CASA

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Compiled Nonlocal Games

Bochum, 2024-12-10

Alexander Kulpe
Chair for Quantum Information, Ruhr-University Bochum

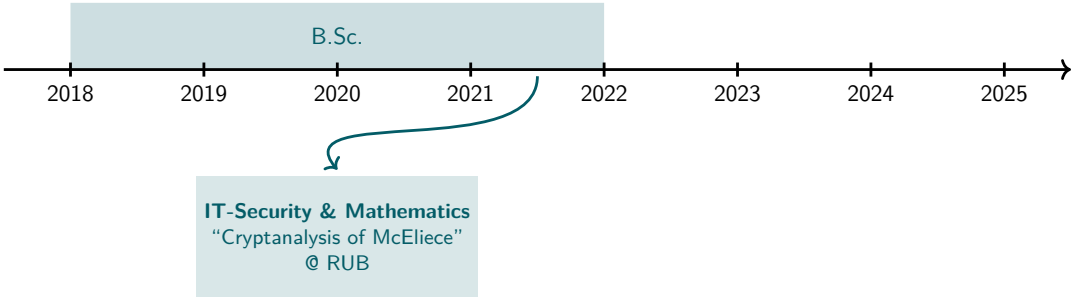
RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HGI HORST GÖRTZ INSTITUT

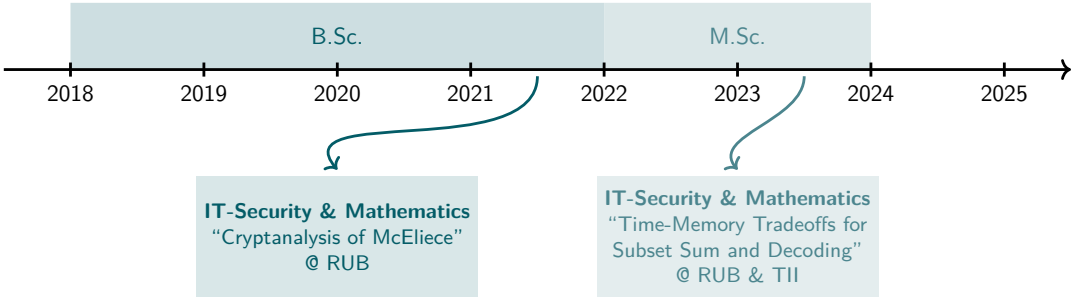
About Me

CASA
Cyber Security in the Age of Large-Scale Adversaries



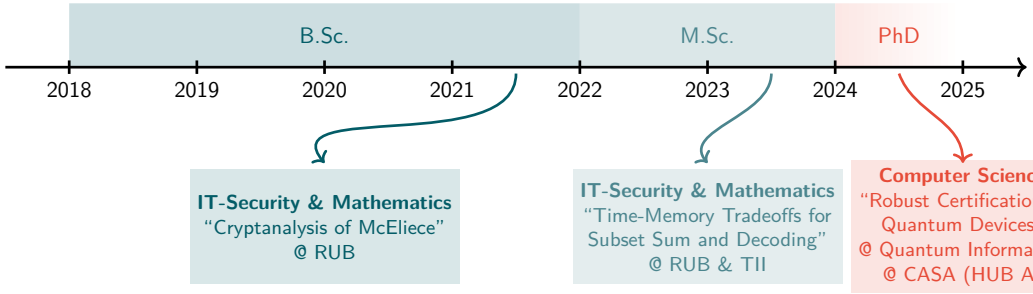
About Me

CASA
Cyber Security in the Age of Large-Scale Adversaries



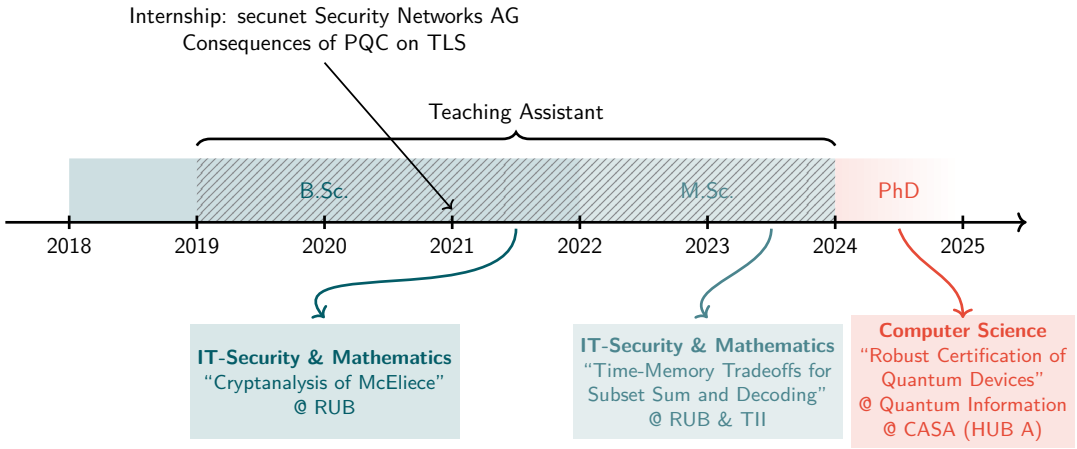
About Me

CASA
Cyber Security in the Age of Large-Scale Adversaries



About Me

CASA
Cyber Security in the Age of Large-Scale Adversaries



About The Project

CASA
Cyber Security in the Age of Large-Scale Adversaries

FRP "Robust Certification of Quantum Devices"

- Use cryptography to verify properties about quantum devices, verify computations etc.
- PIs: Michael Walter (RUB) and Giulio Malavolta (Bocconi/MPI-SP)
- PostDoc: Simon Schmidt
- PhD Student: Alexander Kulpe

- Motivation
- Multi-Interactive Proof Systems
- Quantum Basics
- Compiled Nonlocal Games
- Current Research & Contributions

Motivation

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
    - We would be impressed
    - Maybe factoring is in P?

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
  - Run some quantum protocol (i.e. *QKD*) between two boxes

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
  - Run some quantum protocol (i.e. *QKD*) between two boxes
    - Practical
    - Need *two* quantum devices that communicate

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
  - Run some quantum protocol (i.e. *QKD*) between two boxes
  - Send some *quantum state* to the box and have it apply some operation

Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
  - Run some quantum protocol (i.e. *QKD*) between two boxes
  - Send some *quantum state* to the box and have it apply some operation
    - In principle easy
    - Verifier needs to be quantum

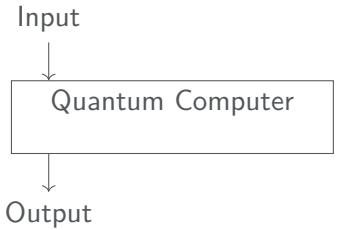
Motivation: Quantum Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

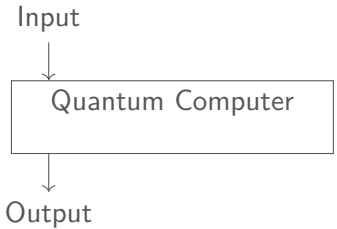
Quantum Computer?

- How to test that this box is a quantum computer?
  - Ask it to *factor* an RSA-2048 number
  - Run some quantum protocol (i.e. *QKD*) between two boxes
  - Send some *quantum state* to the box and have it apply some operation
- Question: Can a *classical* verifier check that the box is quantum?

Motivation: Classically Verifying Quantum Computation

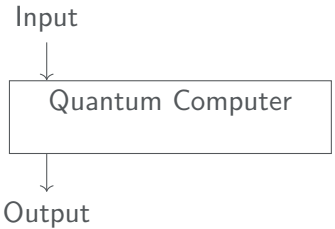


Motivation: Classically Verifying Quantum Computation



- Question: Can a *classical* verifier check that the output is correct, i.e. can we verify the quantum computation *classically*?

Motivation: Classically Verifying Quantum Computation



- Question: Can a *classical* verifier check that the output is correct, i.e. can we verify the quantum computation *classically*?
- Answer: All this and more is possible with *nonlocal games* which are special interactive protocols!

Multi-Interactive Proof Systems

Mathematical Proofs

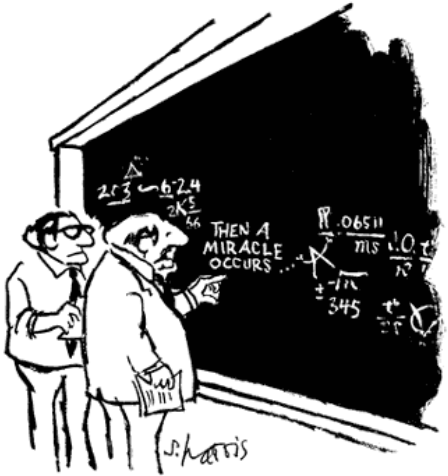
CASA
Cyber Security in the Age of Large-Scale Adversaries

- Informally: Derivation of a statement from a set of axioms using a set of inference rules
- It should be verifiable effectively (efficiently)

$\Rightarrow$ Static Objects

Mathematical Proofs

- Informally: Derivatic ısing a set of inference rules
- It should be verifiabl
- $\Rightarrow$ Static Objects



"I think you should be more explicit here in step two."

Mathematical Proofs

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Informally: Derivation of a statement from a set of axioms using a set of inference rules
- It should be verifiable effectively (efficiently)

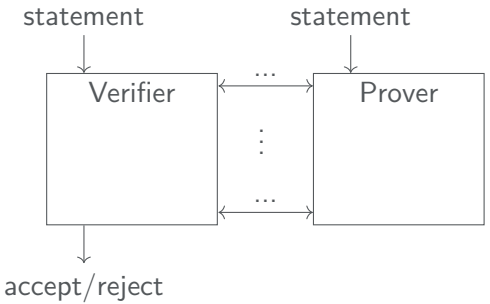
$\Rightarrow$ Static Objects

- Proof process can be divided:
  - Prover, who presents proof candidate
  - Verifier, who checks proof candidate

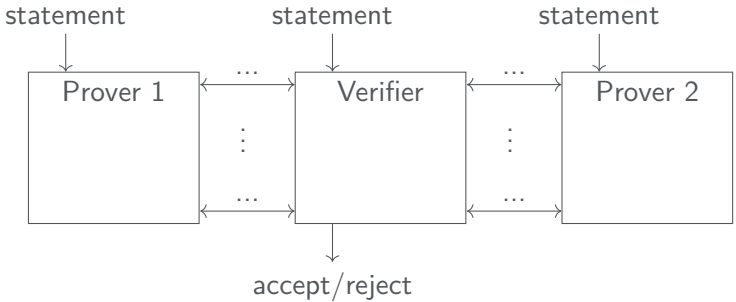
Interactive Proofs

- Prover tries to convince a verifier that statement is true
- Verifier may ask questions

$\Rightarrow$ interactive instead of static



Multi-Interactive Proof Systems



- Provers are not allowed to communicate

Quantum

Entanglement

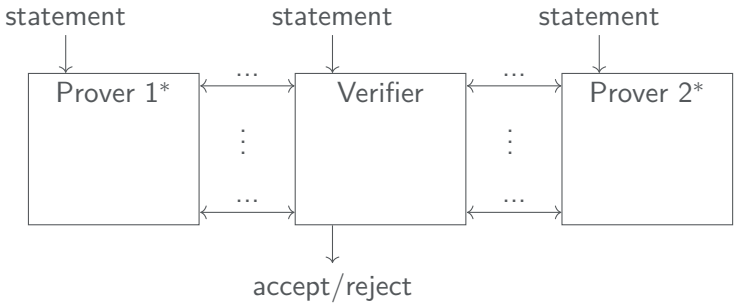
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Bit: $b \in \{0, 1\}$
- Qubit: unit vector $q = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$, i.e. $|\alpha|^2 + |\beta|^2 = 1$
- *Measuring* q gives us 0 w.p. $|\alpha|^2$ and 1 w.p. $|\beta|^2$.

Definition 1 (Entanglement)

If two qubits are *entangled*, their states depend on each other. Measuring one qubit influences the state of the other entangled qubit.

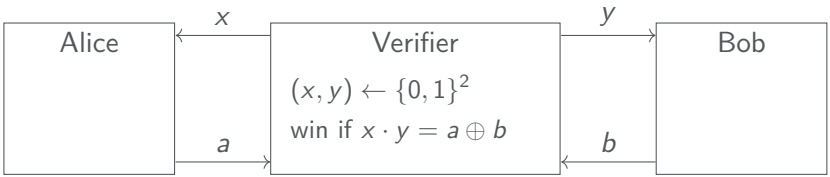
MIP*



- **Quantum** Provers are not allowed to communicate, **but they are allowed to share entangled states**

Nonlocal Games

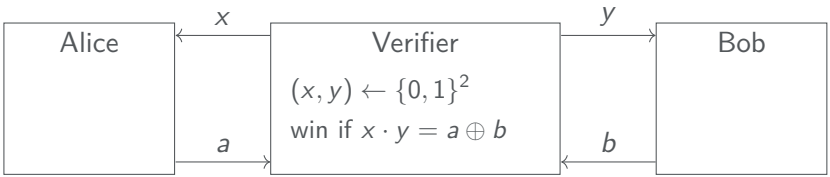
Nonlocal Game Example: CHSH



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

- There exists a classical strategy that wins w.p. 75 %

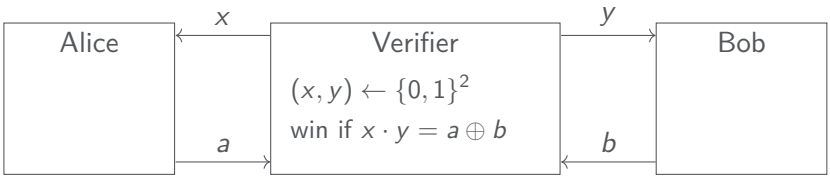
Nonlocal Game Example: CHSH



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

- There exists a classical strategy that wins w.p. 75 %
- There does not exists a classical strategy that wins w.p. > 75 %

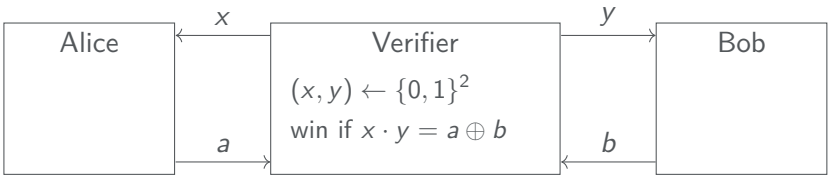
Nonlocal Game Example: CHSH



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

- There exists a classical strategy that wins w.p. 75 %
- There does not exists a classical strategy that wins w.p. > 75 %
- There exists a quantum strategy that wins w.p. ≈ 85 %

Nonlocal Game Example: CHSH

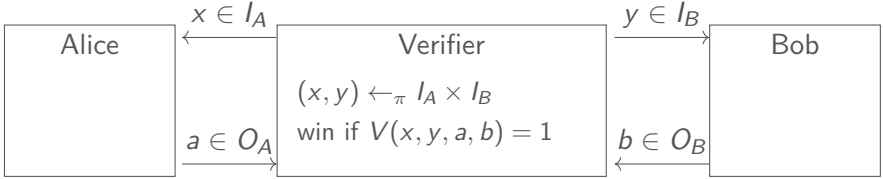


x	y	winning condition
0	0	$a \oplus b = 0$
0	1	$a \oplus b = 0$
1	0	$a \oplus b = 0$
1	1	$a \oplus b = 1$

- There exists a classical strategy that wins w.p. 75 %
- There does not exists a classical strategy that wins w.p. > 75 %
- There exists a quantum strategy that wins w.p. ≈ 85 %

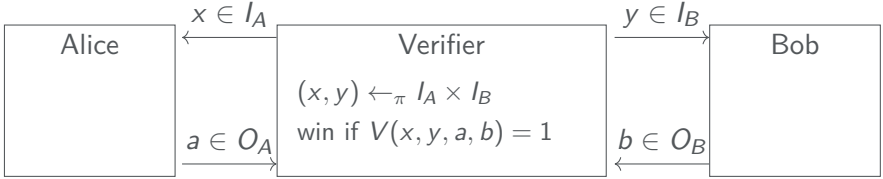
If Alice and Bob win with probability > 75 % they must have quantum capabilities!

Nonlocal Games



- I_A, I_B input sets
- π distribution on questions; known to Alice and Bob
- O_A, O_B output sets
- V function, that decides whether Alice and Bob win or not; known to Alice and Bob

Nonlocal Games



- I_A, I_B input sets
- π distribution on questions; known to Alice and Bob
- O_A, O_B output sets
- V function, that decides whether Alice and Bob win or not; known to Alice and Bob
- Alice and Bob try to maximize their winning probability

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Definition 2 (Self-test)

There are games where the best strategy is unique, i.e. the provers have to perform specific operations, used specific shared state, need a mininum amount of quantum memory.

Applications:

- Certify properties of quantum devices
- Certified randomness expansion
- Device-independent quantum cryptography
- Classical verification of quantum computation

Definition 2 (Self-test)

There are games where the best strategy is unique, i.e. the provers have to perform specific operations, used specific shared state, need a mininum amount of quantum memory.

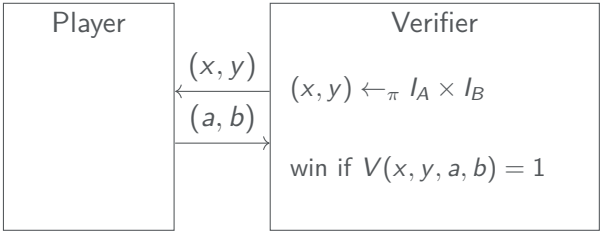
Applications:

- Certify properties of quantum devices
- Certified randomness expansion
- Device-independent quantum cryptography
- Classical verification of quantum computation

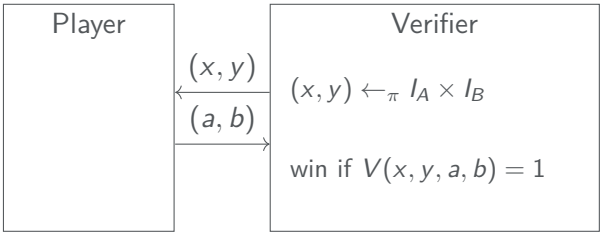
BUT: The provers are not allowed to communicate! How can we enforce this? Can we achieve the same with one player instead of two?

Compiled Nonlocal Games

First Try: Playing In Parallel



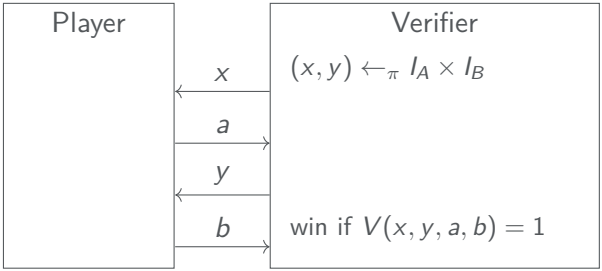
First Try: Playing In Parallel



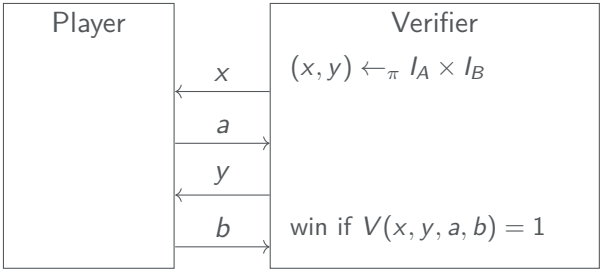
Does not work!

If the player knows both questions before answering, he can adaptively choose a and b dependent on **both** questions. In this case CHSH can be won perfectly

Second Try: Playing Sequentially



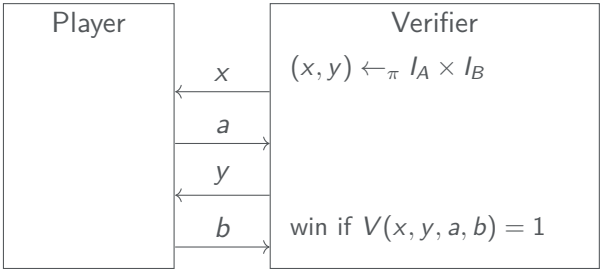
Second Try: Playing Sequentially



Better, but still does not work!

The first two messages simulate Alice's part. But in in the second part, the player knows x, a, y instead of only y and can choose b adaptively. In this case CHSH can be won perfectly

Second Try: Playing Sequentially



Idea

Use cryptography to ensure that the player does not know x, a when providing b.

CASA
Cyber Security in the Age of Large-Scale Adversaries

Definition 3 (Quantum Fully Homomorphic Encryption)

A QFHE scheme consists of a tuple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ such that

- $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a usual encryption scheme
- Eval allows to perform arbitrary efficient mathematical operations on the encrypted data, for example

$$\mathsf{Enc}(x_1 + x_2) \leftarrow \mathsf{Eval}(+, \mathsf{Enc}(x_1), \mathsf{Enc}(x_2))$$
$$\mathsf{Enc}(x_1 \cdot x_2) \leftarrow \mathsf{Eval}(\cdot, \mathsf{Enc}(x_1), \mathsf{Enc}(x_2))$$
$$\mathsf{Enc}(f(x)) \leftarrow \mathsf{Eval}(f, \mathsf{Enc}(x))$$

CASA
Cyber Security in the Age of Large-Scale Adversaries

Definition 3 (Quantum Fully Homomorphic Encryption)

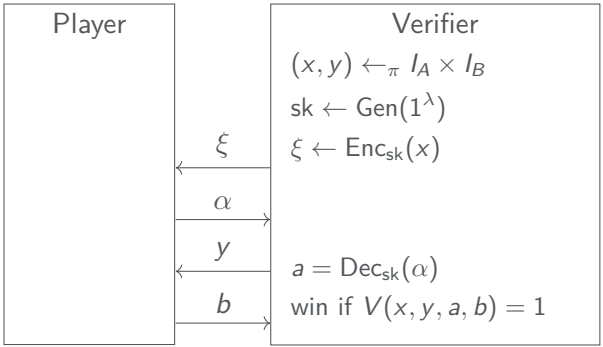
A QFHE scheme consists of a tuple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ such that

- $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a usual encryption scheme
- Eval allows to perform arbitrary efficient mathematical operations on the encrypted data, for example

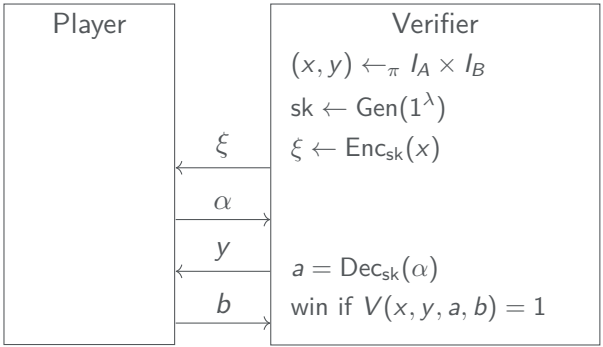
$$\begin{aligned} \mathsf{Enc}(x_1 + x_2) &\leftarrow \mathsf{Eval}(+, \mathsf{Enc}(x_1), \mathsf{Enc}(x_2)) \\ \mathsf{Enc}(x_1 \cdot x_2) &\leftarrow \mathsf{Eval}(\cdot, \mathsf{Enc}(x_1), \mathsf{Enc}(x_2)) \\ \mathsf{Enc}(f(x)) &\leftarrow \mathsf{Eval}(f, \mathsf{Enc}(x)) \end{aligned}$$

A QFHE scheme is called *quantum-secure* if no efficient quantum adversary can distinguish between $\mathsf{Enc}(x_1), \mathsf{Enc}(x_2)$.

KLVY Compiler



KLVY Compiler



KLVY Results

- Players in the compiled game can be *at least as good* as in the nonlocal game!
- Classical Players cannot do better in the compiled game

Open Question: Can quantum players do better in the compiled game or not?

Current Research & Contributions

Quantum Soundness

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- NZ23: Quantum player in the CHSH game cannot do better in the compiled game

Compiled Nonlocal Games | A. Natarajan, et al. *Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification* FOCS'23
D Cui, et al. *A Computational Tsirelson's Theorem for the Value of Compiled XOR Games.* TQC'24, arXiv:2402.17301.
A. Kulpe, G. Malavolta, C. Paddock, S. Schmidt, M. Walter *A bound on the quantum value of all compiled nonlocal games* arXiv:2408.06711.

Quantum Soundness

- NZ23: Quantum player in the CHSH game cannot do better in the compiled game
- C**M**MN**SW**Z24: Quantum players for the class of XOR games (including CHSH) cannot do better in the compiled game

Quantum Soundness

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- NZ23: Quantum player in the CHSH game cannot do better in the compiled game
- C**M**MN**SW**Z24: Quantum players for the class of XOR games (including CHSH) cannot do better in the compiled game
- **KM**P**SW**24: Quantum players for any nonlocal game cannot do better in the compiled game
  - Accepted in QIP'25 & submitted to STOC'25

Alternative Compiler

CASA
Cyber Security in the Age of Large-Scale Adversaries

- KLVY uses QFHE as cryptographic primitive. Currently, we only know two ways to construct a QFHE scheme.
  - LWE
  - iO + dual-mode TCF
- Question & Master's Project: Can we get a compiler with weaker cryptographic assumptions?

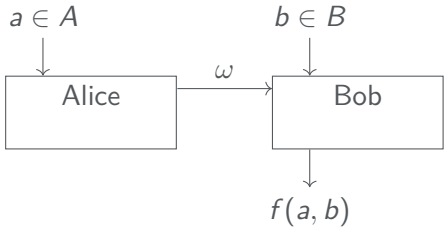
Alternative Compiler

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- KLVY uses QFHE as cryptographic primitive. Currently, we only know two ways to construct a QFHE scheme.
  - LWE
  - iO + dual-mode TCF
- Question & Master's Project: Can we get a compiler with weaker cryptographic assumptions?
- Answer: Yes!
  - **BKMSW**24: Compiler from any TCF
  - Quantum players cannot do better under this compiler, too (follows from [KMP+24])
  - Plan to submit to upcoming crypto conferences

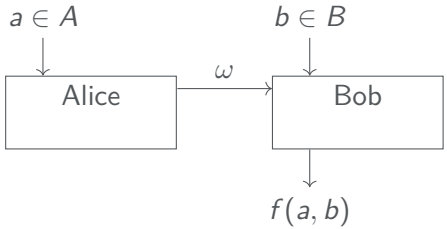
Current Projects: Compiled Communication Complexity

- Until now: No communication between Alice and Bob
- What if we allow some communication between Alice and Bob?



Current Projects: Compiled Communication Complexity

- Until now: No communication between Alice and Bob
- What if we allow some communication between Alice and Bob?



- Can we use similar compilation techniques in this scenario such that the communication that is needed for Bob to compute $f(a, b)$ stays the same (for classical players)?
- ...

CASA
Cyber Security in the Age of Large-Scale Adversaries

Many thanks for your attention!

Contact me

- . . .if you are interested in Quantum Information, (Quantum) Cryptography, etc.
- alexander.kulpe@rub.de, MC 1/85

[BKM+24] Kaniuar Bacho, Alexander Kulpe, Giulio Malavolta, Simon Schmidt, and Michael Walter.
Compiled nonlocal games from any trapdoor claw-free function.
Cryptology ePrint Archive, Paper 2024/1829, 2024.

[CMM+24] David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang.
A computational tsirelson's theorem for the value of compiled xor games.
TQC'24, arXiv:2402.17301, 2024.

[KMP+24] Alexander Kulpe, Giulio Malavolta, Connor Paddock, Simon Schmidt, and Michael Walter.
A bound on the quantum value of all compiled nonlocal games.
arXiv:2408.06711, 2024.