# 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]

NEW

## Half-Blind Quantum Computation

- Generalization of the universal blind quantum computation protocol by Broadbent, Fitzsimons, and Kashefi. No computational assumptions!
- Enables a client to compute on arbitrary quantum states held by a server, even if entangled with the server's internal register, without revealing any information about the computation. Moreover, the server can later continue the computation on its internal registers in the plain.
- Information-theoretic security but requires client to prepare single-qubit states from $\left\{|+_\theta\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta\frac{\pi}{4}}|1\rangle\right), \theta \in \{0,\dots,7\}\right\}$.

+

NEW

## Blind Remote State Preparation

- New blind RSP protocol for $\left\{|+_\theta\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta\frac{\pi}{4}}|1\rangle\right), \theta \in \{0,\dots,7\}\right\}$ from any Trapdoor Claw-Free Function (TCF), e.g., those implied by LWE or cryptographic group actions.
- Classical client can delegate the preparation of single-qubit states to a quantum server without revealing any information about the states.
- Enables us to replace the quantum communication in HBQC with classical communication, leading to CHBQC.

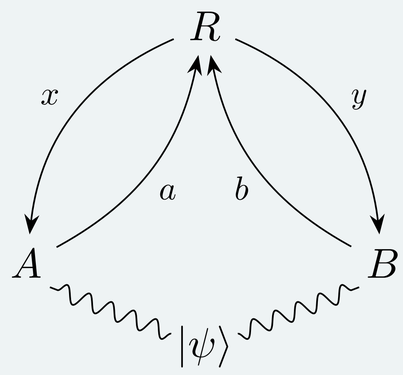
=

## Classical Half-Blind Quantum Computation (CHBQC)

---

## Nonlocal Game $\mathcal{G}$

- **CRUCIAL**: No communication between Alice and Bob during the game! However, can agree on a strategy and share an entangled state beforehand.
- **BUT**: How to enforce the no-communication rule? Can we design a single-player version that preserves the original game's winning probabilities?

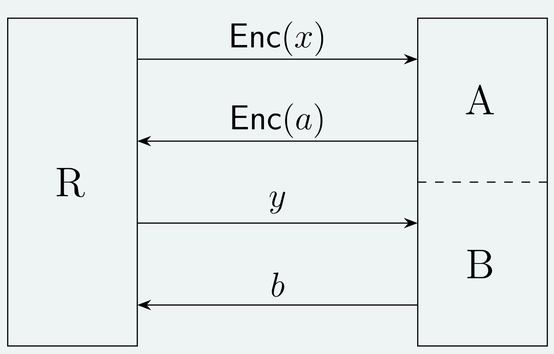



$\omega_c(\mathcal{G}) :=$ maximal winning probability for classical players

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

$\omega_{qc}(\mathcal{G}) :=$ maximal winning probability for general quantum players

## [KLVY23] Compiled Game $\mathcal{G}^{\mathrm{KLVY}}_{comp}$




- Player first simulates Alice's computation by homomorphically evaluating her quantum circuit on the encrypted question using Quantum (Fully) Homomorphic Encryption, then simulates Bob's computation in the plain. Encryption emulates spatial separation.
- Quantum Completeness ([KLVY23]):

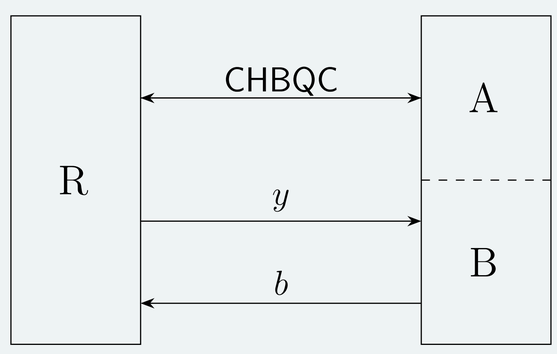
$$\omega_q(\mathcal{G}^{\mathrm{KLVY}}_{comp}) \geq \omega_q(\mathcal{G})$$

- Classical & Quantum Soundness ([KLVY23, KMPSW24, NZ23]):

$$\omega_c(\mathcal{G}^{\mathrm{KLVY}}_{comp}) \leq \omega_c(\mathcal{G}), \quad \omega_q(\mathcal{G}^{\mathrm{KLVY}}_{comp}) \leq \omega_{qc}(\mathcal{G})$$

NEW

## [BKMSW24] Compiled Game $\mathcal{G}^{\mathrm{BKMSW}}_{comp}$




- Verifier and prover run the CHBQC protocol to simulate Alice's computation: Verifier's input is Alice's unitary, while player's input is the quantum state from the underlying nonlocal game. Prover then simulates Bob's computation in the plain. Blindness emulates spatial separation.
- Quantum Completeness:

$$\omega_q(\mathcal{G}^{\mathrm{BKMSW}}_{comp}) \geq \omega_q(\mathcal{G})$$

- Quantum Soundness:

$$\omega_q(\mathcal{G}^{\mathrm{BKMSW}}_{comp}) \leq \omega_{qc}(\mathcal{G})$$

[NZ23]

## Classical Verification of Quantum Computation...

[BKMSW24, NZ23]

...using Q(F)HE.

NEW

...from potentially weaker and new cryptographic assumptions using any TCF!

[BKMSW24] K. Bacho, A. Kulpe, G. Malavolta, S. Schmidt, M. Walter, "Compiled Nonlocal Games from any Trapdoor Claw-Free Function", eprint/2024/1829
[KLVY23] Y. Kalai, A. Lombardi, V. Vaikuntanathan, L. Yang, "Quantum Advantage from Any Non-local Game", STOC'23
[KMPSW24] A. Kulpe, G. Malavolta, C. Paddock, S. Schmidt, M. Walter, "A bound on the quantum value of all compiled nonlocal games", QIP'25 & STOC'25
[NZ23] A. Natarajan, T. Zhang, "Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification", FOCS'23

[BKMSW24]

[1]Ruhr University Bochum
[2]University of Edinburgh
[3]Bocconi University

RUHR UNIVERSITÄT BOCHUM RUB CASA Cyber Security in the Age of Large-Scale Adversaries THE UNIVERSITY of EDINBURGH Bocconi