

CASA

CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Trading Space for Time in Nonlocal Games

Bochum, 2024-12-13

Alexander Kulpe

Chair for Quantum Information, Ruhr-University Bochum

RUHR
UNIVERSITÄT
BOCHUM

RUB

Gefördert durch

DFG

Deutsche
Forschungsgemeinschaft



Motivation: Quantum Advantage

Quantum Computer?

Motivation: Quantum Advantage

Quantum Computer?

 How to test that this box is a quantum computer?

Motivation: Quantum Advantage

Quantum Computer?

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

Motivation: Quantum Advantage

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

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

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

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

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

Quantum Computer?

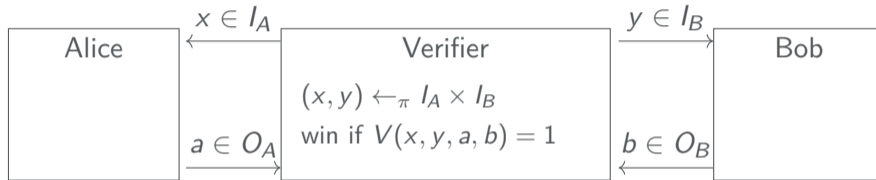
- 🐘 How to test that this box is a quantum computer?
 - 🐘 Ask it to *factor* an RSA-2048 number
 - 🐘 Run some quantum protocol (i.e. *QKD*) between two boxes
 - 🐘 Send some *quantum state* to the box and have it apply some operation
- 🐘 Question: Can a *classical* verifier check that the box is quantum?

Motivation: Quantum Advantage

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?
- 🐘 Answer: This and more is possible with *nonlocal games* which are special interactive protocols!

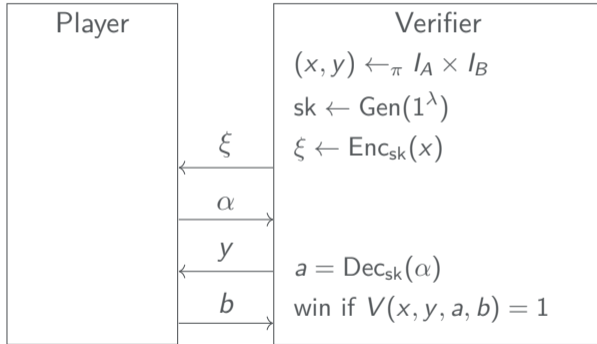
Nonlocal Games



- 🐘 Alice and Bob are **not** allowed to communicate
- 🐘 Alice and Bob try to maximize their winning probability
- 🐘 How to enforce no-communication? Can we play with **one** player instead?

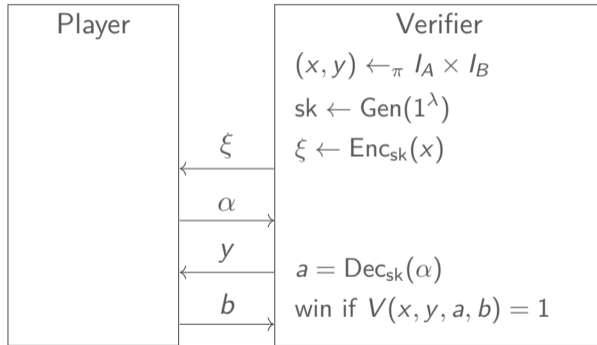
KLVY Compiler

Idea: Play sequentially and use fully homomorphic encryption!





KLVY Compiler

Idea: Play sequentially and use fully homomorphic encryption!



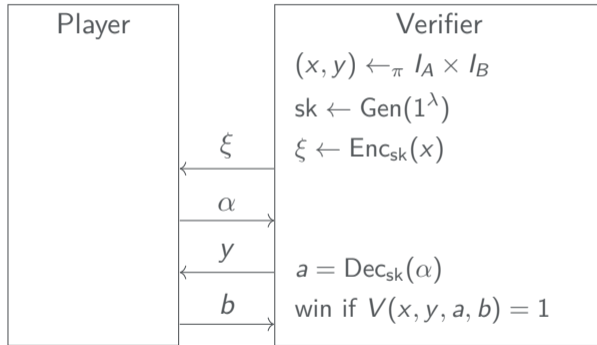
KLVY Results

-  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?

KLVY Compiler

Idea: Play sequentially and use fully homomorphic encryption!



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?

Short Answer: NO, they cannot! :)

Many thanks for your attention!



Colloquium Slides



Poster



Paper



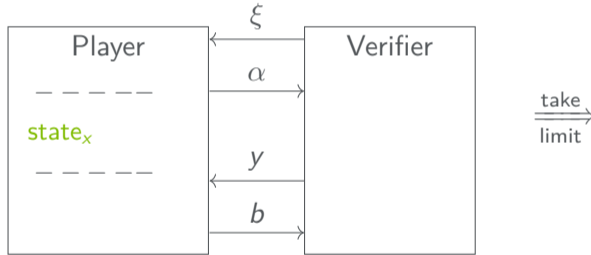
Christmas Surprise

Happy pre-Christmas season!

Quantum Soundness

Answer: Quantum players cannot do better in the compiled game

Computational World

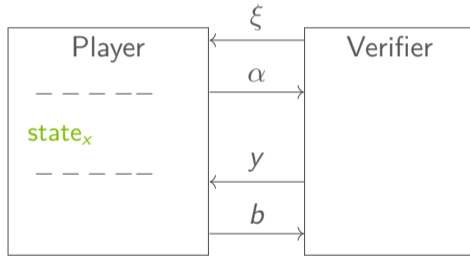


 $state_x \approx_c state_{x'}$

Quantum Soundness

Answer: Quantum players cannot do better in the compiled game

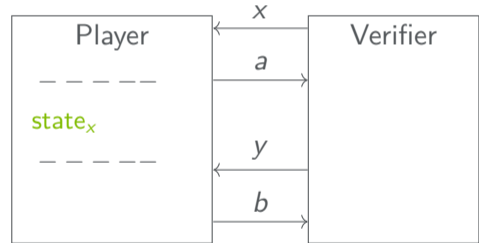
Computational World




 $state_x \approx_c state_{x'}$

Information-Theoretical World

take
limit \Rightarrow

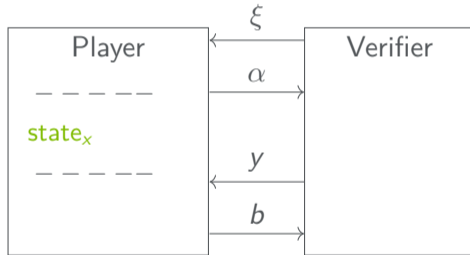


 $state_x = state_{x'}$

Quantum Soundness

Answer: Quantum players cannot do better in the compiled game

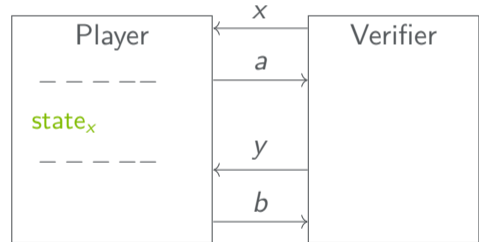
Computational World




 $state_x \approx_c state_{x'}$

Information-Theoretical World

take
limit \Rightarrow



 $state_x = state_{x'}$

\Downarrow Extract
strategy for nonlocal game