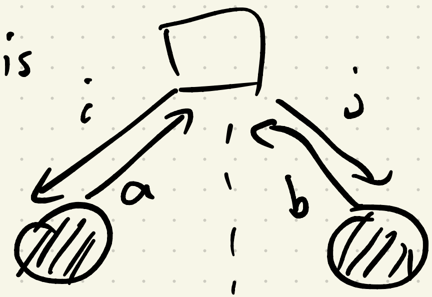
Anticommutation $\Rightarrow$ "complementary measurements" in physics

$\Longrightarrow$ Using CHSH, can build protocols to test quantum computers "gate by gate" [RUV'13]

Drawbacks of nonlocal games

Drawbacks of nonlocal games

- Non-communication between players is <u>essential</u>

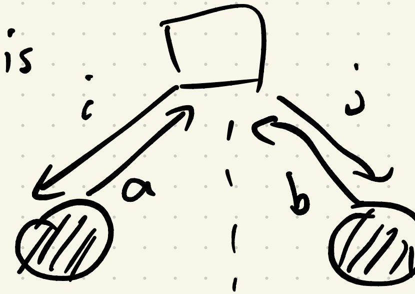


a must only depend on i

b must only depend on j

Drawbacks of nonlocal games

- Non-communication between players is essential



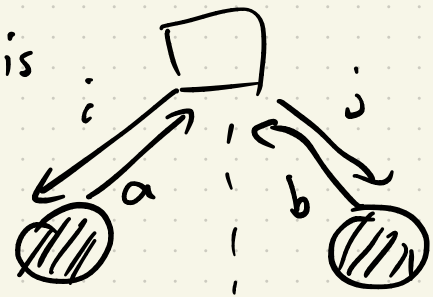
a must only depend on i

b must only depend on j

Quantum: A_i and B_j must be commuting matrices

Drawbacks of nonlocal games

- Non-communication between players is essential



a must only depend on i

b must only depend on j

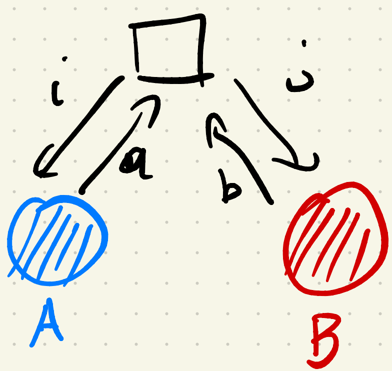
Quantum: A_i and B_j must be commuting matrices

Experimentally very difficult to realize!

Cryptographic compilers

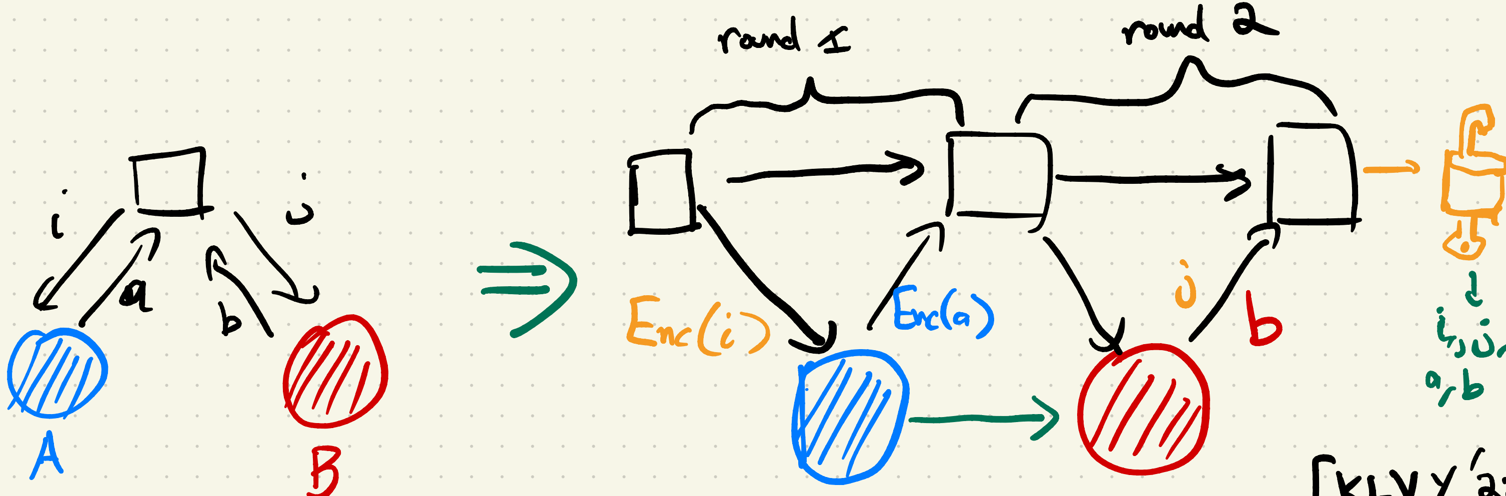
- **Idea:** Use cryptography so one player can "simulate" 2 separated players

[Long history in crypto, e.g. Kilian '92, BMW'98, KRR'14, ...]



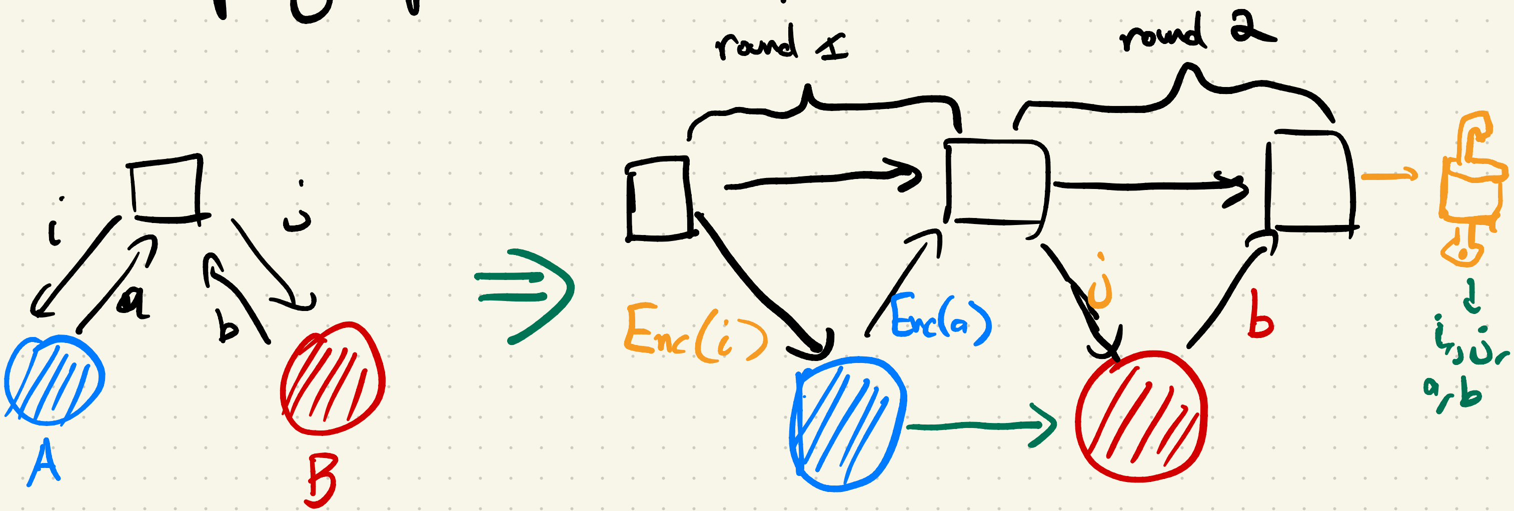
Cryptographic compilers

- **Idea:** Use cryptography so one player can "simulate" 2 separated players



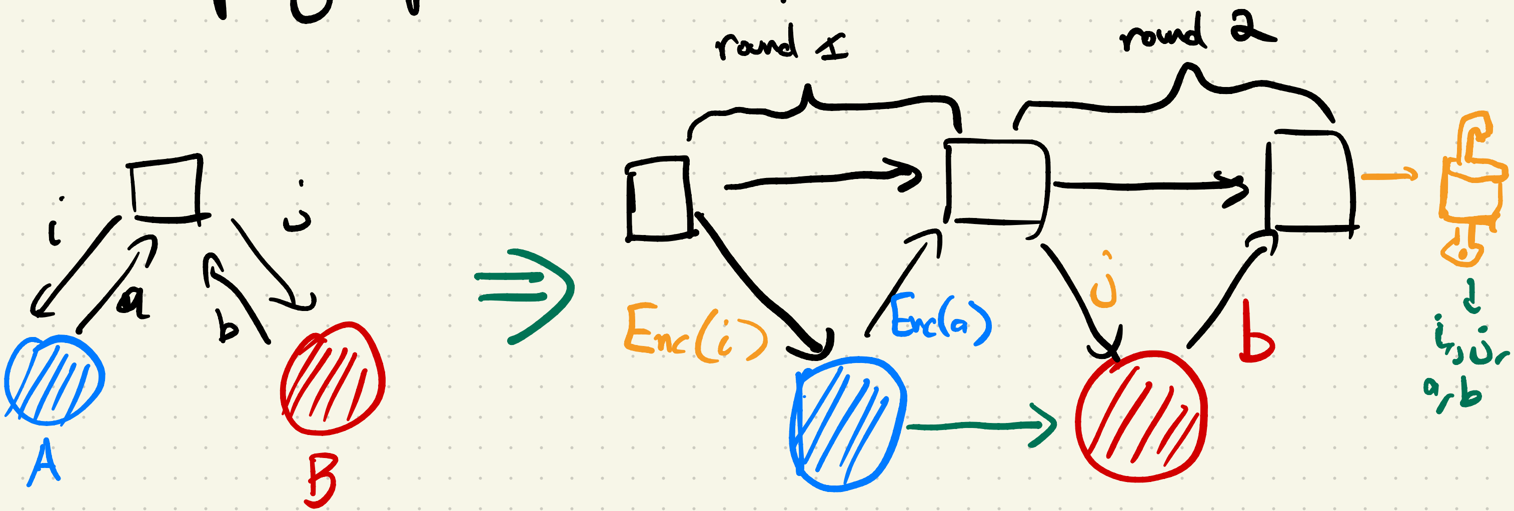
[KLVY'22]

Cryptographic compilers



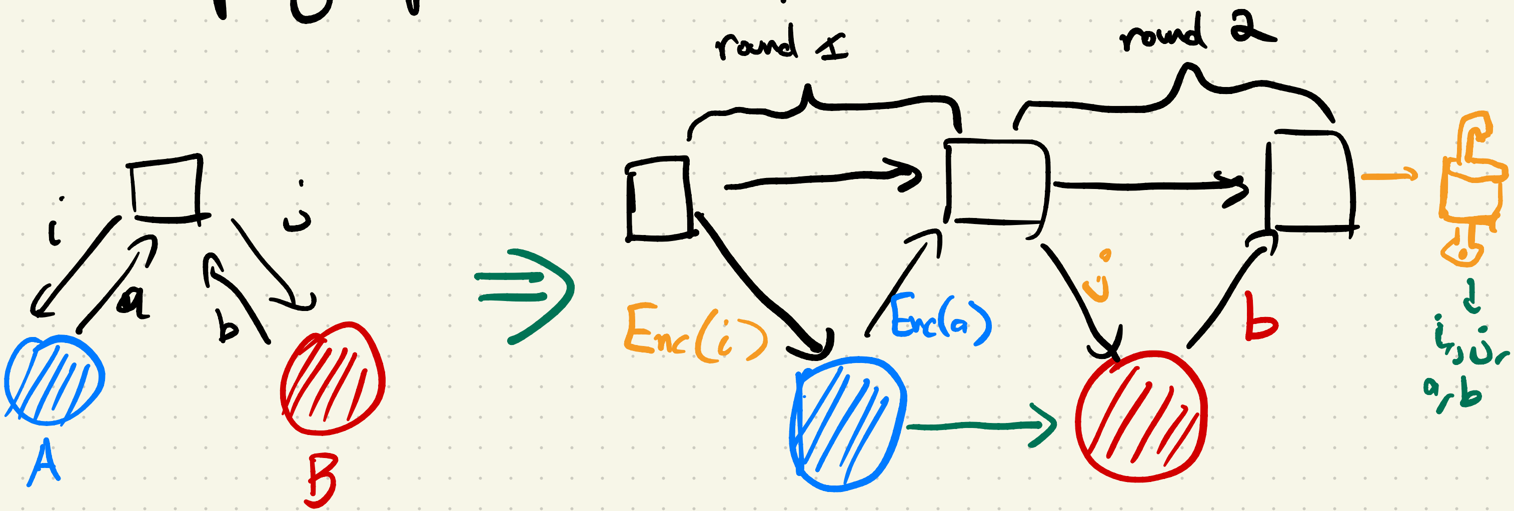
[KLVY'22]: $P_{win}^{\text{classical, compiled}} \leq P_{win}^{\text{classical nonlocal}} + \text{negl.}$

Cryptographic compilers



[KLVY'22]: $P_{\text{win}}^{\text{quantum compiled}} \overset{???}{\leq} P_{\text{win}}^{\text{quantum nonlocal}} + \text{negl.}$???

Cryptographic compilers: CHSH



	classical	quantum
nonlocal	$3/4$	0.85 $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)$
compiled	$3/4$ + neg!	????

(is it even < 1?)

Our results

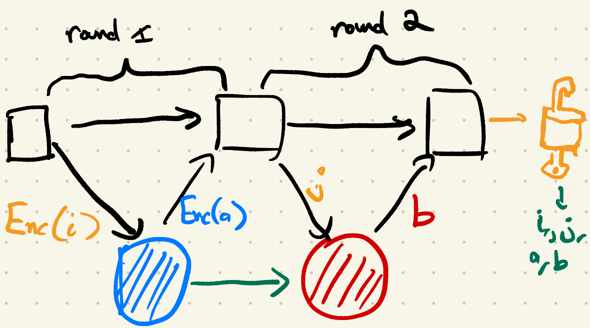
	classical	quantum
nonlocal	$3/4$	0.85 $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)$
compiled	$3/4$ + neg!	0.85 + neg ! $\left(\frac{1}{2}+\frac{\sqrt{2}}{4} + \text{neg}!\right)$

Our results: rigidity

	classical	quantum
nonlocal	3/4	0.85 $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)$
compiled	3/4 + negl	0.85 + negl $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}+\text{negl}\right)$

→ Any strategy that is near optimal must have

$$B_0 B_1 \approx -B_1 B_0$$

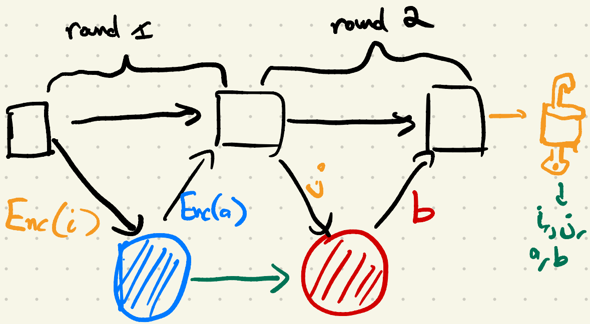


Our results: delegation

	classical	quantum
nonlocal	$3/4$	0.85 $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)$
compiled	$3/4 + \text{negl}$	$0.85 + \text{negl}$ $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}+\text{negl}\right)$

$\rightarrow$ A delegation scheme for poly time quantum computation w/ classical client

(assuming quantum fully homomorphic encryption $\Leftarrow$ LWE [Mahadev'17])



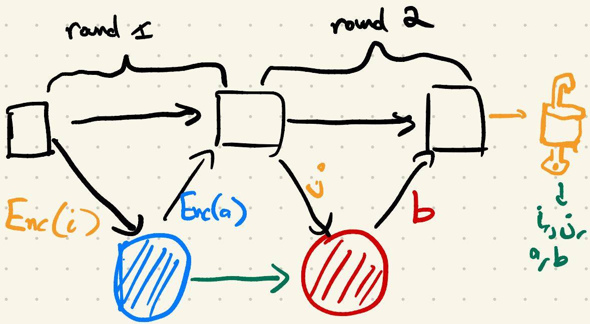
Our results: delegation

	classical	quantum
nonlocal	3/4	0.85 $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)$
compiled	3/4 + negl	0.85 + negl $\left(\frac{1}{2}+\frac{\sqrt{2}}{4}+\text{negl}\right)$

→ A delegation scheme for poly time quantum computation w/ classical client

(assuming quantum fully homomorphic encryption $\Leftarrow$ LWE [Mahadev '17])

Matches [Mahadev '18] by new techniques



Techniques: outline

1) Prove $\beta^Q \leq \frac{1}{2} \cdot \sqrt{2}$ in nonlocal world using noncommutative Sum-of-Squares

2) Modify this proof to show

$$\beta^Q_{\text{compiled}} \leq \frac{1}{2} \cdot \sqrt{2} + \text{negl.}$$

SoS for β^Q

$$\beta^Q = \max \ \mathrm{tr}\Big[\overbrace{\mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i B_j}^{\hat{G}(A_0, A_1, B_0, B_1)} \ \rho \Big]$$

s.t. $\quad A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i$

$\rho \succeq 0, \quad \mathrm{tr}\,\rho = 1$

SoS for β^Q

$$\beta^Q = \max \operatorname{tr}\Big[\overbrace{\mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i B_j}^{\hat{G}(A_0, A_1, B_0, B_1)} \rho\Big]$$

$$\text{s.t.} \quad A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i \quad (*)$$

$$\rho \succeq 0, \quad \operatorname{tr}\rho = 1$$

To show $\beta^Q \leq \frac{1}{2} \cdot \sqrt{2}$, suffices to show

$$\frac{1}{2}\sqrt{2} - \hat{G} \succeq 0 \quad \text{whenever } (*) \text{ holds}$$

SoS for β^Q

To show $\beta^Q \leq \frac{1}{2}\cdot\sqrt{2}$

suffices to show

$\frac{1}{2}\sqrt{2} - \hat{G} \geq 0 \quad \Leftarrow (*)$

$\Uparrow$

$$\beta^Q = \max \operatorname{tr}\Big[\overbrace{\mathbb{E}_{i,j}(-1)^{s_{ij}} A_i B_j}^{\hat{G}(A_0, A_1, B_0, B_1)} \rho\Big]$$

s.t. $A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i \quad (*)$

$\rho \geq 0, \quad \operatorname{tr}\rho = 1$

$$\frac{1}{2}\cdot\sqrt{2} - \hat{G}(A, B) = \underbrace{\sum_k p_k(A,B)^\dagger p_k(A,B)}_{\text{Sum of squares (must be } \geq 0)} \mod (*)$$

SoS for β^Q

To show $\beta^Q \le \frac{1}{2}\cdot\sqrt{2}$

suffices to show

$$\beta^Q = \max \operatorname{tr}\Big[\overbrace{\mathbb{E}_{i,j}(-1)^{s_{ij}} A_i \, B_j}^{\hat{G}(A_0,A_1,B_0,B_1)} \; \rho\Big]$$

s.t. $A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i \quad (*)$

$\rho \geq 0, \quad \operatorname{tr}\rho = 1$

$$\frac{1}{2}\cdot\sqrt{2} - \hat{G}(A, B) = \sum_k P_k(A,B)^\dagger P_k(A,B) \mod (*)$$

Take $P_1 \propto \left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)$

$P_2 \propto \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)$

SoS for β^Q

$$\beta^Q = \max \operatorname{tr}\Big[\overbrace{\mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i B_j}^{\hat{G}(A_0,A_1,B_0,B_1)} \rho\Big]$$

s.t. $A_i^2 = B_j^2 = I, \quad A_i B_j = B_j A_i \quad (*)$

$\rho \succeq 0, \quad \operatorname{tr}\rho = 1$

To show $\beta^Q \le \frac{1}{2}\cdot\sqrt{2}$

suffices to show

$$\frac{1}{2}\cdot\sqrt{2} - \hat{G}(A, B) = \sum_k p_k(A,B)^\dagger p_k(A,B) \mod (*)$$

Take $p_1 \propto \left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)$

$p_2 \propto \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)$

$\Rightarrow$ rigidity (near optimal strategies have $p_k \approx 0$)

SoS for $\beta^{Q}_{\text{compiled}}$

$$\beta^{Q}_{\text{compiled}} = \max \operatorname{tr}\left[\sum_a \mathbb{E}_{ij} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)} \rho \right]$$

s.t.

$$\forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$$

$$\forall j \qquad B_j^2 = I$$

$$\rho \succeq 0, \quad \operatorname{tr} \rho = 1$$

SoS for $\beta^{Q}_{\text{compiled}}$

sequential quantum measurement

$$\beta^{Q}_{\text{compiled}} = \max \operatorname{tr}\left[\sum_a \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)} \rho \right]$$

s.t.

$$\forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$$

$$\forall j \quad B_j^2 = I$$

$$\rho \geq 0, \quad \operatorname{tr}\rho = 1$$

SoS for $\beta^{Q}_{\text{compiled}}$

$$\beta^{Q}_{\text{compiled}} = \max \operatorname{tr}\left[\sum_a \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)} \rho\right]$$

s.t.

$$\forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$$

$$\forall j \qquad B_j^2 = I$$

$$\boxed{\forall\, i, i', \ \forall \text{ "efficient" } f(B) \quad \operatorname{tr}\left[\sum_a A_i^{(a)} f(B) A_i^{(a)} \rho\right] \approx_{\text{negl}} \operatorname{tr}\left[\sum_a A_{i'}^{(a)} f(B) A_{i'}^{(a)} \rho\right]}$$

$$\rho \succeq 0, \quad \operatorname{tr}\rho = 1$$

SoS for $\beta^{Q}_{compiled}$

$$\beta^{Q}_{compiled} = \max \operatorname{tr}\left[\sum_a \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)} \rho \right]$$

s.t.

$$\forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$$

$$\forall j \quad B_j^2 = I$$

$$\boxed{\forall\, i, i', \ \forall \text{ "efficient" } f(B) \quad \operatorname{tr}\left[\sum_a A_i^{(a)} f(B) A_i^{(a)} \rho \right] \approx_{negl} \operatorname{tr}\left[\sum_a A_{i'}^{(a)} f(B) A_{i'}^{(a)} \rho \right]}$$

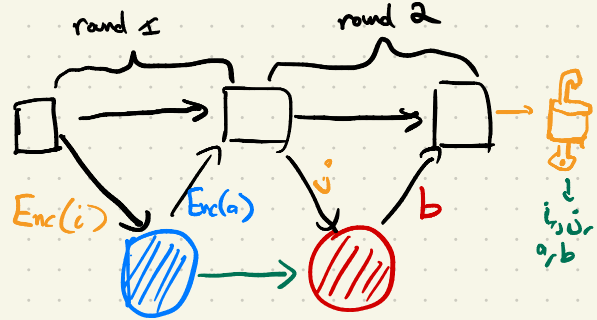
$\rho \geq 0, \ \operatorname{tr}\rho = 1$

from cryptography

replaces

$A_i B_j = B_j A_i$

SoS for $\beta^{Q}_{\text{compiled}}$



$$\beta^{Q}_{\text{compiled}} = \max \operatorname{tr}\left[\sum_a \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)} \rho \right]$$

s.t. $\quad \forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$

$\quad \forall j \quad B_j^2 = I$

"No measurement in round 2 can leak info about i (since it is encrypted)"

$\forall\, i, i', \ \forall$ "efficient" $f(B)$ $\quad \operatorname{tr}\left[\sum_a A_i^{(a)} f(B) A_i^{(a)} \rho\right] \approx_{\text{negl}} \operatorname{tr}\left[\sum_a A_{i'}^{(a)} f(B) A_{i'}^{(a)} \rho\right]$

$\rho \geq 0, \quad \operatorname{tr} \rho = 1$

SoS for $\beta^{Q}_{\text{compiled}}$

$$\beta^{Q}_{\text{compiled}} = \max \operatorname{tr}\Big[\overbrace{\sum_a \mathbb{E}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)}}^{\mathcal{G}_{\text{compiled}}} \rho \Big]$$

s.t.

$$\forall i, \quad \sum_a A_i^{(a)\dagger} A_i^{(a)} = I$$

$$\forall j \quad B_j^2 = I$$

$$\forall i, i', \ \forall \text{ "efficient" } f(B) \quad \operatorname{tr}\Big[\sum_a A_i^{(a)} f(B) A_i^{(a)} \rho\Big] \approx_{negl} \operatorname{tr}\Big[\sum_a A_{i'}^{(a)} f(B) A_{i'}^{(a)} \rho\Big]$$

$$\rho \geq 0, \quad \operatorname{tr} \rho = 1$$

$(**)$

Can we show

$$\frac{1}{2}\cdot\sqrt{2} - \mathcal{G}_{\text{compiled}} = \sum p^\dagger p$$

mod $(**)$?

SoS for $\beta^{Q}_{compiled}$

$$\beta^{Q}_{compiled} = \max \operatorname{tr}\Big[\overbrace{\sum_a \mathop{\mathbb{E}}_{i,j} (-1)^{s_{ij}} A_i^{(a)} B_j A_i^{(a)}}^{\hat{\mathcal{G}}_{compiled}} \rho\Big]$$

s.t.

$$\left.\begin{array}{l} \forall i, \ \sum_a A_i^{(a)\dagger} A_i^{(a)} = I \\ \forall j \quad B_j^2 = I \\ \forall i, i', \ \forall \text{ "efficient" } f(B) \quad \operatorname{tr}\Big[\sum_a A_i^{(a)} f(B) A_i^{(a)} \rho\Big] \approx_{negl} \\ \qquad \operatorname{tr}\Big[\sum_a A_{i'}^{(a)} f(B) A_{i'}^{(a)} \rho\Big] \end{array}\right\} (**)$$

$\rho \geq 0, \ \operatorname{tr}\rho = 1$

We show

$$\operatorname{tr}\Big[\Big(\tfrac{1}{2}\cdot\sqrt{2} - \hat{\mathcal{G}}_{compiled}\Big)\rho\Big] = \operatorname{tr}\Big[\sum p^\dagger p \, \rho\Big]$$

mod $(**)$

which is sufficient!

Open questions

- What about other games?

  When is $p_{win}^{Q,\,compiled} \leq p_{win}^{Q} + \text{negl}$?

Open questions

- What about other games?

  When is $p_{win}^{Q,\text{compiled}} \le p_{win}^{Q} + \text{negl}$?

- Our SoS manipulations are very specific to CHSH
  - can we "lift" all simple SoS proofs (e.g. degree-2 proofs)?

Open questions

- What about other games?

  When is $p_{win}^{Q,\text{compiled}} \leq p_{win}^{Q} + \text{negl}$?

  - Our SoS manipulations are very specific to CHSH
    - can we "lift" all simple SoS proofs (e.g. degree-2 proofs)?

- Can the cryptographic requirements be relaxed? (Less than full QFHE?)

Open questions

- Does quantum crypto give rise to interesting new <u>non-commutative</u> polynomial optimization problems?

Thank you!

arXiv: 2303.01545