Compiled Nonlocal Games from any Trapdoor Claw-Free Function

Kaniuar Bacho[1,2], Alexander Kulpe[1], Giulio Malavolta[3], Simon Schmidt[1], Michael Walter[1]

[1]Ruhr University Bochum

[2]University of Edinburgh

[3]Bocconi University

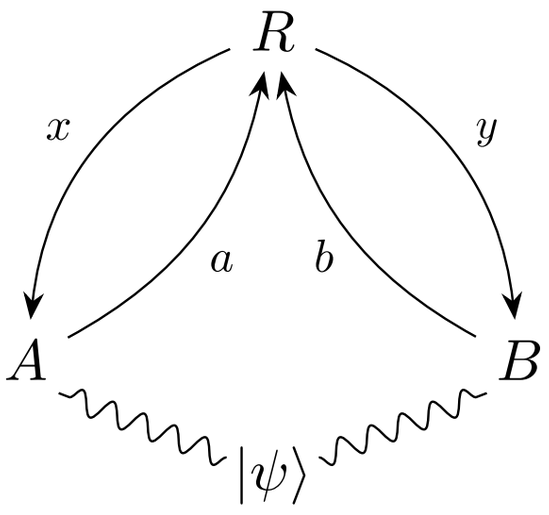
RUHR UNIVERSITÄT BOCHUM

RUB

THE UNIVERSITY of EDINBURGH

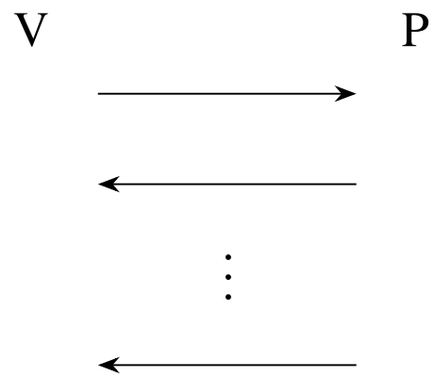
Bocconi

Nonlocal Game



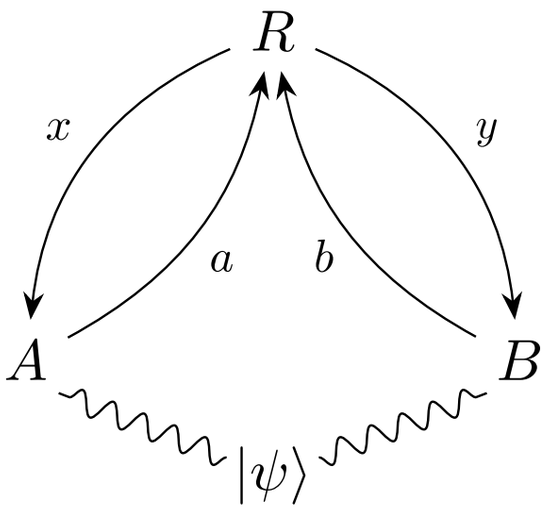
Compiler

Compiled Nonlocal Game



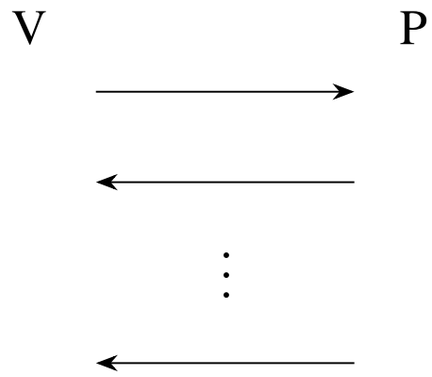
Compiler should preserve properties of the nonlocal game

Nonlocal Game

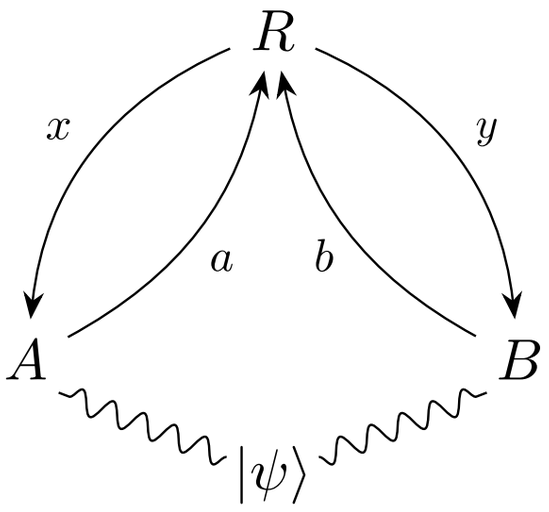


Compiler

Compiled Nonlocal Game

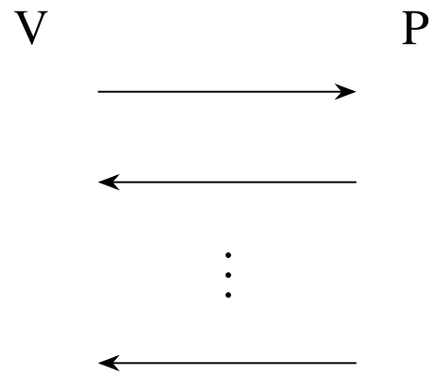


Nonlocal Game



Compiler

Compiled Nonlocal Game

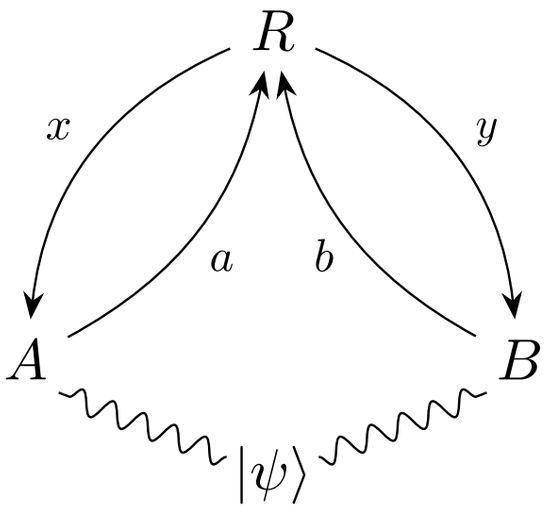


<u>CHSH Game</u> (Clauser–Horne–Shimony–Holt)

- Questions & answers: $x, y, a, b \in \{0,1\}$
- No communication between A and B
- Winning condition: $a \oplus b = x \cdot y$

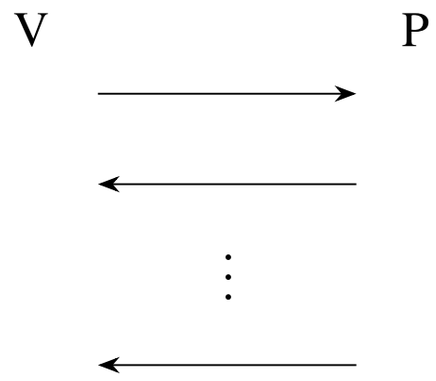
x	y	winning condition
0	0	$a = b$
0	1	$a = b$
1	0	$a = b$
1	1	$a \neq b$

Nonlocal Game



Compiler

Compiled Nonlocal Game



<u>CHSH Game</u> (Clauser–Horne–Shimony–Holt)

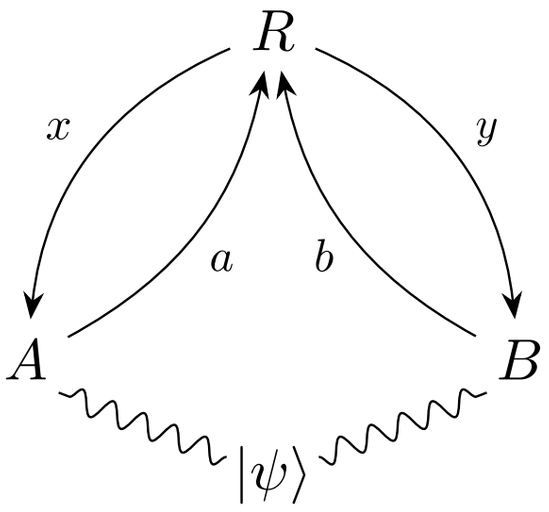
- Questions & answers: $x, y, a, b \in \{0,1\}$
- No communication between A and B
- Winning condition: $a \oplus b = x \cdot y$

x	y	winning condition
0	0	$a = b$
0	1	$a = b$
1	0	$a = b$
1	1	$a \neq b$

$\omega_c(\mathcal{G}) :=$ maximal winning probability for classical players

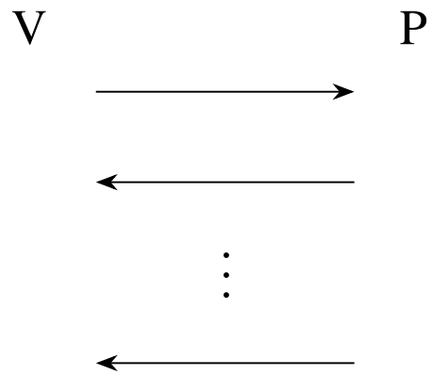
$\omega_q(\mathcal{G}) :=$ maximal winning probability for $\otimes$ quantum players

Nonlocal Game



Compiler

Compiled Nonlocal Game



CHSH Game (Clauser–Horne–Shimony–Holt)

- Questions & answers: $x, y, a, b \in \{0,1\}$
- No communication between A and B
- Winning condition: $a \oplus b = x \cdot y$

x	y	winning c
0	0	$a =$
0	1	$a =$
1	0	$a = b$
1	1	$a \neq b$

2-Prover Proof of Quantumness

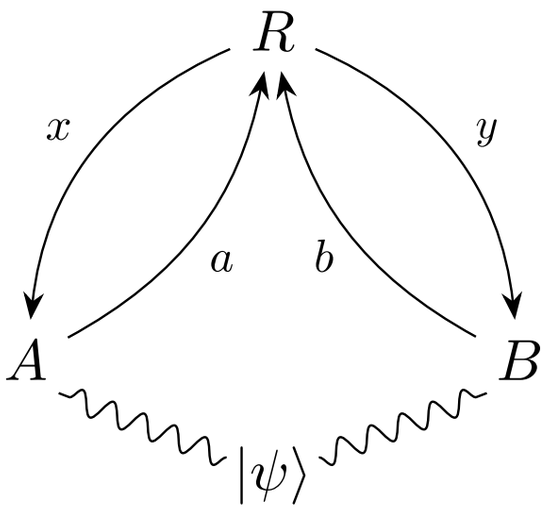
$\omega_c(\mathcal{G}) :=$ maximal winning probability for classical players

$\omega_q(\mathcal{G}) :=$ maximal winning probability for $\otimes$ quantum players

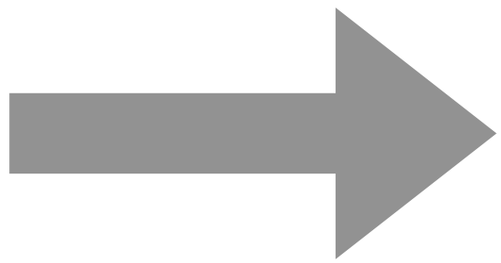
$\omega_c(\mathcal{G}_{\mathsf{CHSH}}) = 75\%$

$\omega_q(\mathcal{G}_{\mathsf{CHSH}}) = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 85\%$

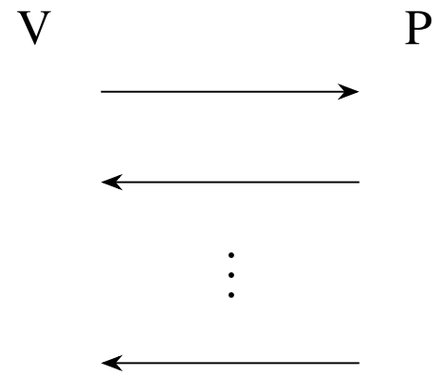
Nonlocal Game



Compiler

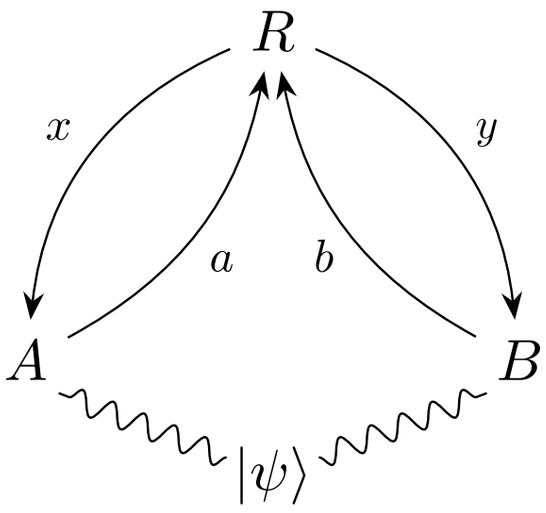


Compiled Nonlocal Game



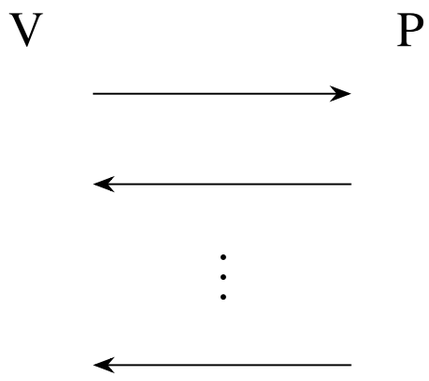
- Compiler should preserve properties of the nonlocal game

Nonlocal Game



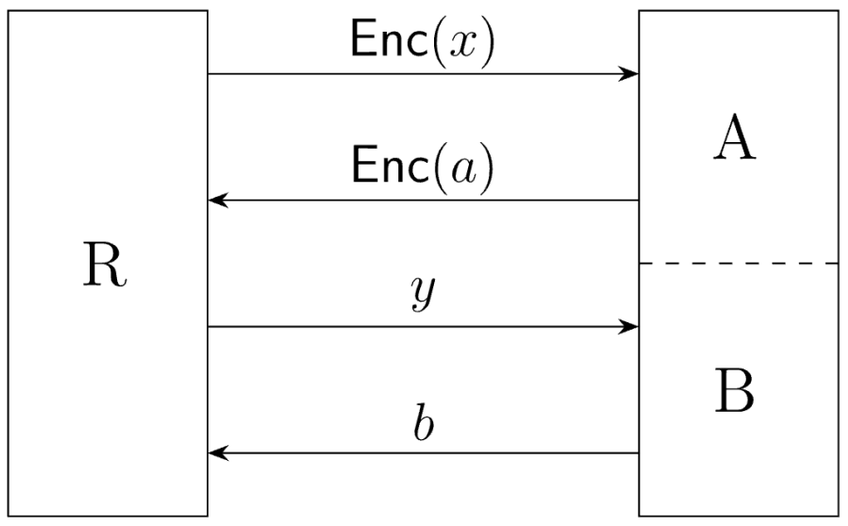
Compiler

Compiled Nonlocal Game

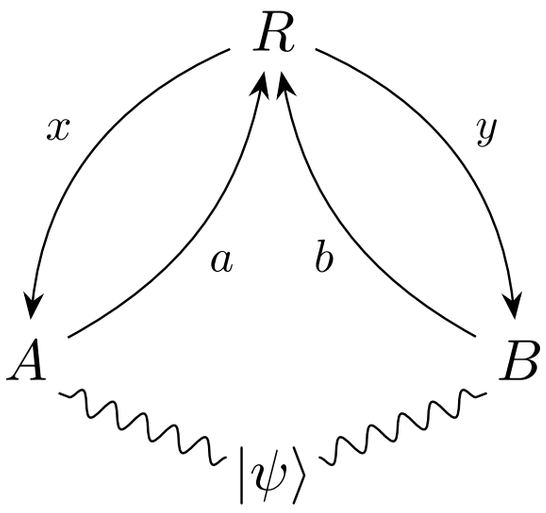


KLVY Compiler

- Kalai, Lombardi, Vaikuntanathan, and Yang [KLVY21] compiler from Quantum Fully Homomorphic Encryption

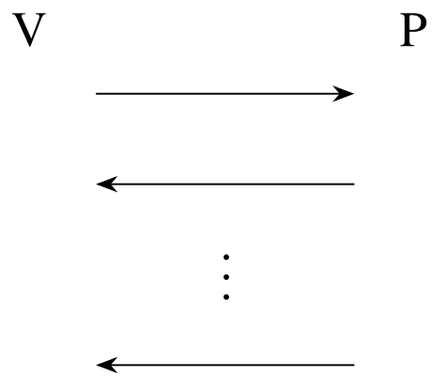


Nonlocal Game



Compiler

Compiled Nonlocal Game



KLVY Compiler

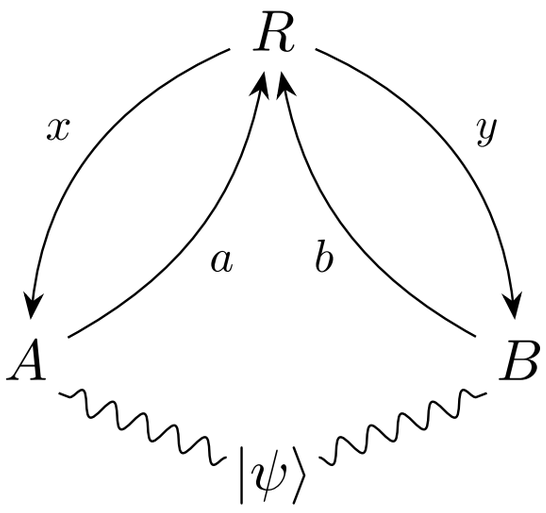
- Quantum Completeness ([KLVY23])

$$\omega_q(\mathcal{G}_{\text{comp}}) \geq \omega_q(\mathcal{G})$$

- Classical Soundness ([KLVY23])

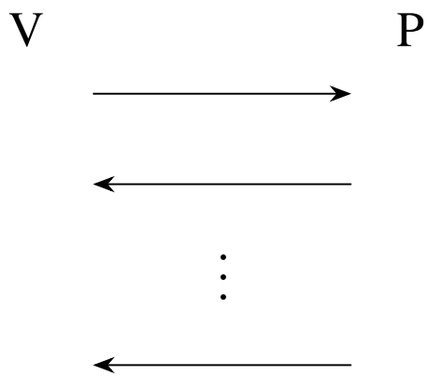
$$\omega_c(\mathcal{G}_{\text{comp}}) \leq \omega_c(\mathcal{G})$$

Nonlocal Game



Compiler

Compiled Nonlocal Game

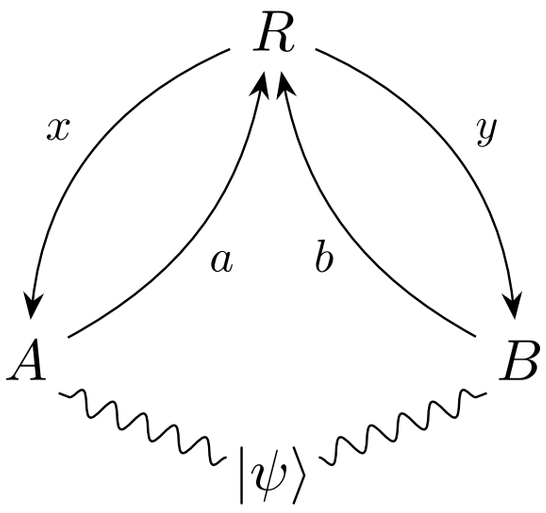


KLVY Compiler

- Quantum Completeness ([KLVY23])
- Classical Soundness ([KLVY23])

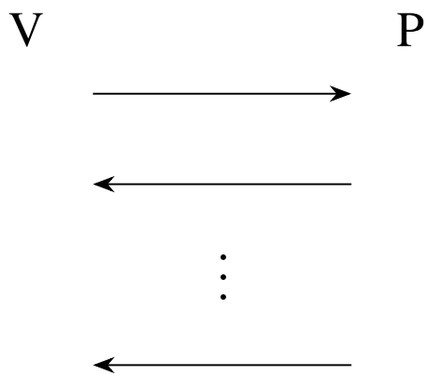
Proof of Quantumness

Nonlocal Game



Compiler

Compiled Nonlocal Game



KLVY Compiler

- Quantum Completeness ([KLVY23])

$$\omega_q(\mathcal{G}_{\mathsf{comp}}) \geq \omega_q(\mathcal{G})$$

- Classical Soundness ([KLVY23])

$$\omega_c(\mathcal{G}_{\mathsf{comp}}) \leq \omega_{qc}(\mathcal{G})$$

Proof of Quantumness

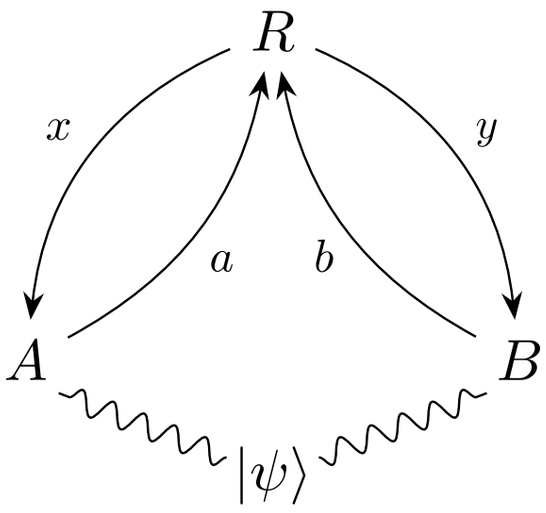
- Quantum Soundness ([NZ23, KMPSW24]):

$$\omega_q(\mathcal{G}_{\mathsf{comp}}) \leq \omega_{qc}(\mathcal{G})$$

+

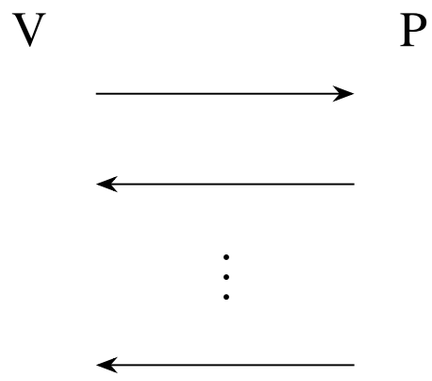
Rigidity

Nonlocal Game



Compiler

Compiled Nonlocal Game



KLVY Compiler

- Quantum Completeness ([KLVY23])
- Classical Soundness ([KLVY23])

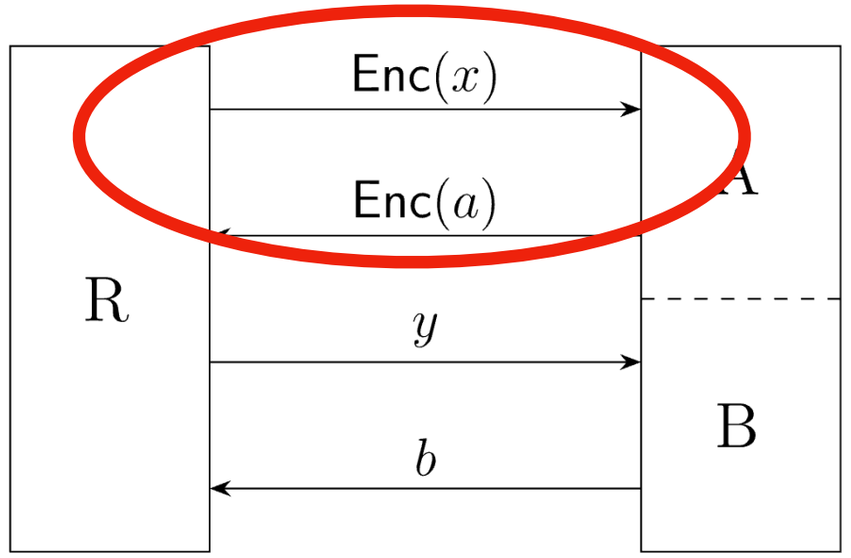
Proof of Quantumness

- Quantum Soundness ([MPSW24]):

Classical Verification of Quantum Computation

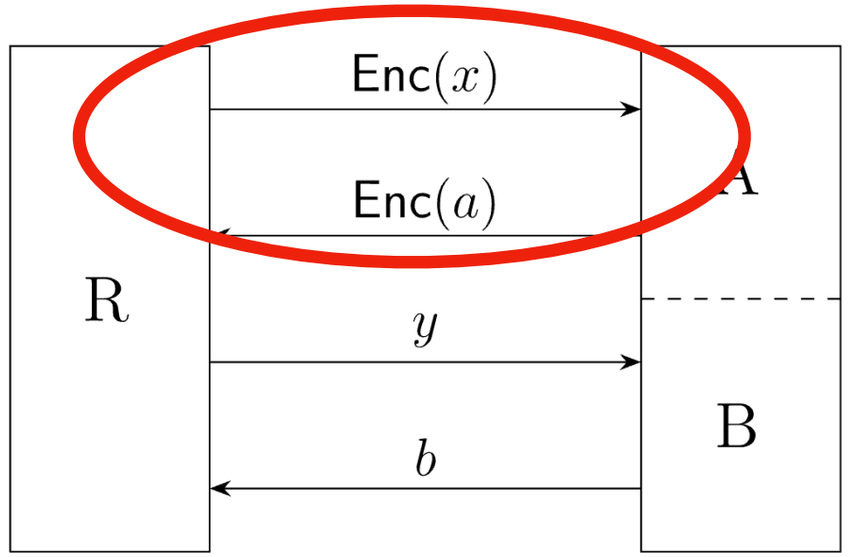
Our Compiler

- Idea 1: Replace QFHE with interactive blind classical delegation of any quantum computation



Our Compiler

- Idea 1: Replace QFHE with interactive blind classical delegation of any quantum computation



- Idea 2:

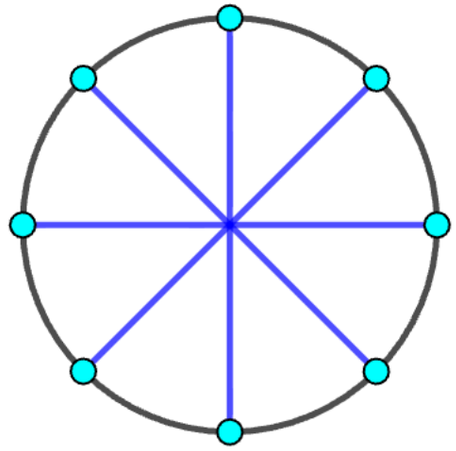
Blind classical delegation
=
Modification of universal blind quantum computation (UBQC) [BFK09]
in the measurement-based quantum computation (MBQC) model
+
Blind remote state preparation (blind RSP)

Half-Blind Quantum Computation (HBQC)

- Assumption: V can prepare single qubits in the state

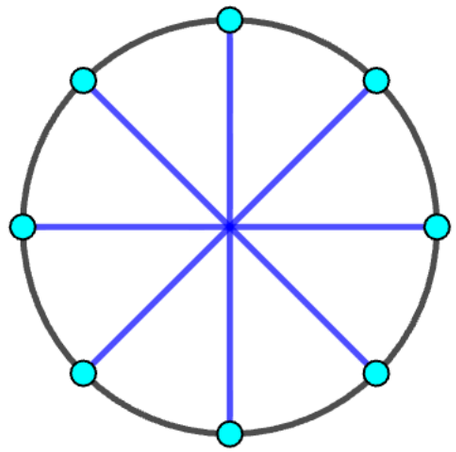
$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}\,|1\rangle),$$

where $\theta \in \Theta := \{k \cdot \pi/4 \mid k = 0, \ldots, 7\}$ is uniformly random.



(X, Y)-plane Bloch sphere

Half-Blind Quantum Computation (HBQC)



(X, Y)-plane Bloch sphere

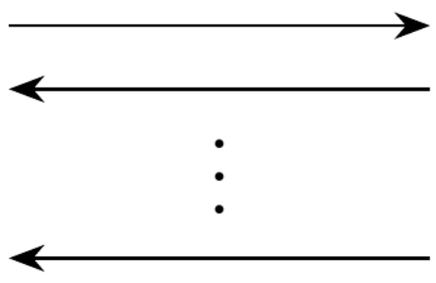
- Assumption: V can prepare single qubits in the state

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}\,|1\rangle),$$

where $\theta \in \Theta := \{k \cdot \pi/4 \mid k = 0, \ldots, 7\}$ is uniformly random.

- HBQC protocol:

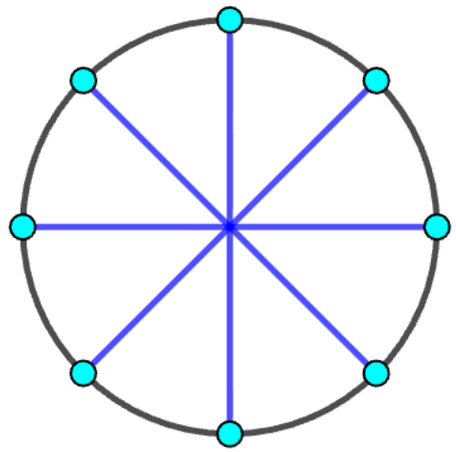
V(classical description of U) P($|\psi\rangle$)



Outputs: a_i, b_i Outputs: $(U' \otimes I)\,|\psi\rangle$

$$U' := \left(X^{a_1} Z^{b_1} \otimes \ldots \otimes X^{a_n} Z^{b_n}\right) U$$

Half-Blind Quantum Computation (HBQC)



(X, Y)-plane Bloch sphere

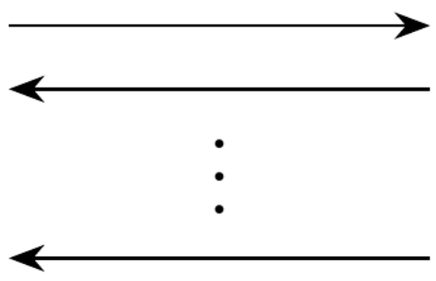
- Assumption: V can prepare single qubits in the state

$$|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}\,|1\rangle),$$

where $\theta \in \Theta := \{k \cdot \pi/4 \mid k = 0, \ldots, 7\}$ is uniformly random.

- HBQC protocol:

V(classical description of U) P($|\psi\rangle$)



Outputs: a_i, b_i Outputs: $(U' \otimes I)\,|\psi\rangle$

$$U' := \left(X^{a_1} Z^{b_1} \otimes \ldots \otimes X^{a_n} Z^{b_n}\right) U$$

- Security: Prover gains no information about U and a_i, b_i
- Security holds unconditionally (no computational assumptions!)

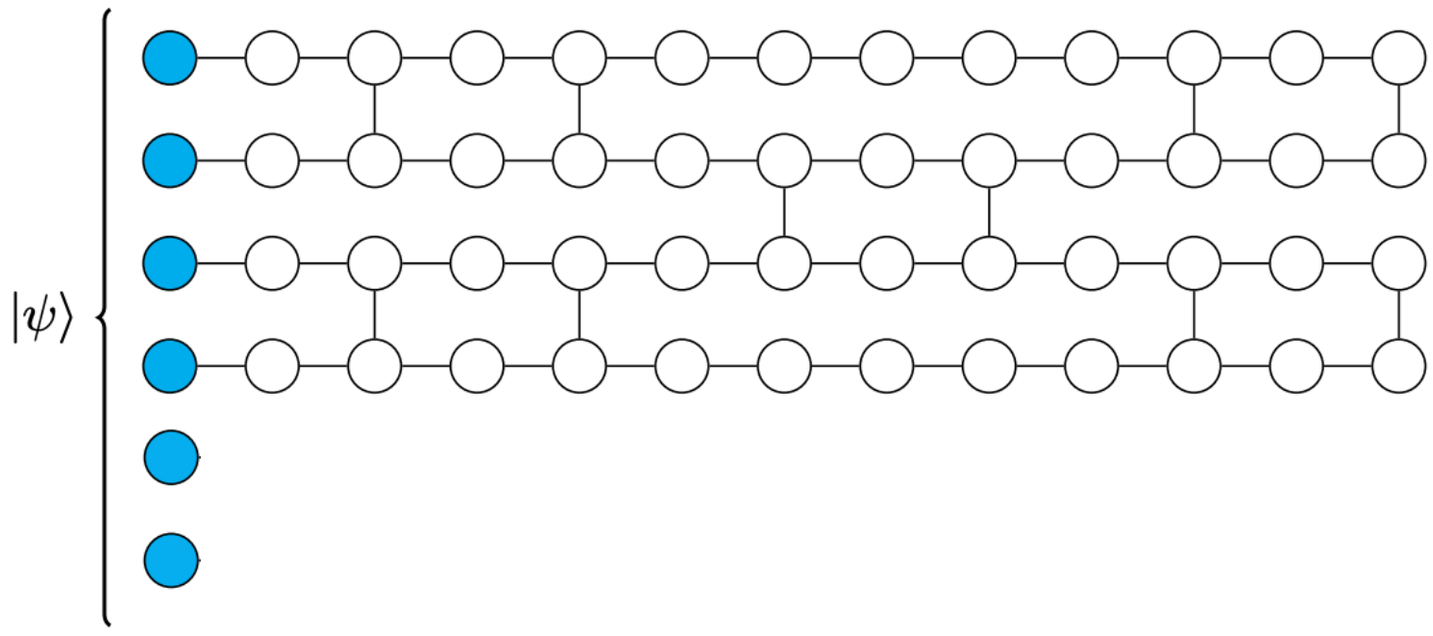
Half-Blind Quantum Computation (HBQC)

- HBQC protocol:

V(description of U)

$\left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle$

P($\left|\psi\right\rangle$)



V computes the updated measurement angle

P transmits the result

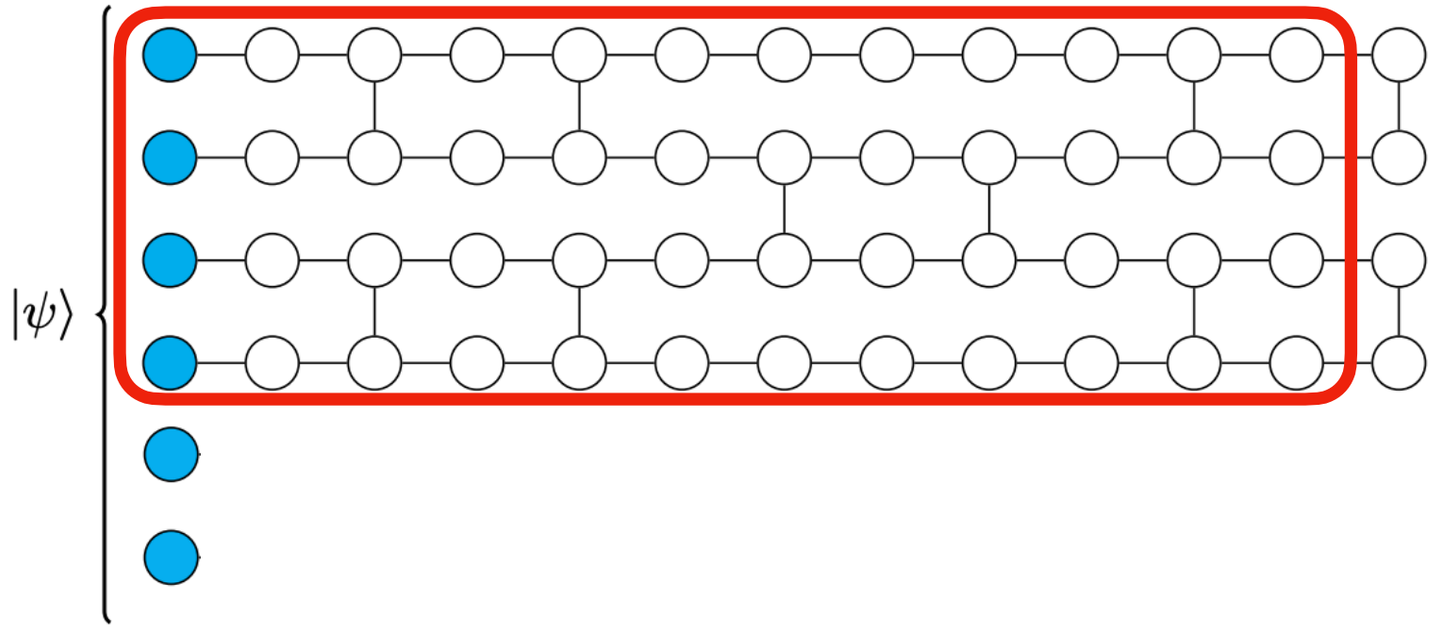
Half-Blind Quantum Computation (HBQC)

- HBQC protocol:

V(description of U)

$\left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle$

P($\left|\psi\right\rangle$)



V computes the updated measurement angle

P transmits the result

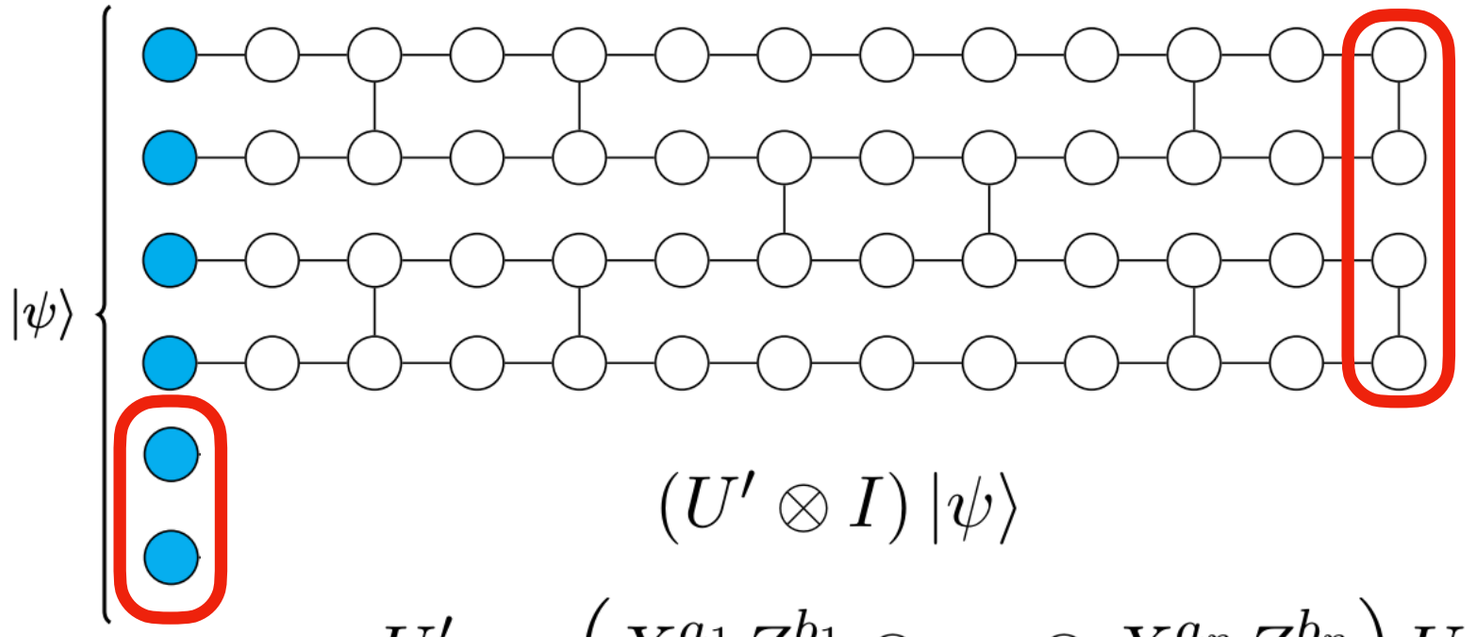
Half-Blind Quantum Computation (HBQC)

- HBQC protocol:

V(description of U)

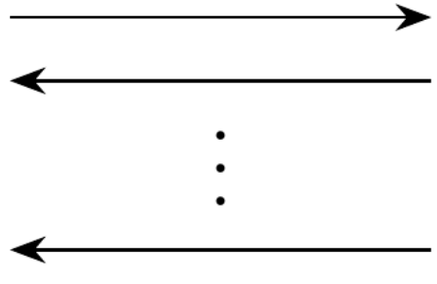
$$\left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle \quad \left|+\theta_{x,y}\right\rangle$$

P($|\psi\rangle$)



$$(U' \otimes I)\,|\psi\rangle$$

$$U' := \left(X^{a_1} Z^{b_1} \otimes \ldots \otimes X^{a_n} Z^{b_n}\right) U$$



V computes the updated measurement angle

P transmits the result

Blind Remote State Preparation

- Blind RSP = Classical client delegates preparation of single-qubit states to quantum server without revealing information about the state

$$\left\{ |+_\theta\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta \frac{\pi}{4}} |1\rangle \right), \theta \in \{0, \ldots, 7\} \right\}$$

Blind Remote State Preparation

- Blind RSP = Classical client delegates preparation of single-qubit states to quantum server without revealing information about the state

$$\left\{ |+_\theta\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta \frac{\pi}{4}} |1\rangle \right), \theta \in \{0, \ldots, 7\} \right\}$$

- Assumption: Existence of a post-quantum secure trapdoor claw-free function (TCF)

- TCF:

1. Family of injective function pairs $(f_0, f_1) : X \to Y$ with same image
2. Claw-freeness: Infeasible to find a claw (x_0, x_1) s.t. $f_0(x_0) = f_1(x_1)$
3. Given trapdoor and $y \in Y$ in the image, possible to efficiently invert to obtain a claw (x_0, x_1) s.t. $f_0(x_0) = f_1(x_1) = y$.

Blind Remote State Preparation

Subroutine parameterized by n and state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ held by the prover:

$V(n)$		$P(\|\psi\rangle)$
$((f_0, f_1), \mathrm{td}) \leftarrow \mathrm{Gen}(1^\lambda)$	$\xrightarrow{n, (f_0, f_1)}$	Compute claw state $\alpha\|0, x_0\rangle + \beta\|1, x_1\rangle$ with $f_0(x_0) = f_1(x_1) = y$
$(x_0, x_1) \leftarrow \mathrm{Invert}(\mathrm{td}, y)$	$\xleftarrow{y}$	
$r_0, r_1 \leftarrow\!\!\$\ \{0,1\}^{\mathrm{poly}(\lambda)}$	$\xrightarrow{(r_0, r_1)}$	1. Compute $\alpha\|0, x_0, -x_0 r_0\rangle + \beta\|1, x_1, x_1 r_1\rangle$ 2. Apply QFT_n to last register and measure; abort if outcome $\neq 1$. $\alpha\|0, x_0\rangle + \omega_n^{x_0 r_0 + x_1 r_1}\beta\|1, x_1\rangle$ 3. Measure last register in Hadamard basis with outcome $d \in \{0,1\}^{p(\lambda)}$. $\alpha\|0\rangle + \beta(-1)^{d\cdot(x_0 \oplus x_1)}\omega_n^{x_0 r_0 + x_1 r_1}\|1\rangle$
$b := d \cdot (x_0 \oplus x_1)$ $\theta := x_0 r_0 + x_1 r_1$	$\xleftarrow{d}$	

Blind Remote State Preparation

Blind RSP Protocol: Use the subroutine three times:

- Subroutine with $n = 2$ and $|+\rangle$.
  Let (b_1, θ_1) be the output of V, and $|\psi_1\rangle$ the output state of P.
- Subroutine with $n = 4$ and $|\psi_1\rangle$.
  Let (b_2, θ_2) be the output of V, and $|\psi_2\rangle$ the output state of P.
- Subroutine with $n = 8$ and $|\psi_2\rangle$.
  Let (b_3, θ_3) be the output of V, and $|\psi_3\rangle$ the output state of P.

The prover P holds the final state

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b \omega_8^\theta |1\rangle)$$

The verifier V holds

$$b := b_1 \oplus b_2 \oplus b_3 \text{ and } \theta := 4\theta_1 + 2\theta_2 + \theta_3 \mod 8.$$

- Security: From the prover's point of view, θ is uniformly random

Summary

- HBQC = generalized UBQC protocol [BFK09]
- TCF ⇒ blind RSP for $\left\{ |+_\theta\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta \frac{\pi}{4}} |1\rangle \right), \theta \in \{0, \ldots, 7\} \right\}$
- HBQC + blind RSP ⇒ classical blind delegation of QC
- New compiler from classical blind delegation of QC, satisfying
  1. Quantum Completeness
  2. Quantum Soundness
- Extending Mahadev's result from
  '*specific TCF from LWE ⇒ CVQC*' to '*any TCF ⇒ CVQC*'

Summary

- HBQC = generalized UBQC protocol [BFK09]
- TCF ⇒ blind RSP for $\left\{ |+_\theta\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta \frac{\pi}{4}} |1\rangle \right), \theta \in \{0, \ldots, 7\} \right\}$
- HBQC + blind RSP ⇒ classical blind delegation of QC
- New compiler from classical blind delegation of QC, satisfying
  1. Quantum Completeness
  2. Quantum Soundness
- Extending Mahadev's result from
  '*specific TCF from LWE ⇒ CVQC*' to '*any TCF ⇒ CVQC*'

Thank you for your attention!