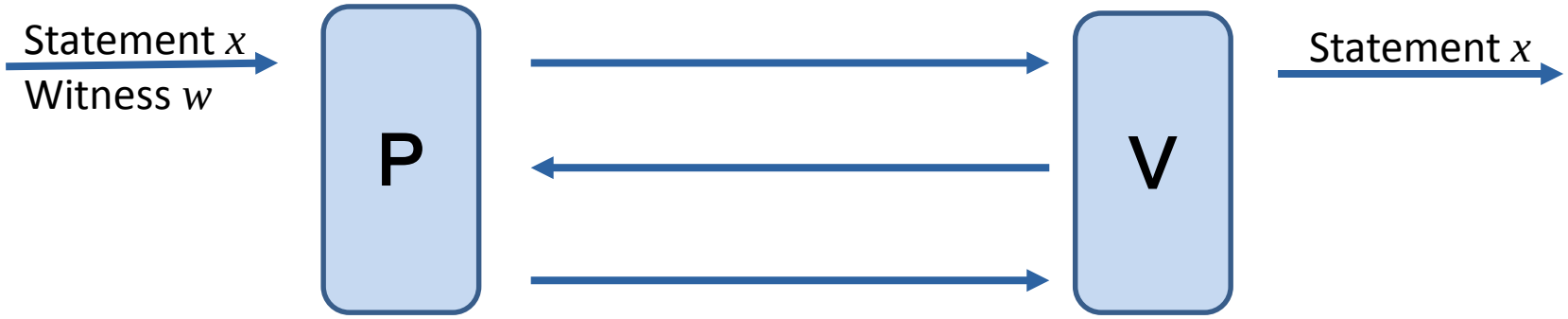
Non-interactive quantum zero-knowledge proofs

Quantum "Fiat-Shamir"

Dominique Unruh

University of Tartu

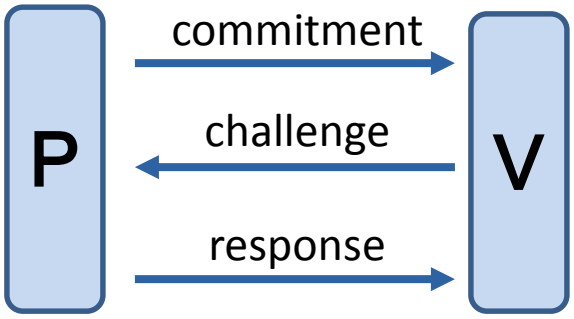
Intro: Proof systems



- **Soundness:** Verifier accepts only true statements
- **Zero-knowledge:** Verifier learns nothing

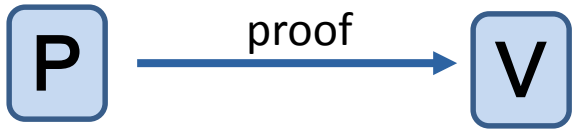
Intro: Proof systems

Sigma-protocols



- Specific 3-round proofs
- Versatile combiners
- Simple to analyze
- Weak security

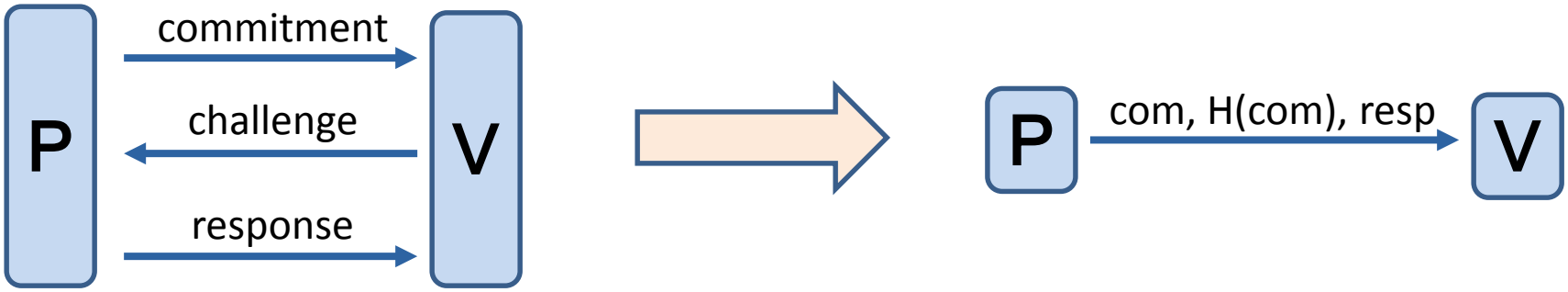
Non-interactive ZK



- Ease of use
  - Concurrency, offline
- Need RO or CRS
- Lack of combiners
- Specific languages

Intro: Best of two worlds

Fiat-Shamir: Convert sigma-proto into NIZK



- Ease of use (concurrent, offline)
- Versatile combiners
- Simple analysis
- Uses random oracle

Intro: Best of two world (ctd.)

- Fiat-Shamir also implies:
  - Sigma-proto → signatures (in RO)

- But: not known to be quantum secure
- Impossibility results [Ambainis, Rosmanis, U]
- Reason: rewinding

NIZK without rewinding?

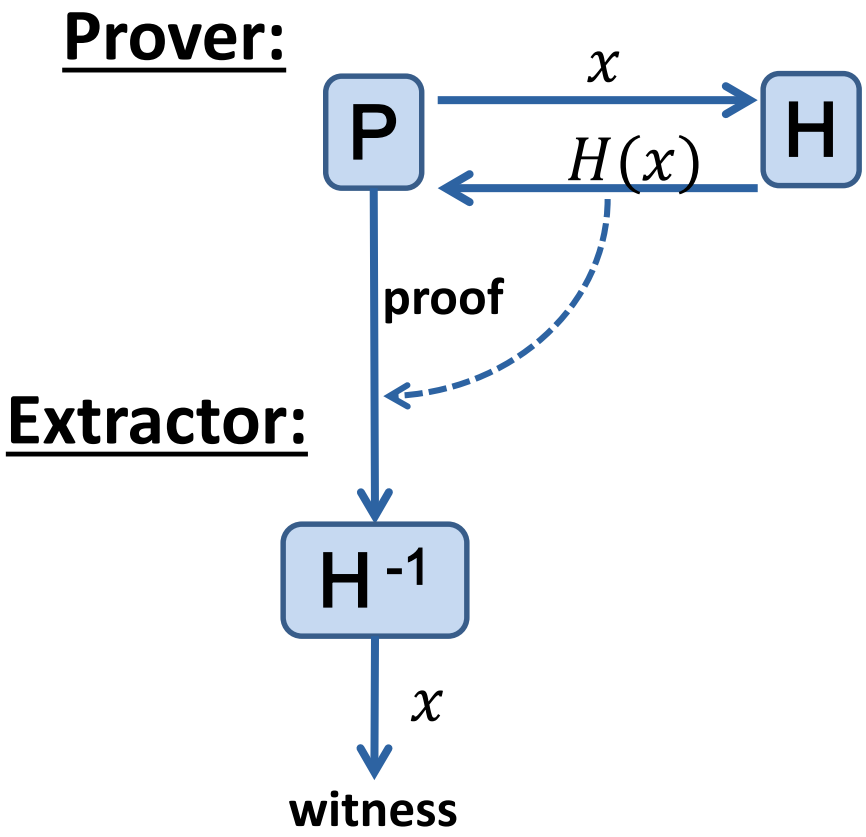
Fischlin's scheme:

- No rewinding
- Online extraction: List of queries → Witness
- But again: No relativizing security proof
- List of queries:
  - Not well-defined: need to measure to get them
  - Disturbs state

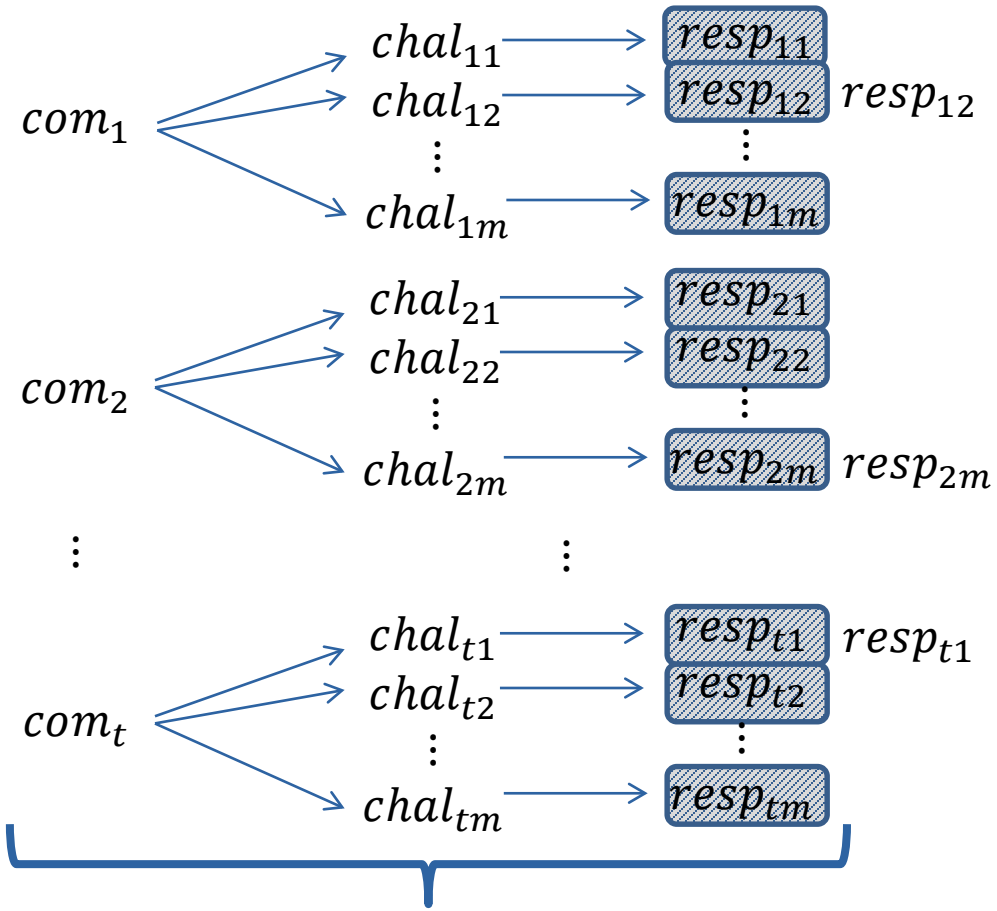
Quantum online-extraction

Idea:

- Make RO invertible (for extractor)
- Ensure: all needed outputs contained in proof



Protocol construction



Hash to get selection what to open (Fiat-Shamir style)

(xxx hash invertibly)

all this together is the proof

- W.h.p. at least one com has two valid $resp$
- Extractor gets them by inverting hash
- Two $resp$ → witness

Invertible random oracle

- Random functions: not invertible
- Zhandry: RO $\approx$ $2q$-wise indep. Function

Idea: Use invertible $2q$-wise indep. function

Problem: None known

Solution: Degree $2q$ polynomials

- Almost invertible ($2q$ candidates)
- Good enough

Final result

Theorem:

If the sigma-protocol has:

- Honest verifier zero-knowledge
- Special soundness

Then our protocol is:

- Zero-knowledge
- Simulation-sound online extractable

Further results

- Strongly unforgeable signatures
  (implied by the NIZK)
- New results for adaptive programming of quantum random oracle
- Invertible oracle trick
  (also used for variant of Fujisaki-Okamoto)

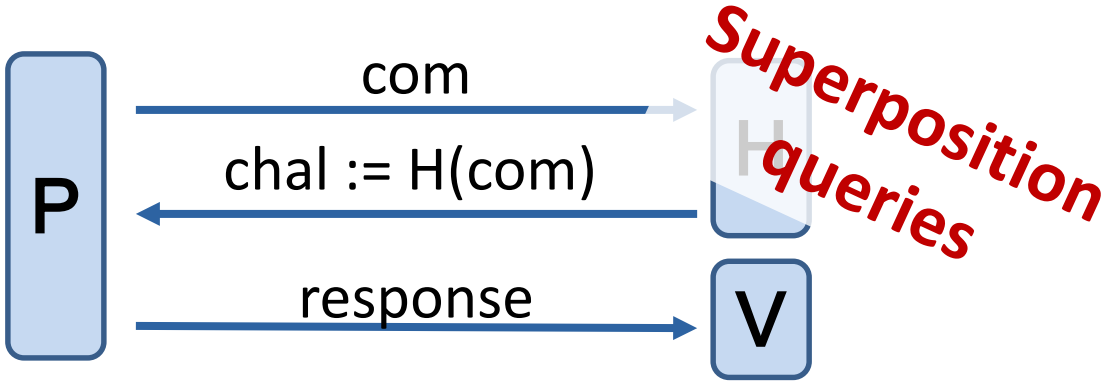
I thank for your attention

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

Quantum Fiat-Shamir soundness

Fiat-Shamir:

Can be seen as:



- Rewinding → Get ~~two responses~~ messed-up state
- "Special soundness" of ~~sigma-proto~~ → ~~Compute~~ witness