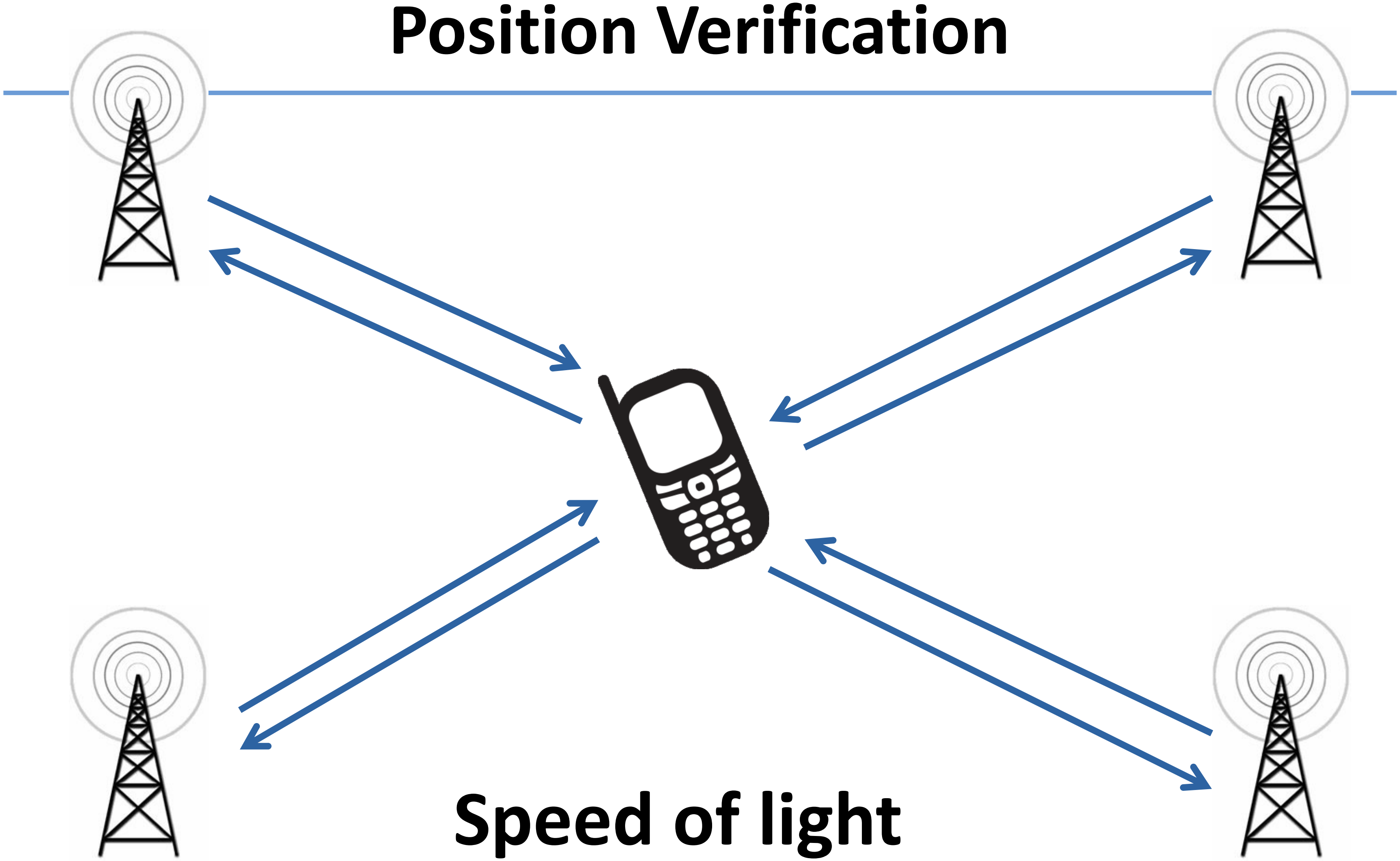
Quantum Position Verification in the Plane

Serge Fehr and Dominique Unruh

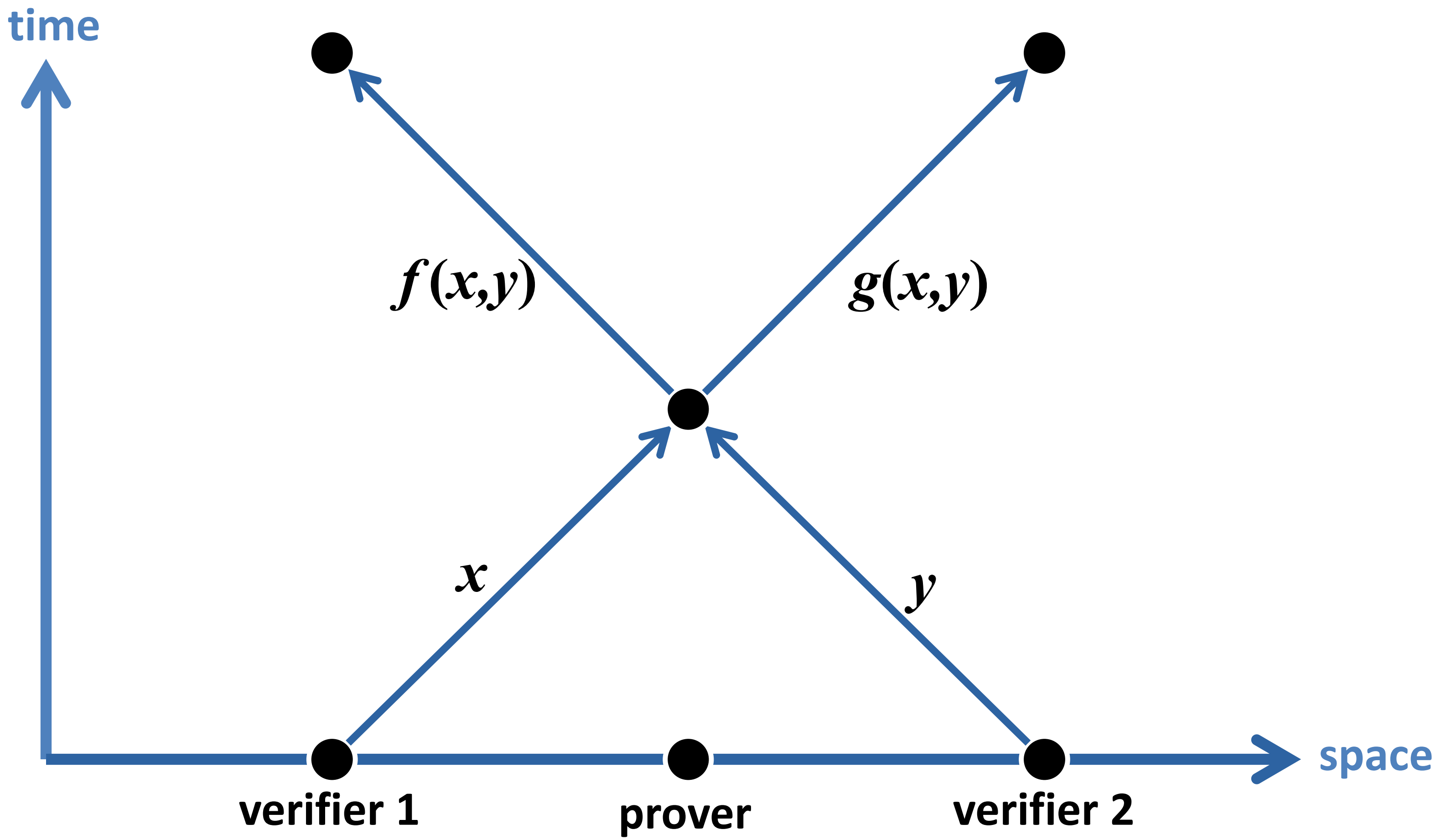
CWI University of Tartu

Position Verification

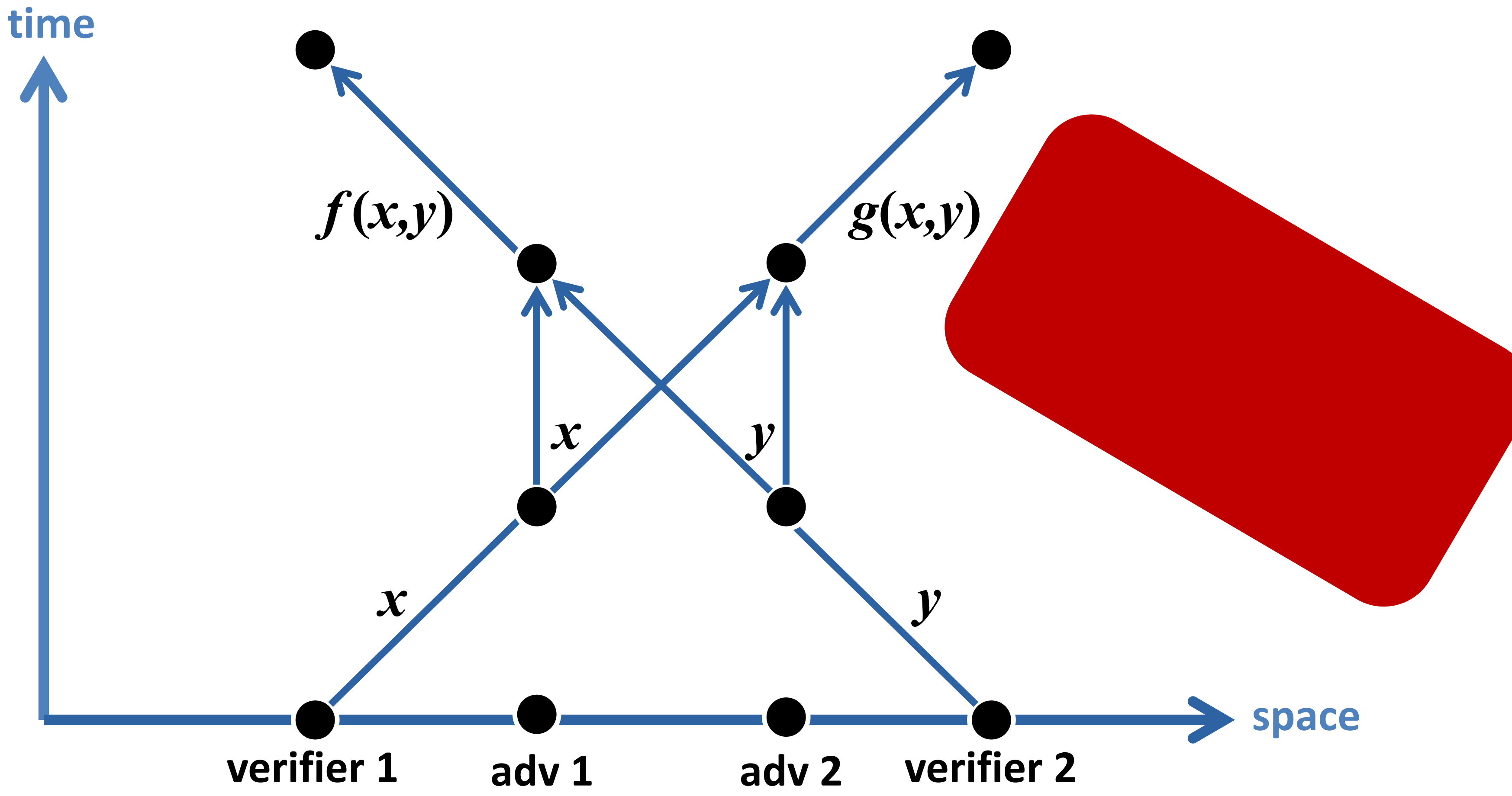


Speed of light
→ Position verified

A generic protocol



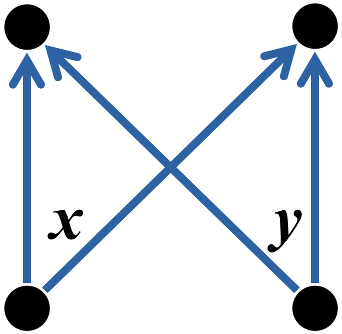
A generic attack



[CGMO09] Chandran, Goyal, Moriarty, Ostrovsky, *Position Based Cryptography*, Crypto 2009

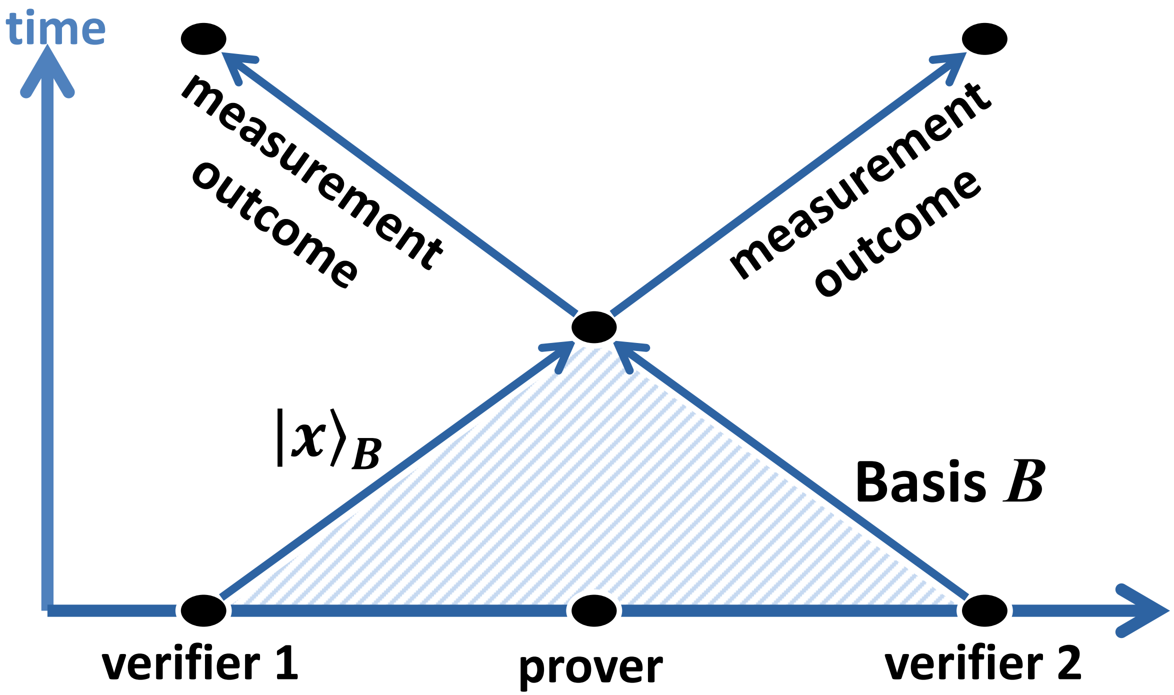
Way out: quantum crypto

- In attack: adversary copies x,y
- If x or y quantum: No cloning!
- Attack does not work
- Other attacks?
  - Without extra assumptions:
    Generic attack (exponential entanglement)



[BCF⁺11] Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner: *Position-Based Quantum Crypto*, Crypto 2011

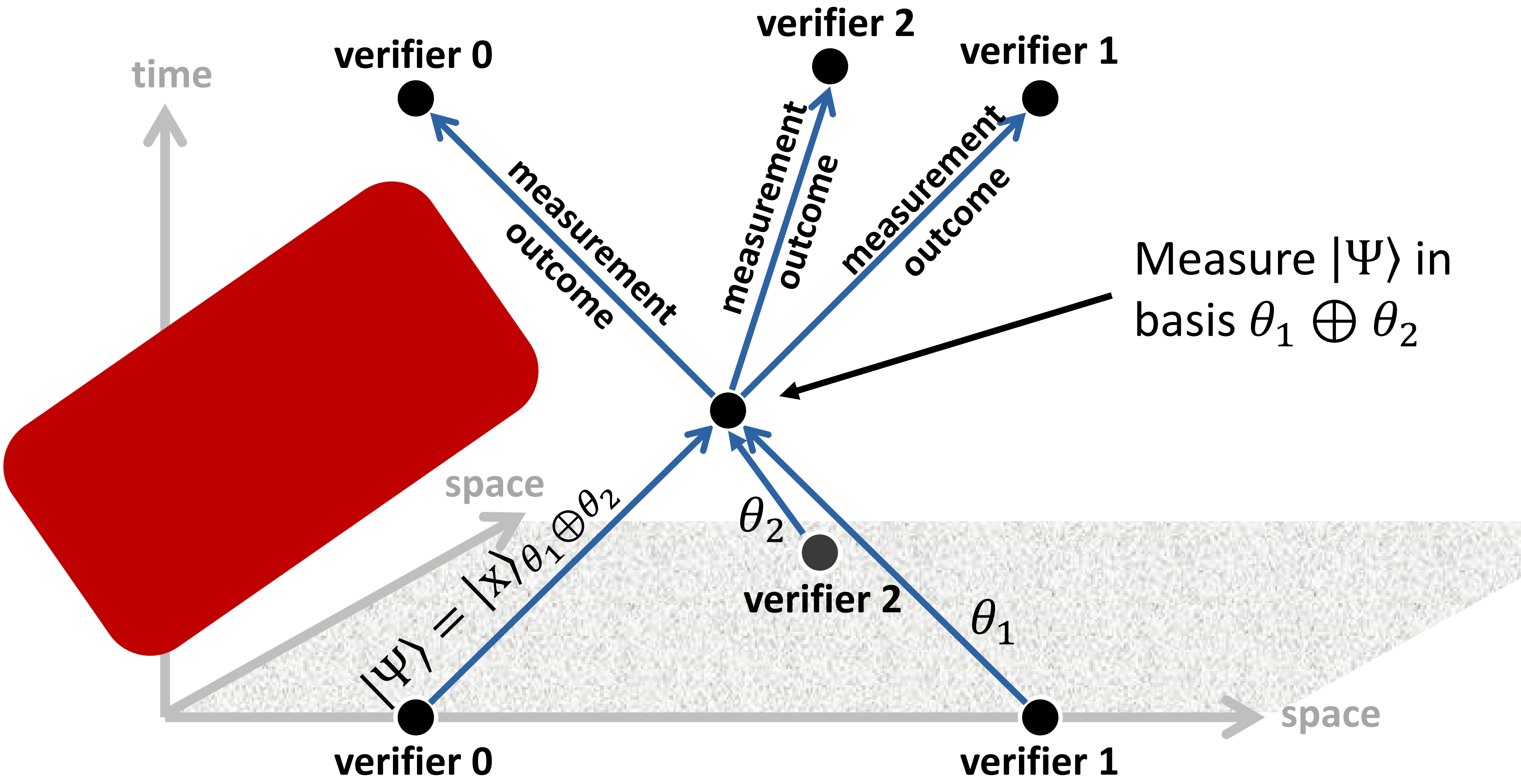
Quantum crypto: A secure protocol



Assumption:
No entangled photons in ▨

[TFKW13] Tomamichel, Fehr, Kaniewski, Wehner: *One-Sided Device-Independent QKD and Position-Based Cryptography from Monogamy Games*, Eurocrypt 2013 (and [BCF+11])

2D/3D case



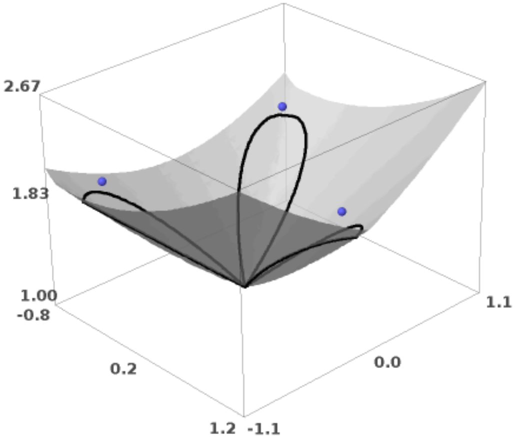
(There is a secure 3D protocol in the random oracle model, though [Unr14])

Our result

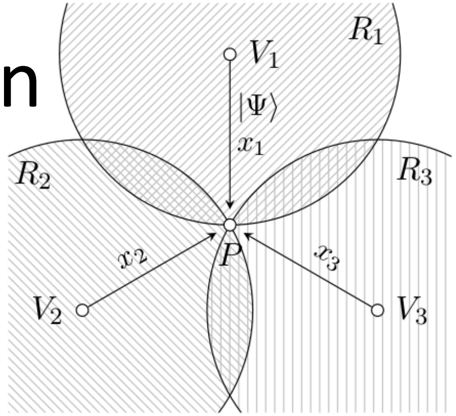
- Security proof in **2D-case**
- Sufficient for position verification “on earth”
- 3D-case: open problem

Why is 2D/3D tricky?

- Events (like getting all three messages) along complicated space-time surfaces



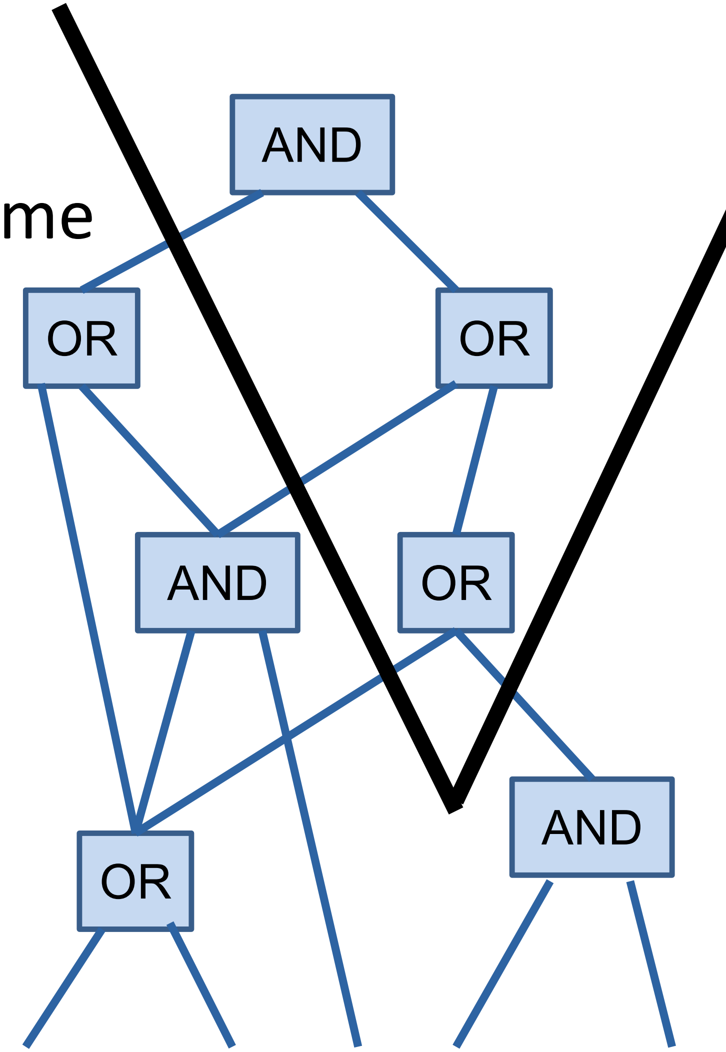
- In some space-time areas, some but not all messages known



- Complicated mix geometry + quantum

Proof technique: Space-time circuits

- Tool: Space-time circuits
  - Gates have positions in space-time
  - No wire leaves light cone
- Derive connectivity from geometry
- Then forget about geometry, only use connectivity
  - Normal game-based proof



[Unruh, *Quantum Pos. Verif. in the RO model*, Crypto 14]

Proof – analyzing space-time regions

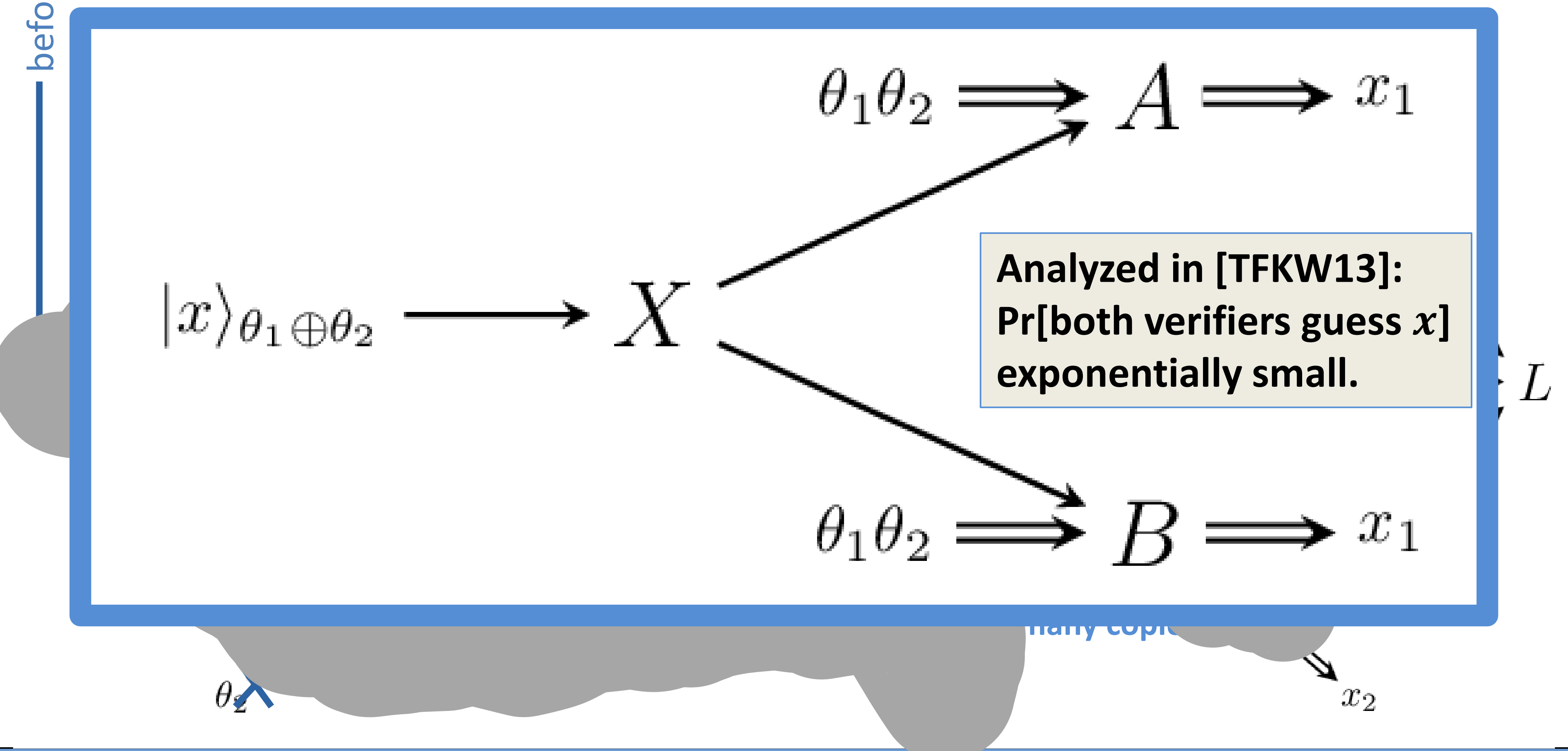
before protocol

reachable by one verifier

reachable by two verifiers

reaches two verifiers

reaches one verifier



Analyzed in [TFKW13]: Pr[both verifiers guess x] exponentially small.

Conclusion

- 2D case solved
- Lesson learned:
  Relativistic protocols complicated in 2D/3D
  - [BCF$^+$11] got it wrong.
- Use space-time circuits!
  (Also for relativistic commitments)
- 3D case: open problem

Thank you for your attention

European Union
European Social Fund

Investing in your futu

ARCHIMEDES

DoRa

European Union
Regional Development Fund

Investing in your future

EXCS
ESTONIAN COMPUTING

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
PRIMUM ACQUIRERE COGNITIONEM
UNITED STATES AIR FORCE

Postdoc Positions (also phd)

Verification of Quantum Crypto

Formal verification of quantum crypto protocols
(“QuEasyCrypt” tool)

http://tinyurl.com/postdoc-vqc