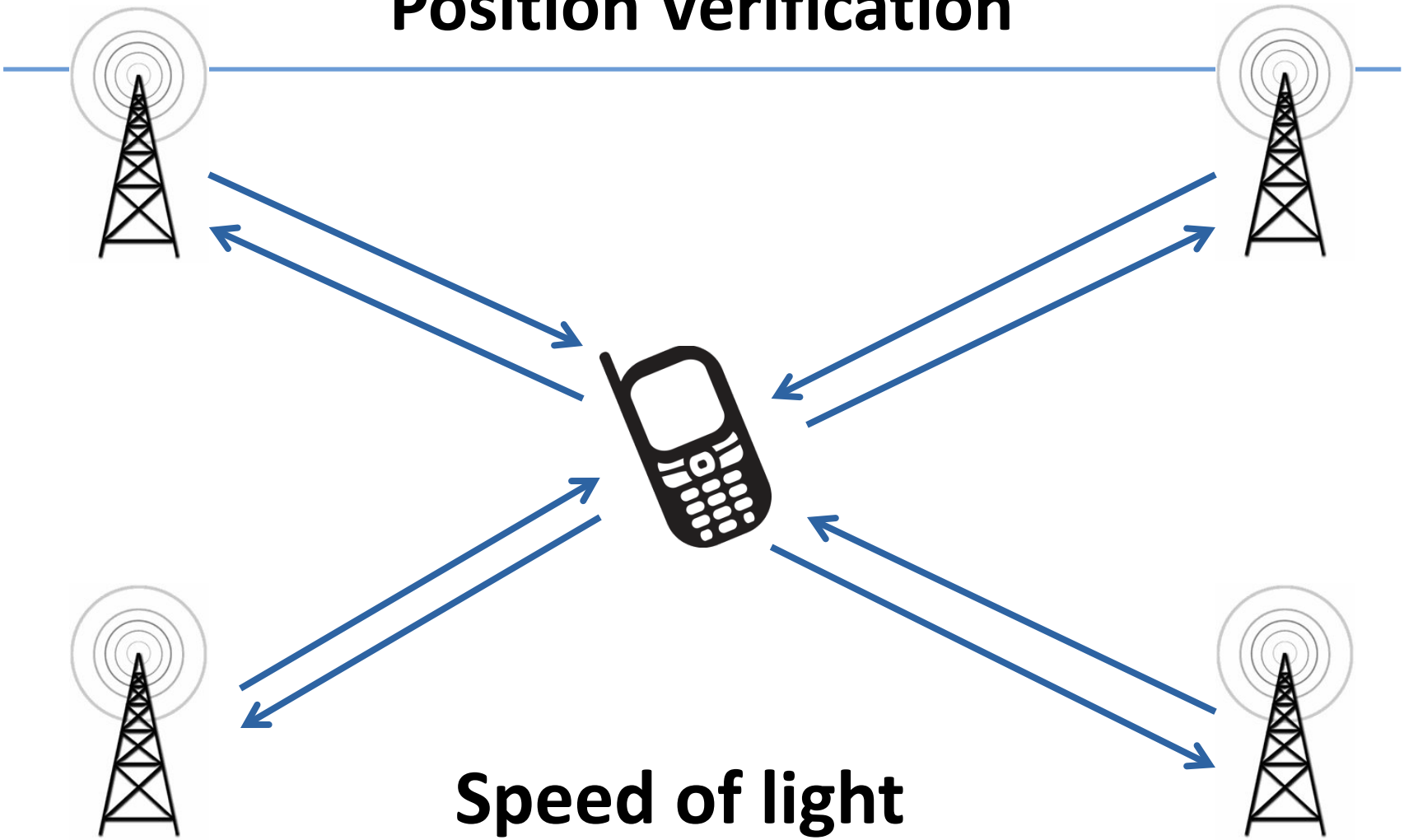
Quantum Position Verification in the random oracle model

Dominique Unruh

University of Tartu

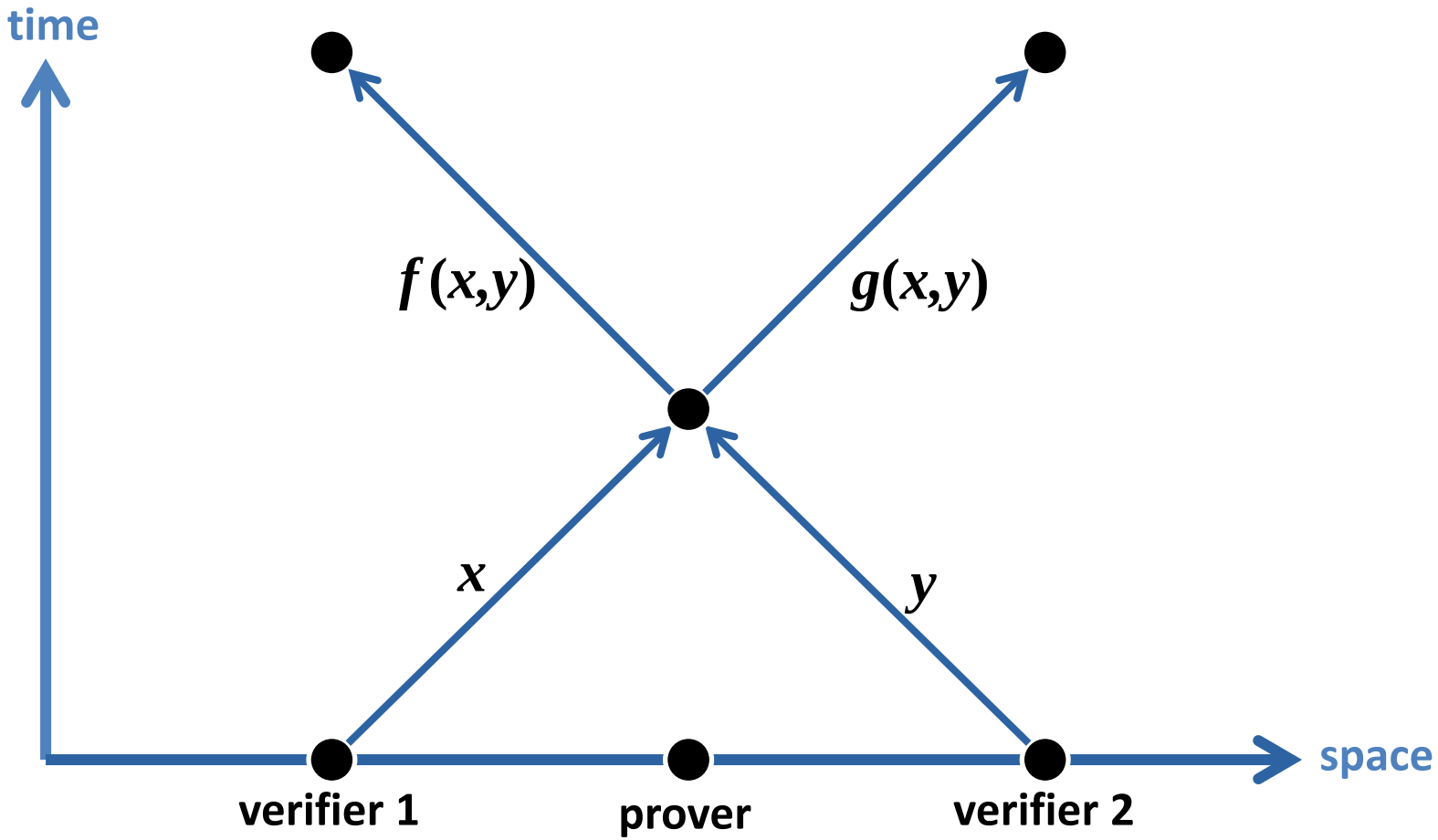
Position Verification



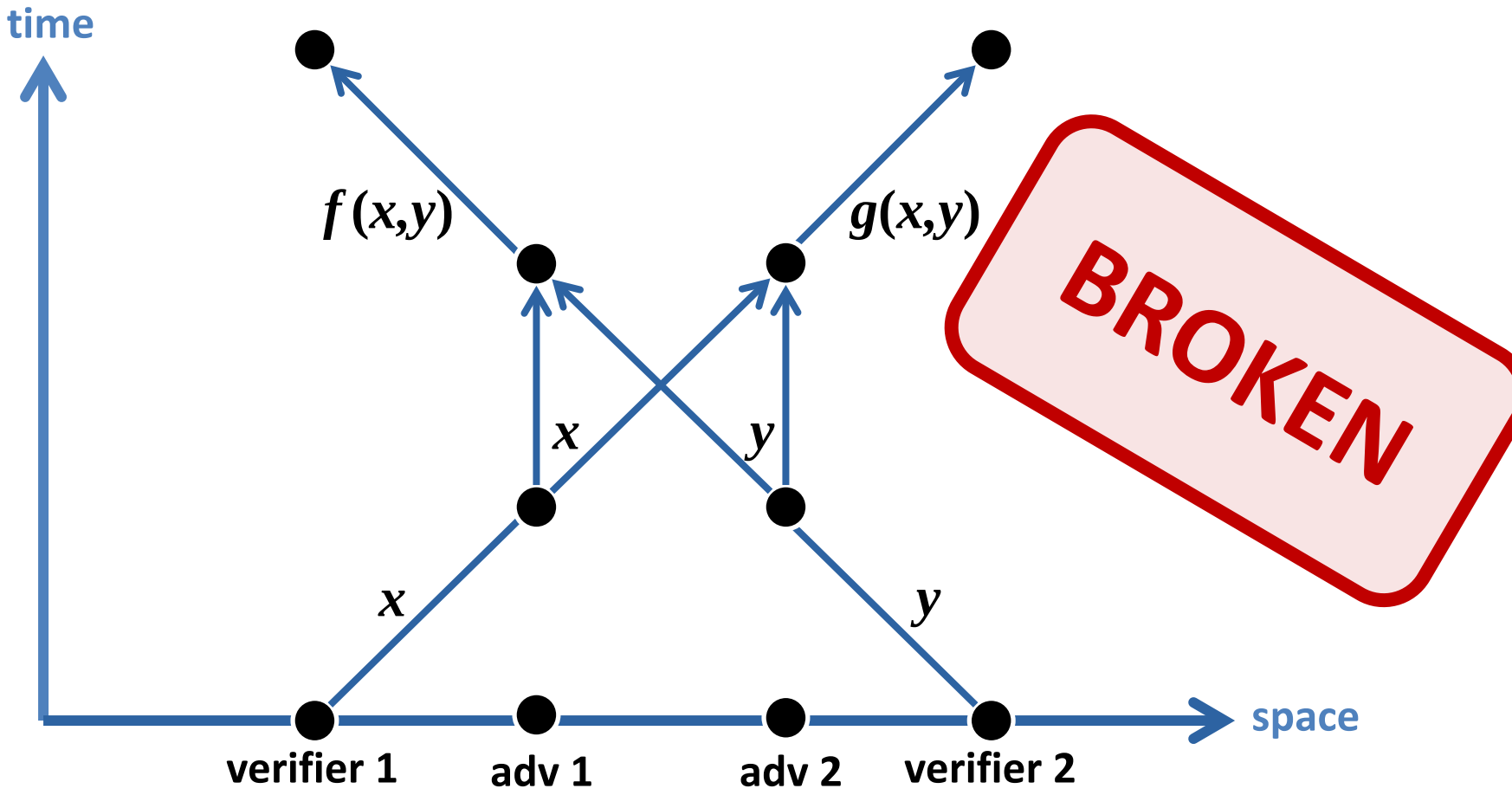
Speed of light

→ Position verified

A generic protocol



A generic attack



Impossibility

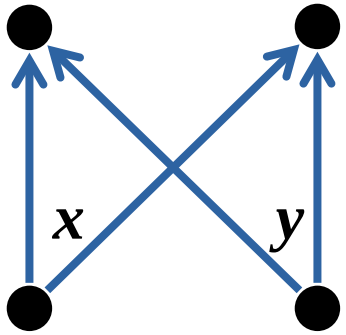
- Applies to 3D-protocols as well
- Any number of verifiers
- Any computational assumptions (exception: transfer capacity limitations)

no mirrors?

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

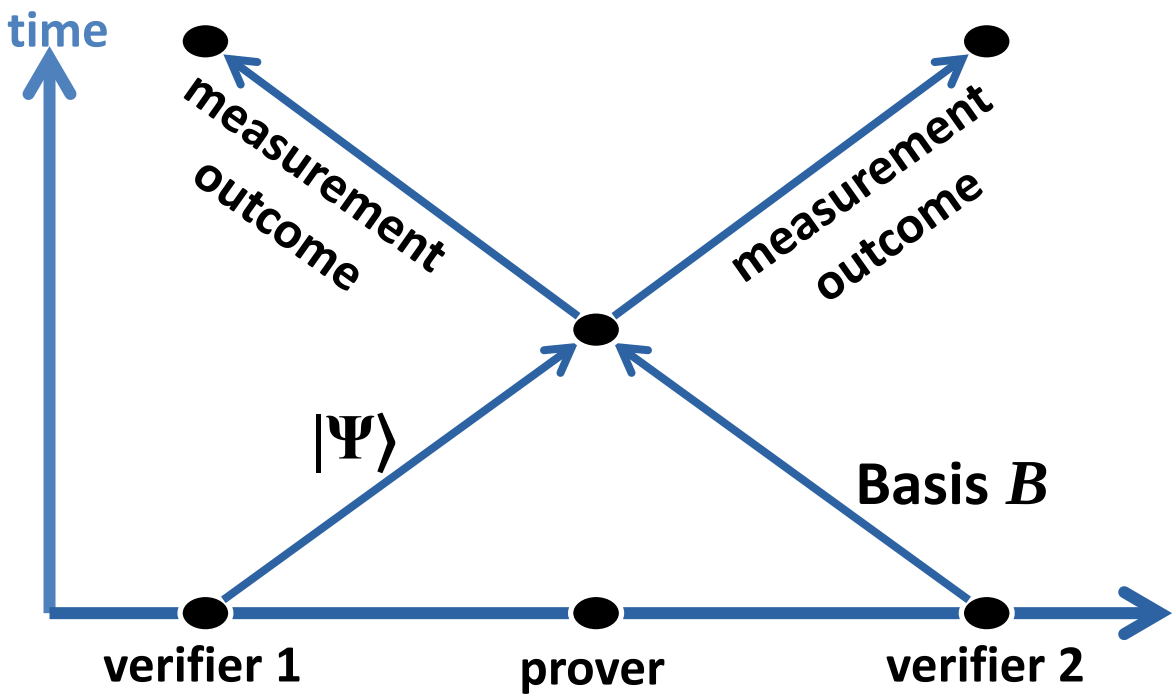
Way out: quantum crypto

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



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

Quantum crypto: A secure protocol

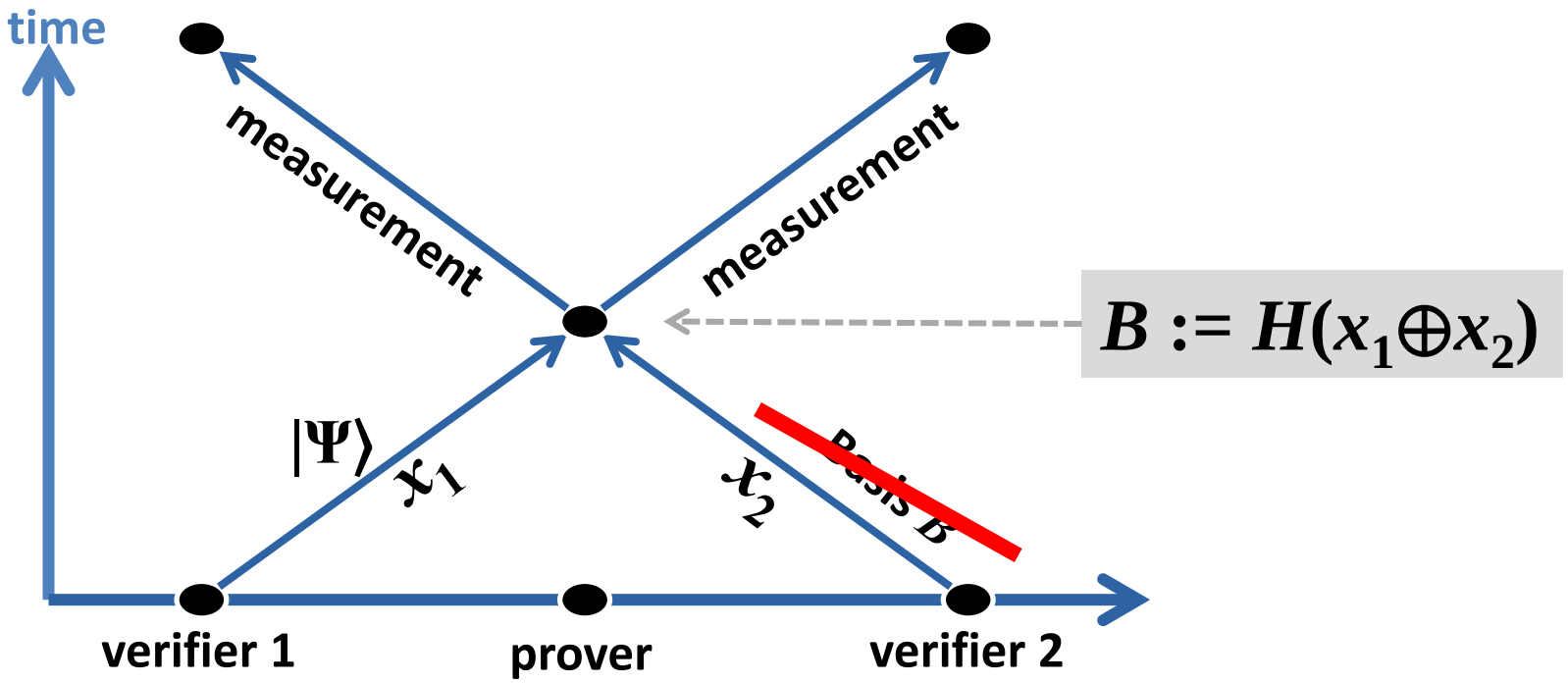


Assumption:
No entangled photons

Only 1D proof

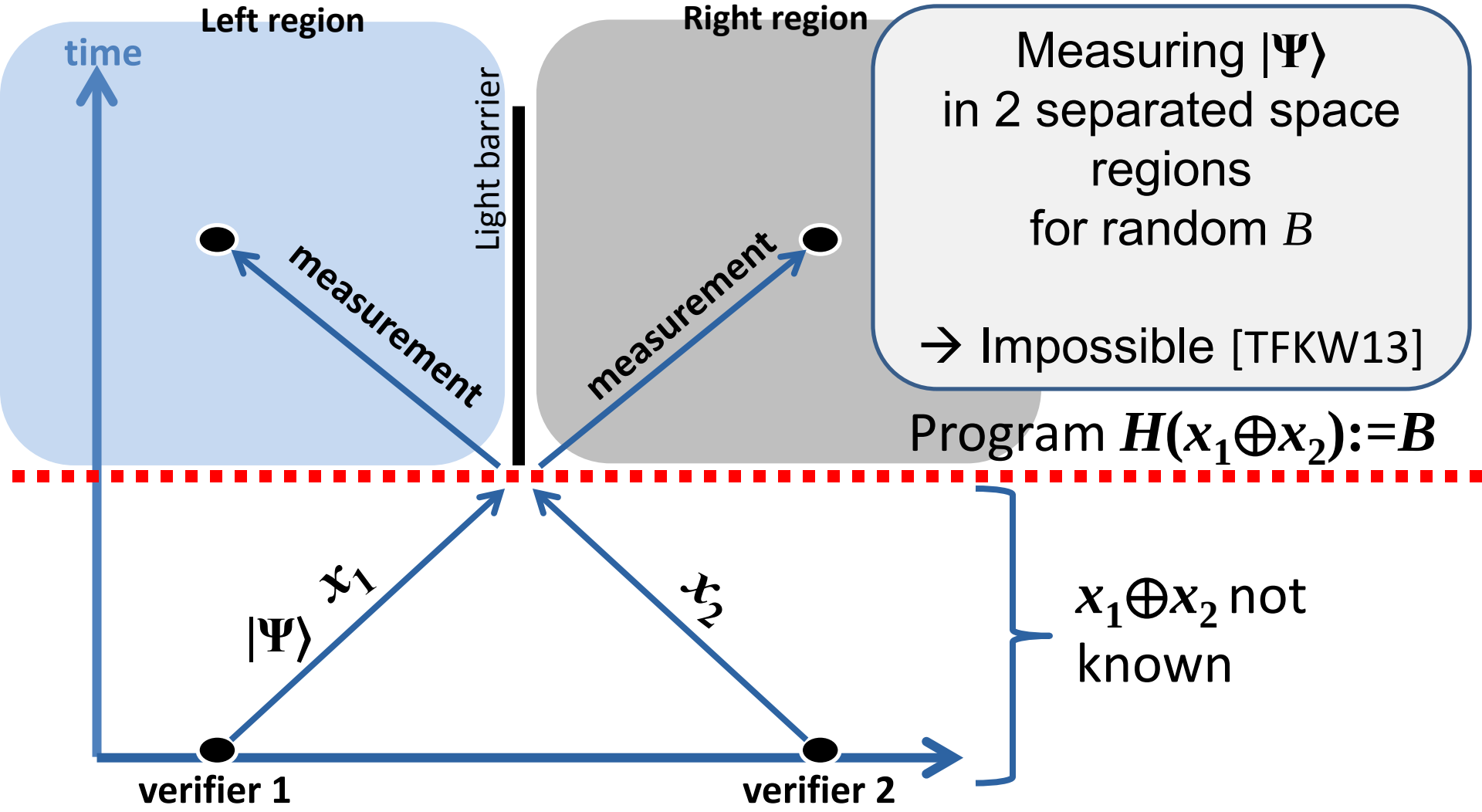
[TFKW13] Tomamichel, Fehr, Kaniewski, Wehner: *One-Sided Device-Independent QKD and Position-Based Cryptography from Monogamy Games*, Eurocrypt 2013 (and [BCF+11])

Our protocol



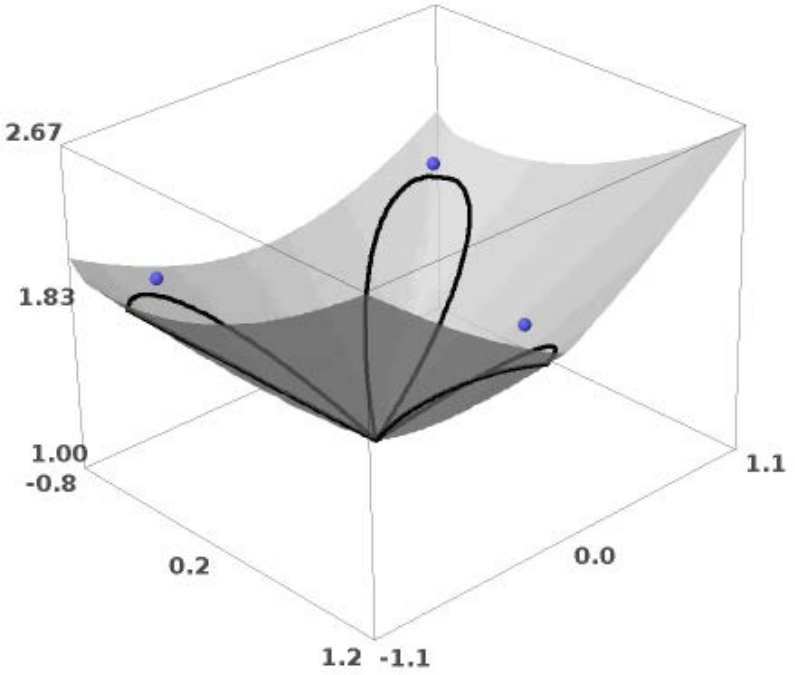
- Avoids attack
- Provably secure (in random oracle model)

Security proof (overview, 1D)



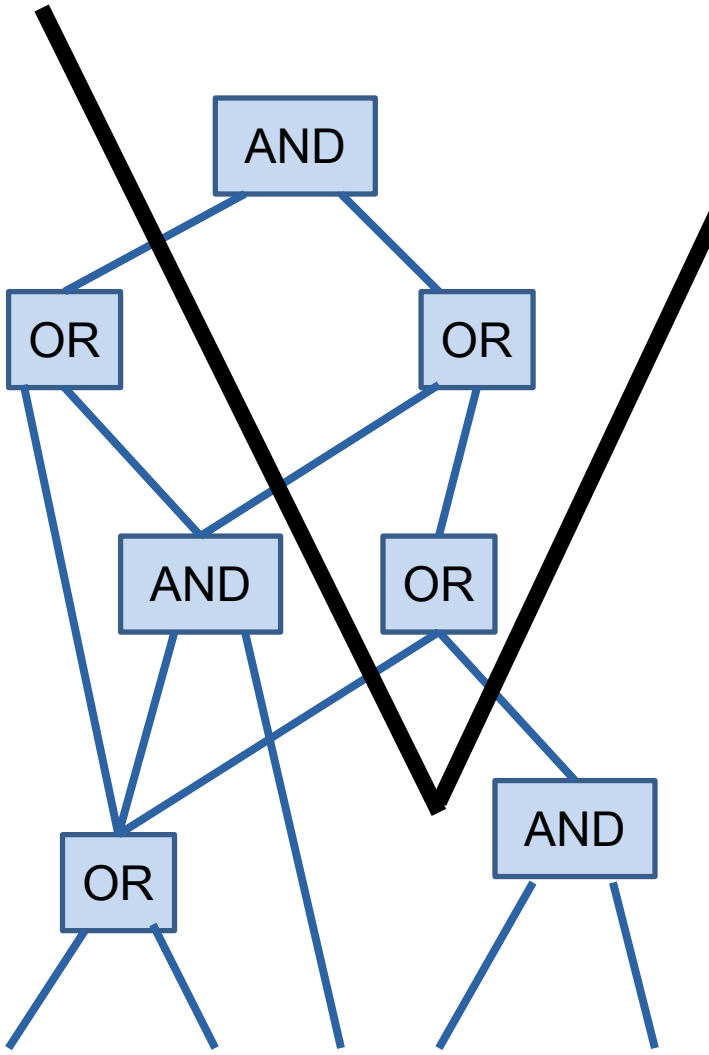
3D case

- 3D proof: regions overlap!
- Need to program RO at different times in different locations!
- Leads to curved "programming surface"
- New tool: spacetime circuits



Proof technique: Space-time circuits

- How to reason about events happening along curved space-time surfaces? Tricky!
- Tool: Space-time circuits
  - No wire leaves light cone
- Then forget about geometry, only connectivity



Open problems

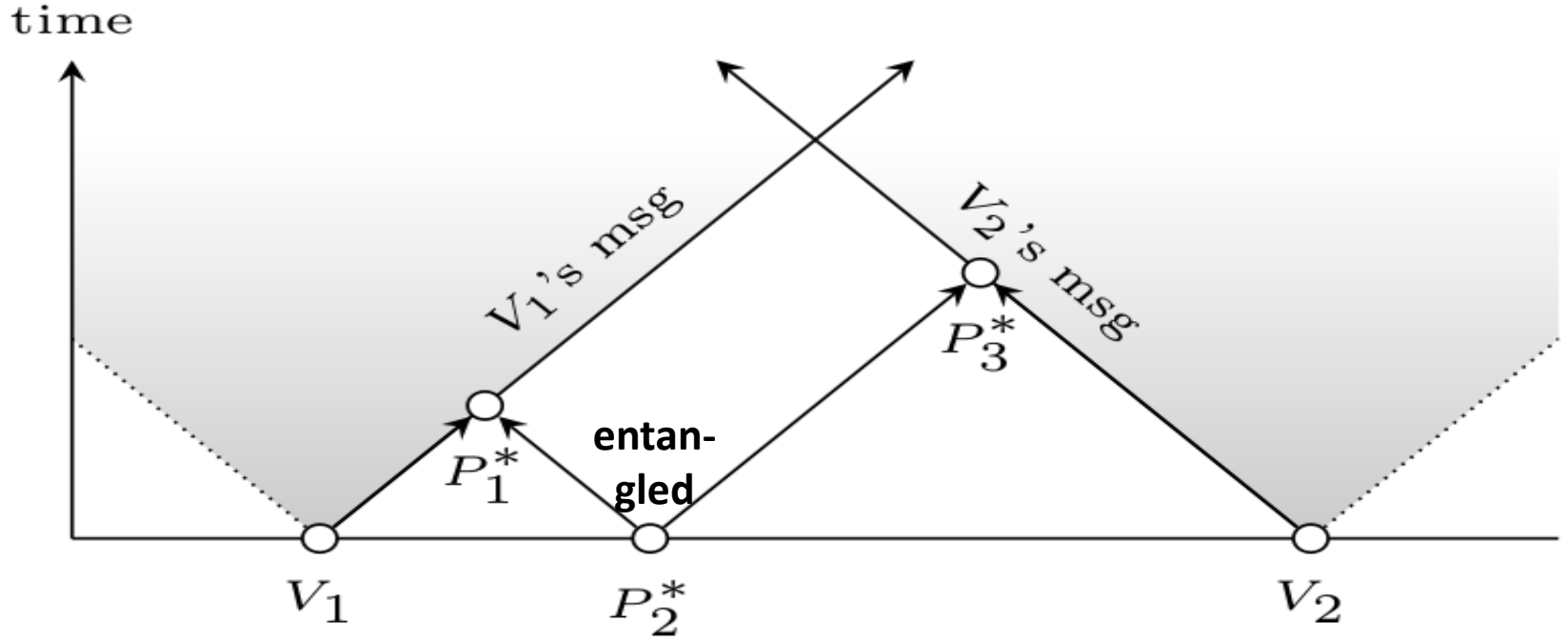
- Improve error tolerance (3.7%)
- Improve precision in 3D case
- Security in standard model (no random oracle)?
  Or even without hardness assumptions?

I thank for your attention

Logo soup

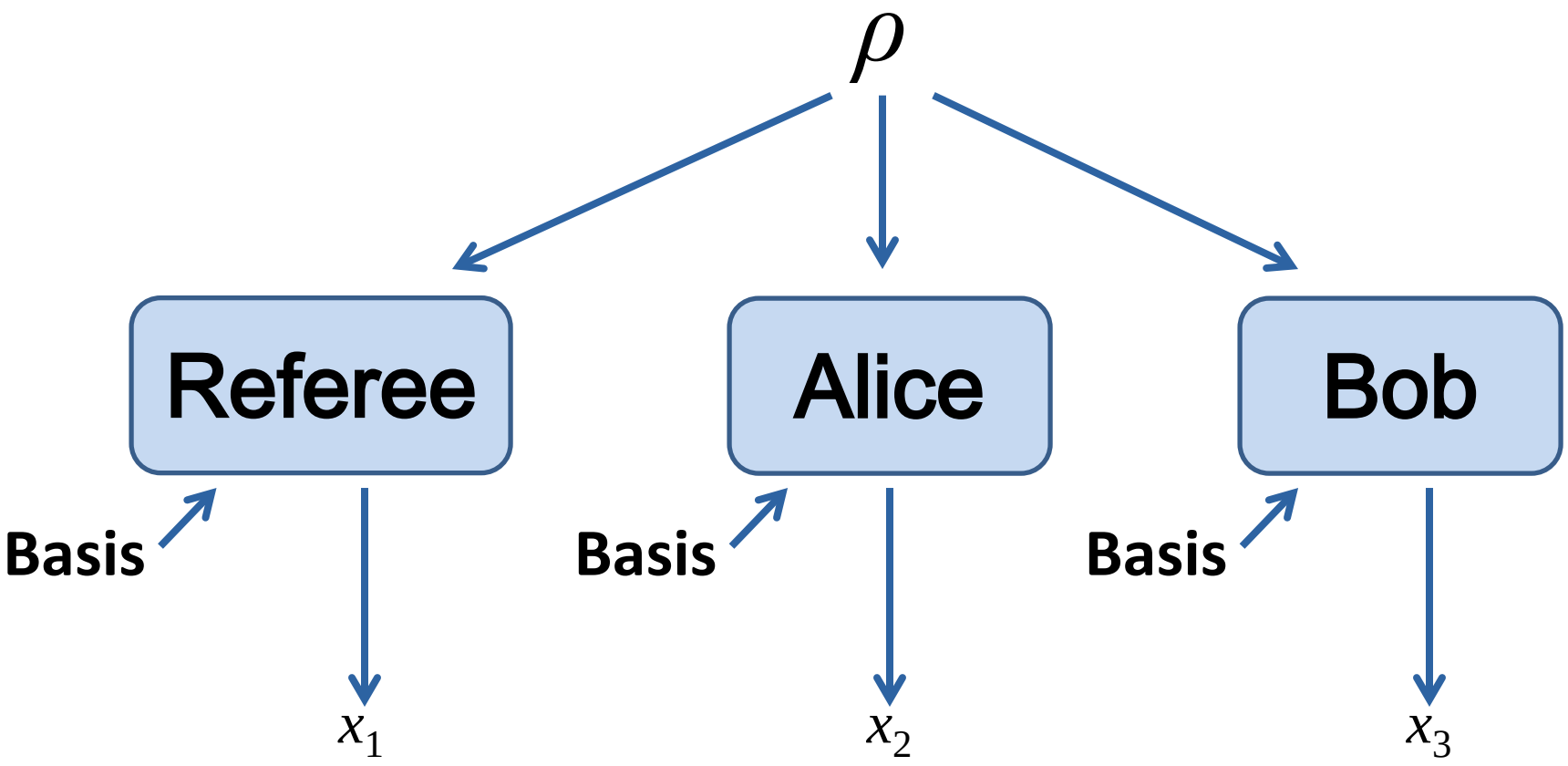
This research was supported by European Social Fund's Doctoral Studies and Internationalisation Programme DoRa

Attack on [TFKW13]



- No entanglement = strong assumption
- Does not work in 3D (bug in [BCF+09] proof)

Monogamy game



$\Pr[x_1=x_2=x_3]$ small

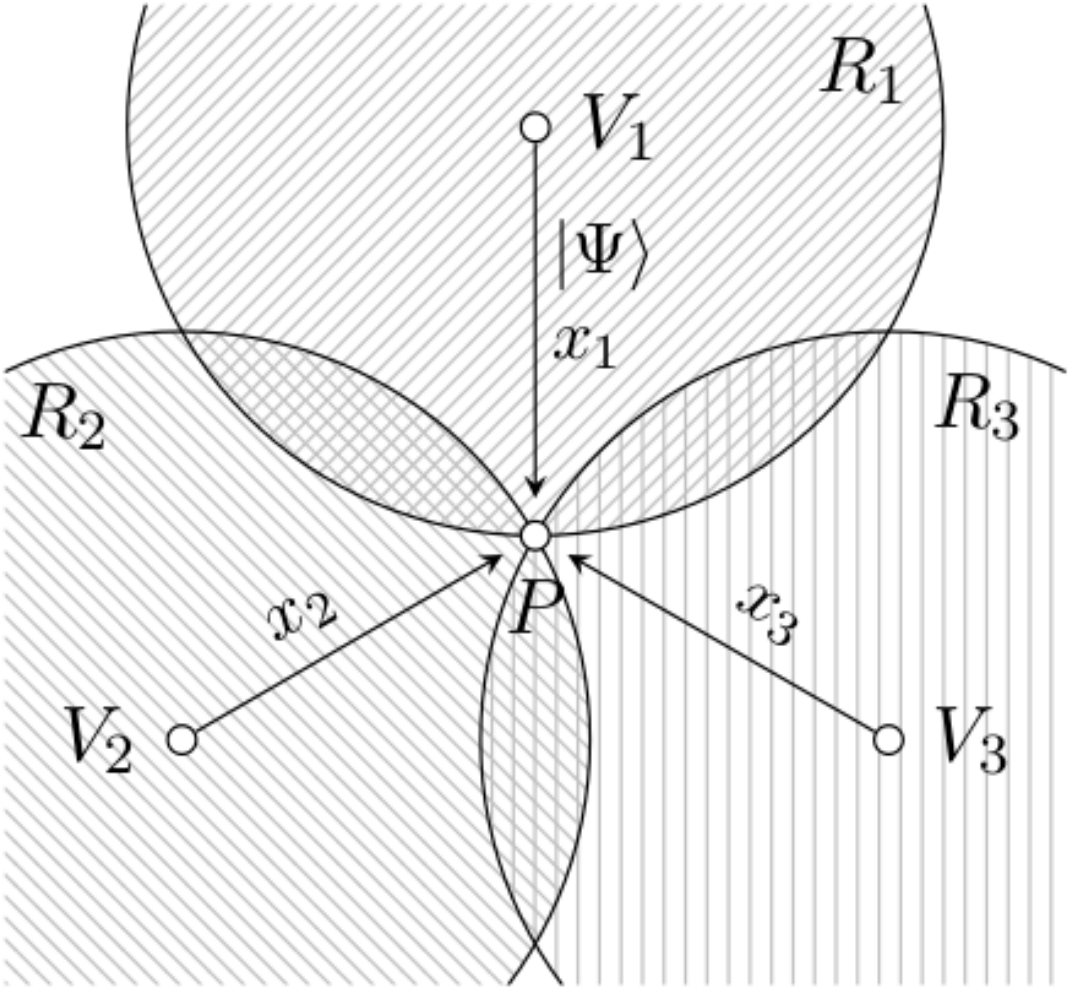
[TFKW13]

Security in higher dimensions?

Programming the random oracle:

When all signals reach honest P (no later!)

Picture: Which space-point reaches which verifier after programming

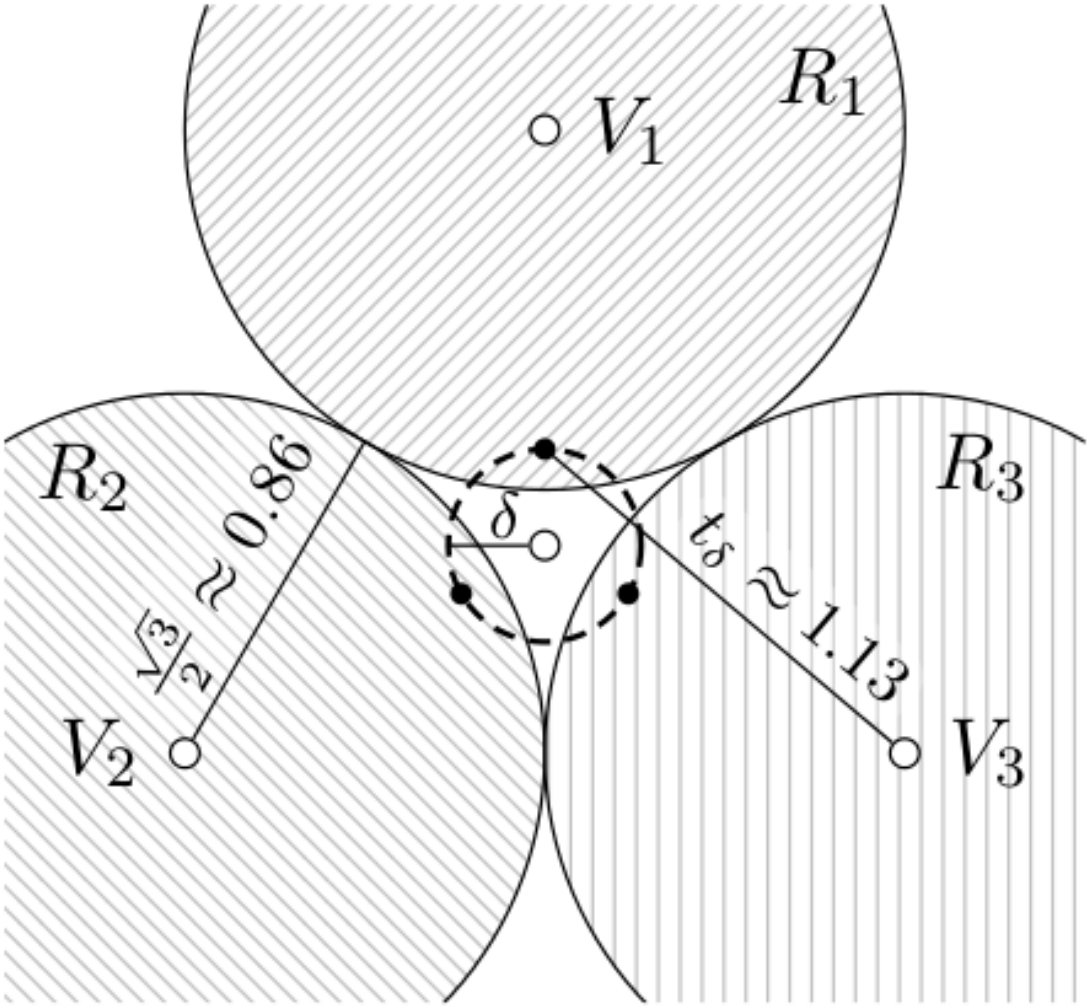


Programming later?

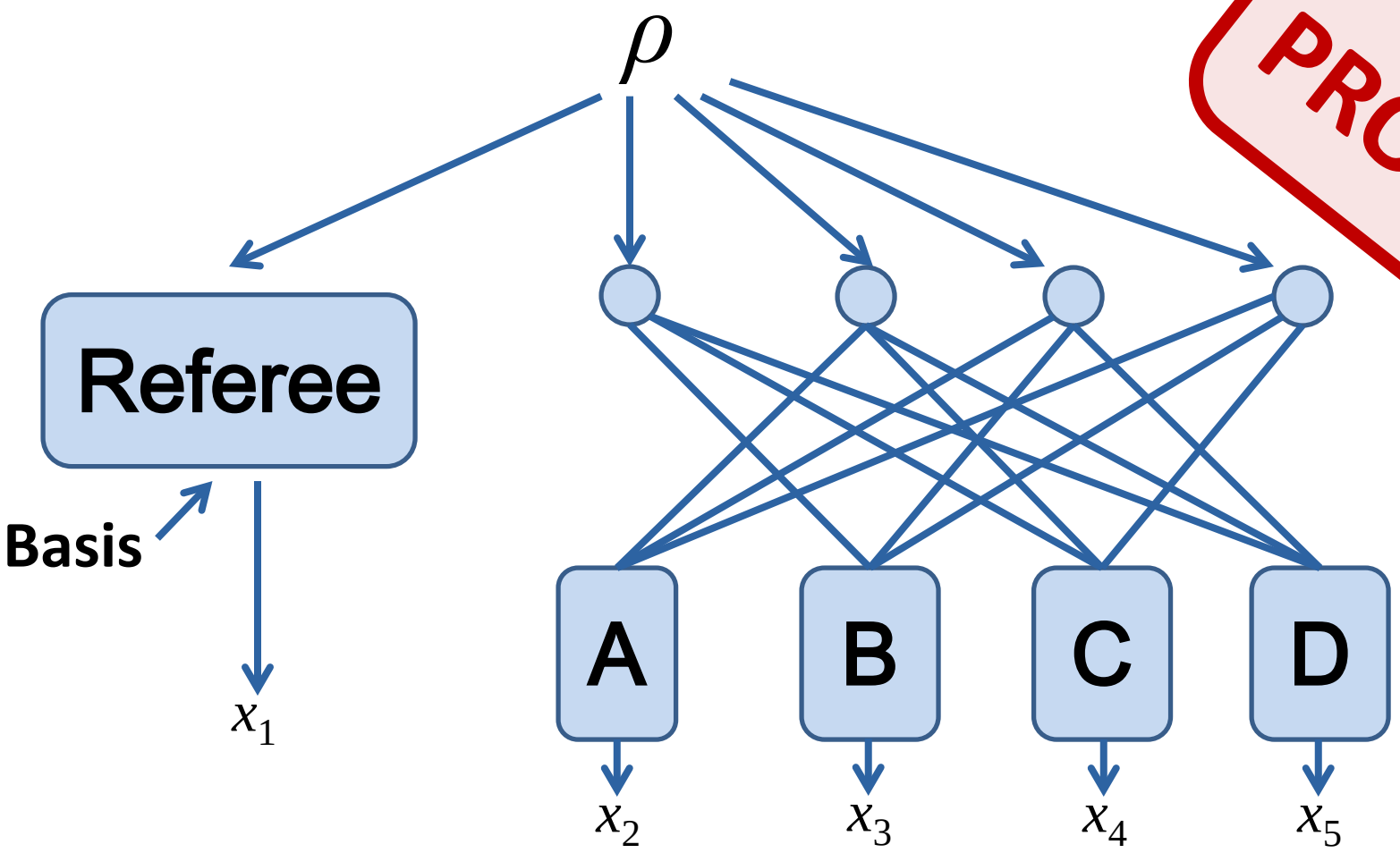
Assume that adv is not in δ radius of P.

Then achieve non-overlapping regions → apply monogamy

Quality:
$\delta = 0.38 * |V\text{-}P|$



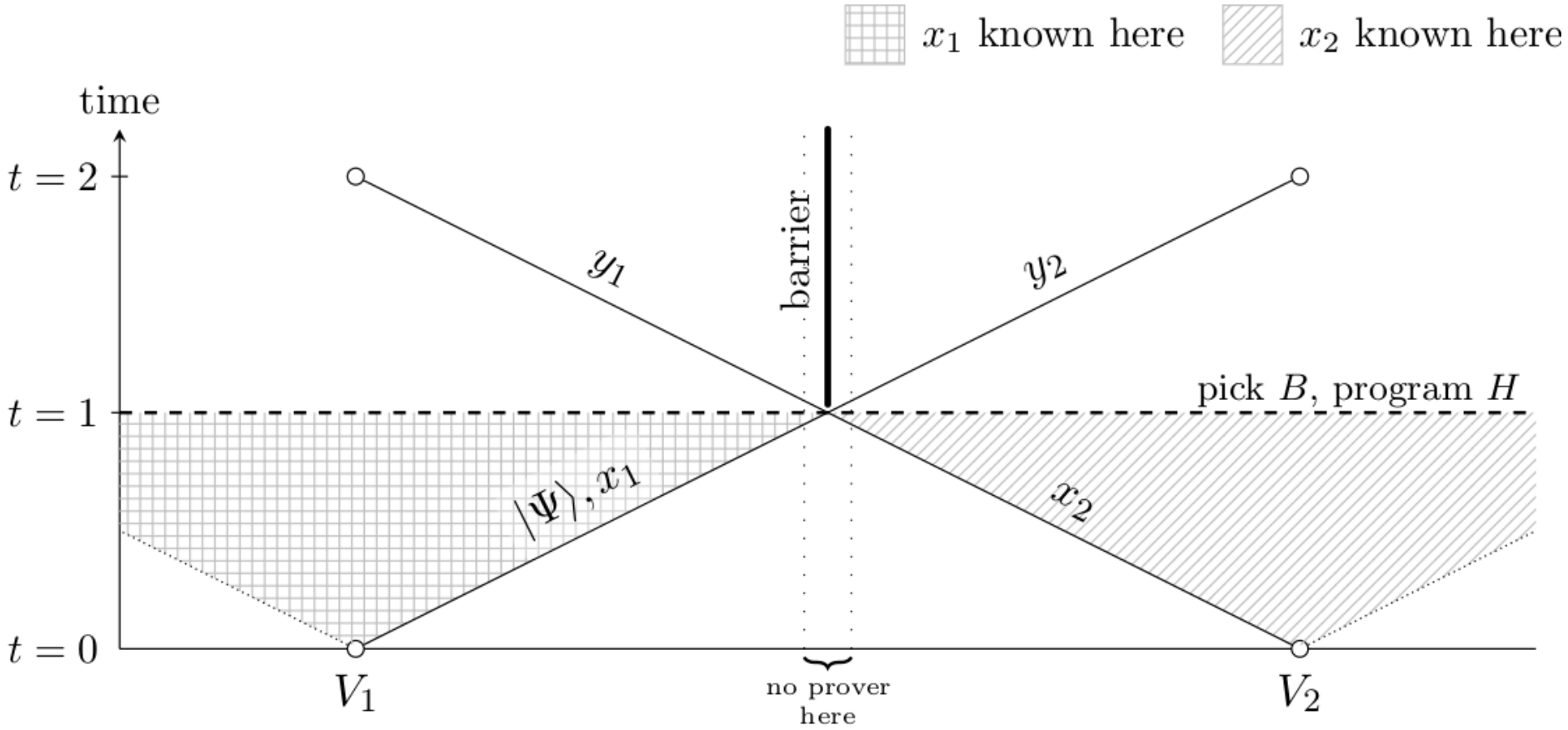
Multiparty Monogamy Game



OPEN PROBLEM

Pr[all x_i equal] small???

Security proof



Result:

- Our protocol is secure if:

Only the honest prover is at a point in spacetime such that:

- Can be reached from all verifiers
- Can reach V_1, V_2

Because monogamy-games for two recipients only

- Geometric condition, e.g. honest prover in the middle of verifier-tetrahedron

Proof technique: Space-time circuits

- How to reason about events happening along curved space-time surfaces? Tricky!
- Tool: Space-time circuits
  - No wire leaves light cone
- Then forget about geometry, only connectivity