Quantum Proofs of Knowledge

Dominique Unruh

University of Tartu

Post Quantum Crypto

- Post Quantum Crypto
  - Classical crypto
  - Secure against quantum computers

- Needs:
  - Quantum hard problems (e.g., lattice crypto)
  - New security proofs

This talk

Zero Knowledge Proofs

Prover

Graphs G and H are isomorphic

Verifier

Permute G

Permuted graph J

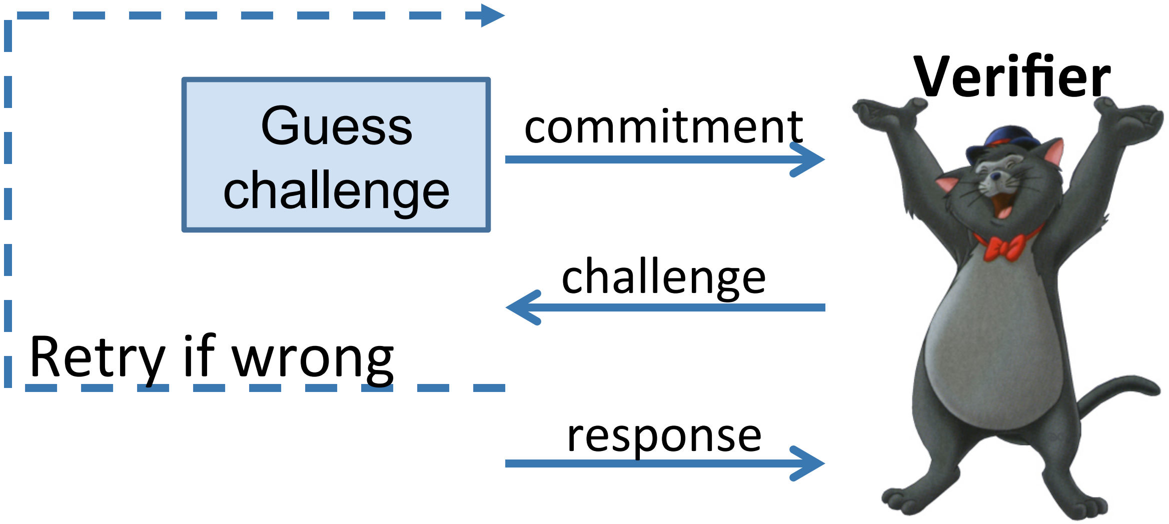
G or H

Pick G or H

Iso between $\boldsymbol{J}$ **and** $\boldsymbol{G}$ or $\boldsymbol{J}$ **and** $\boldsymbol{H}$

Zero-knowledge: how to show?

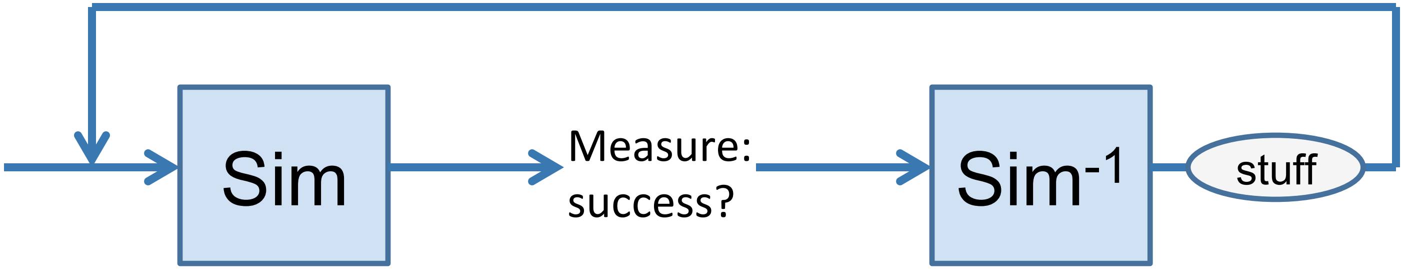
- Given only malicious verifier:
  simulate interaction ⇒ nothing learned



- Quantum case: Rewinding = state copying!

Watrous' quantum rewinding

- Cannot copy state → have to restore it



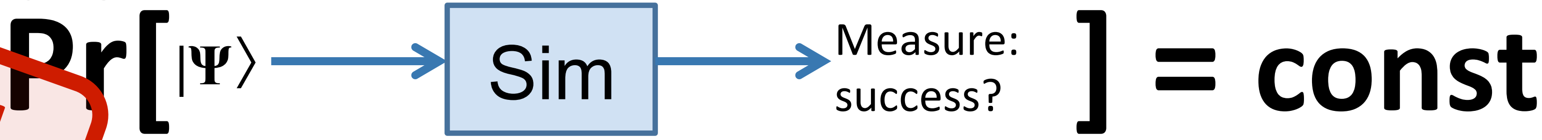
- Variant of amplitude amplification

[Watrous 09]

Limitations of Watrous' rewinding

- Oblivious rewinding:
  When simulator rewinds, he forgets everything

- Success probability independent of initial state



Pr[$|\Psi\rangle$ → Sim → Measure: success?] = const

OPEN PROBLEM

Intuition: success carries no info about $|\Psi\rangle$

Quantum ZK solved?

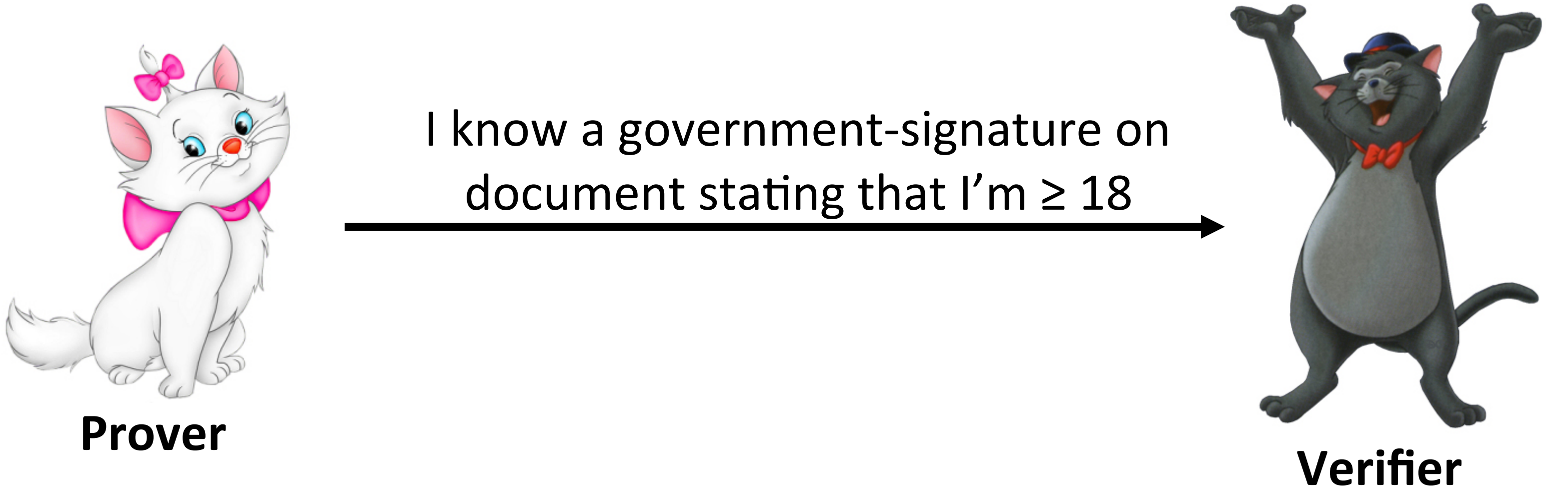
- Watrous' rewinding
  covers many important ZK proofs
- But not all…
  E.g., graph non-isomorphism.

OPEN PROBLEM

- And not: Proofs of knowledge

Proofs of knowledge

- Example: Want to prove age (e.g., e-passport)



I know a government-signature on document stating that I’m ≥ 18

Prover

Verifier

Proofs of knowledge – definition

If prover is successful:

~~prover knows witness~~

~~could output witness~~

there is an extractor that,

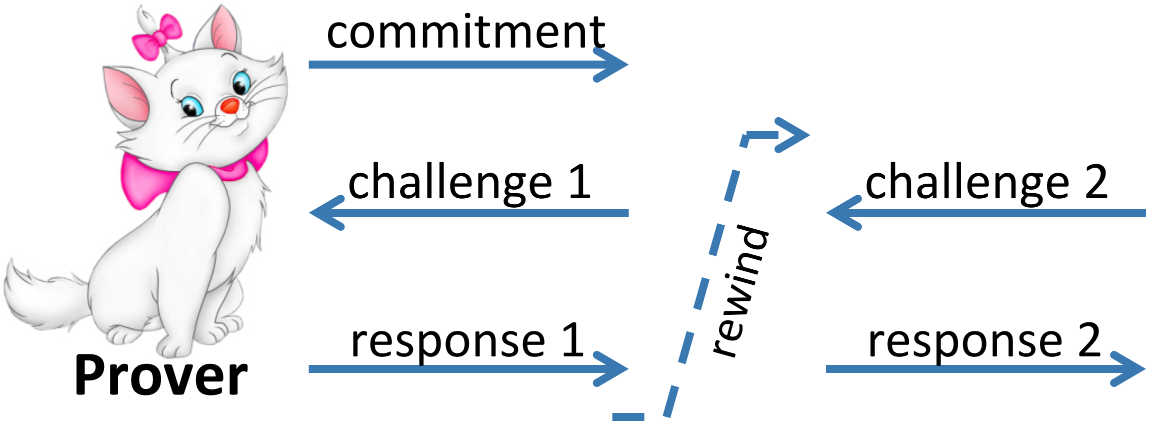
given provers state,

outputs witness

Definition – more formally

- There is a poly time extractor E
- Such that for any malicious prover P^*
- If P^* makes the verifier accept with probability α
- Then E^{P^*} outputs witness with probability $\Omega(poly(\alpha\text{-}const))$.

Constructing extractors



Prover

commitment

challenge 1

response 1

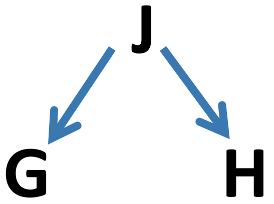
rewind

challenge 2

response 2

“Special soundness”: Two different responses allow to compute witness

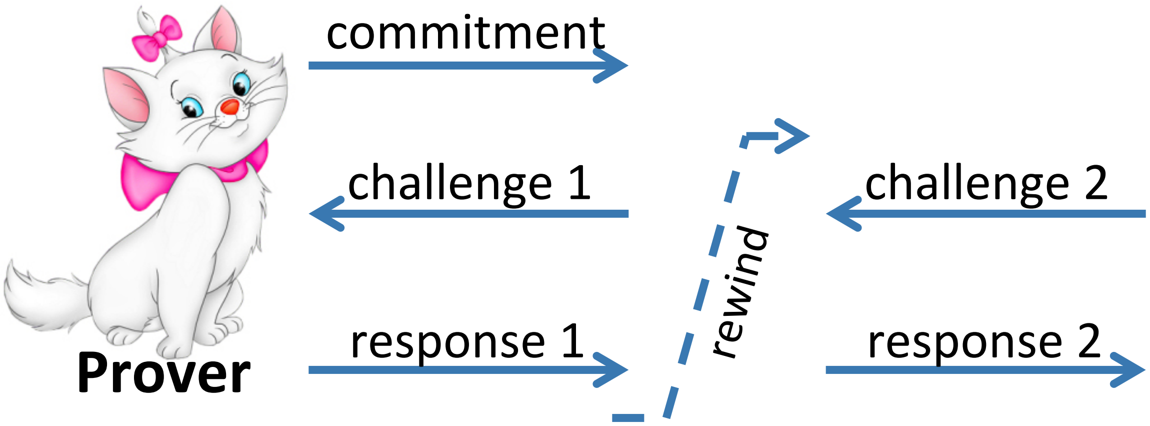
- E.g., isomorphisms from J to G and H give isomorphism between G and H



Quantum extractors?

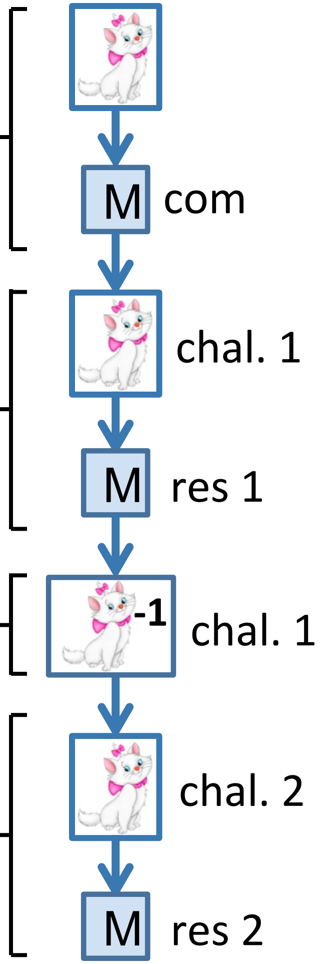
- Quantum case:
  Rewinding = copying. Not possible

- Watrous' "oblivious" rewinding does not work:
  Forgets response 1



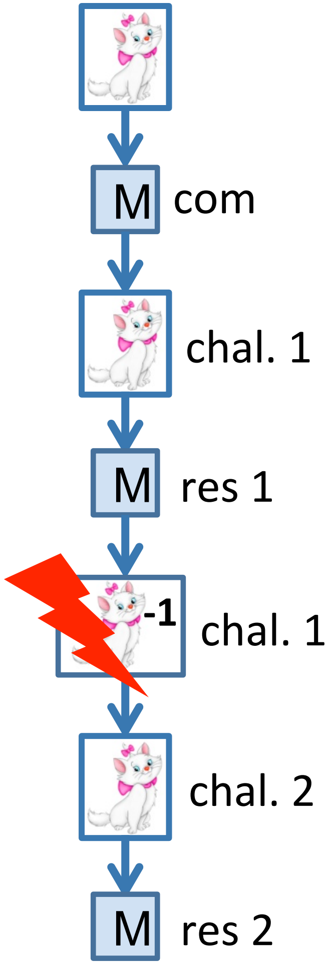
Canonical extractor

1. Run prover, measure commitment
2. Run prover on “challenge 1”, measure response 1
3. Run inverse prover
4. Run prover on “challenge 2”, measure response 2



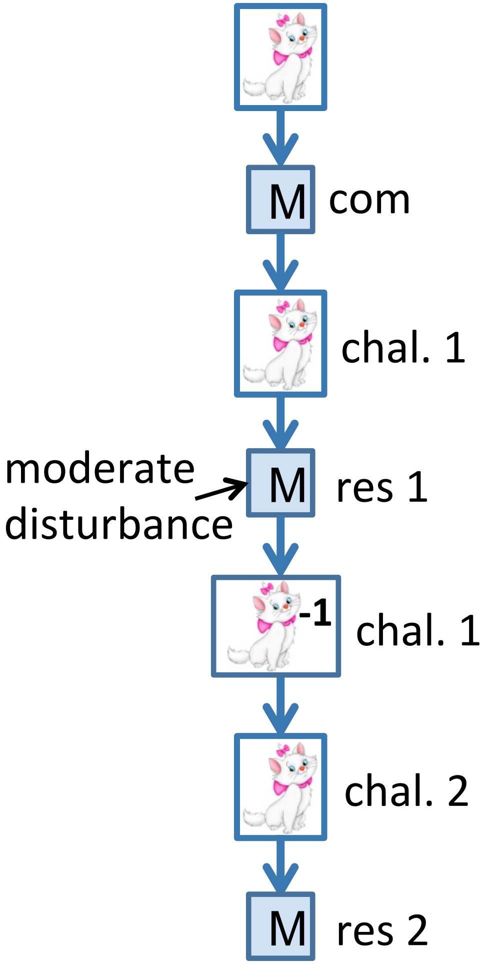
Canonical extractor (ctd.)

- Does it work?
- Measuring “response 1” disturbs state
- Rewinding fails…



Making extraction work

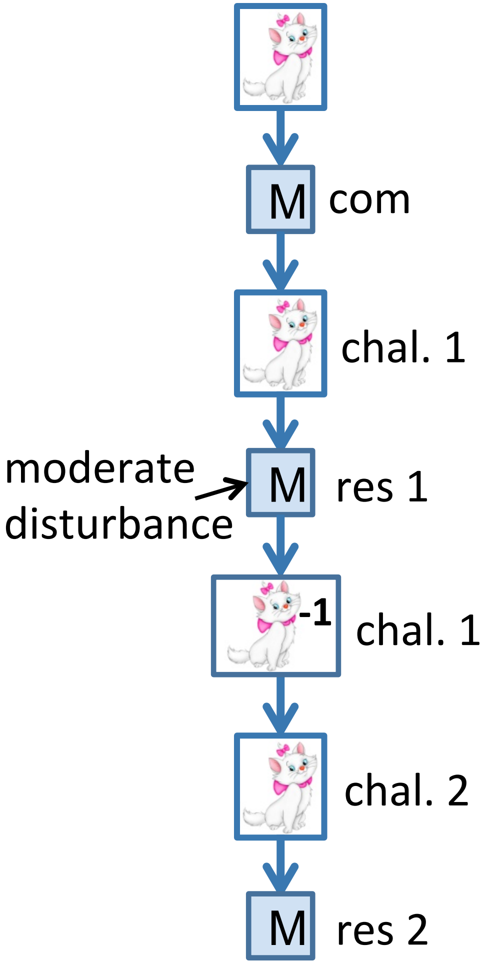
- Thought experiment: “response” was only 1 bit
- Then: measuring “res 1” disturbs only moderately
- Extraction would work



Making extraction work (ctd.)

- Idea: Make “response” effectively be 1 bit
- **“Strict soundness”:** For any challenge, exists at most 1 valid response
- Given strict soundness, canonical extractor works!

OPEN PROBLEM



[Unruh 12]

Main result

Assume: Special soundness, strict soundness

Then

$$\Pr[extract] \geq \left(\Pr[verify] - 1/\sqrt{\#challenges}\right)^{3}$$

- Classical: no √, exponent 2.
- Computational security?

OPEN PROBLEMS

Achieving strict soundness

- Graph Isomorphism proof does not have strict soundness
  - Unless graphs are "rigid"

OPEN PROBLEM

- Discrete log proof has (but uninteresting quantumly)

- Alternative trick (for #challenges poly):
  - Commit to all responses in advance
  - Need: "Strict binding" for unique unveil

Plugging things together

- Proof system for Hamiltonian cycles
- Commitments from injective OWFs

Assuming injective quantum OWFs,

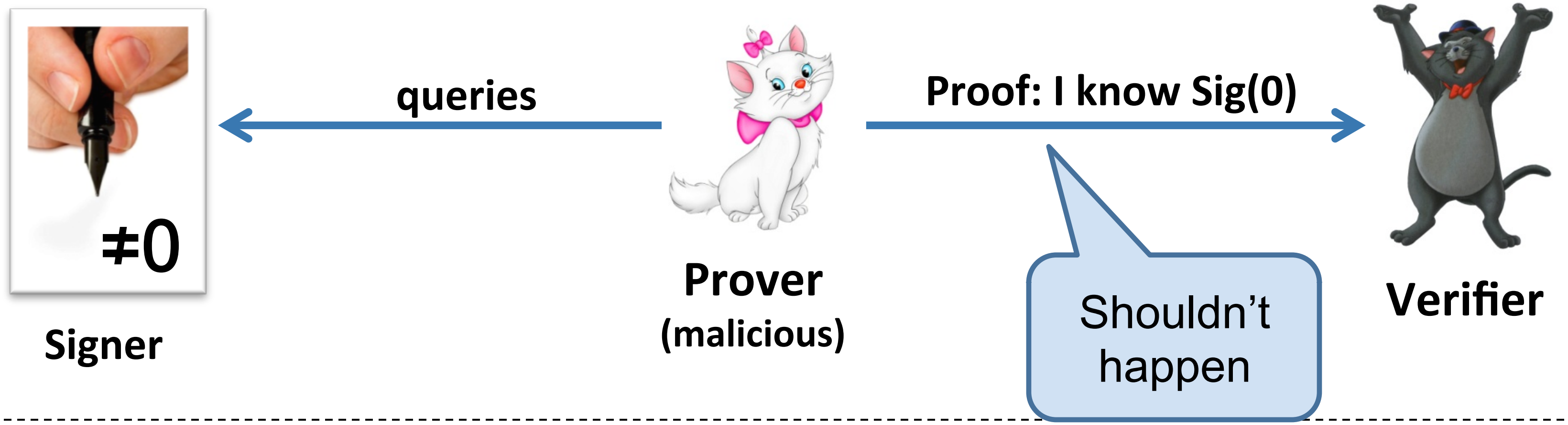
quantum ZK proofs of knowledge

exist for all NP languages

OPEN PROBLEM

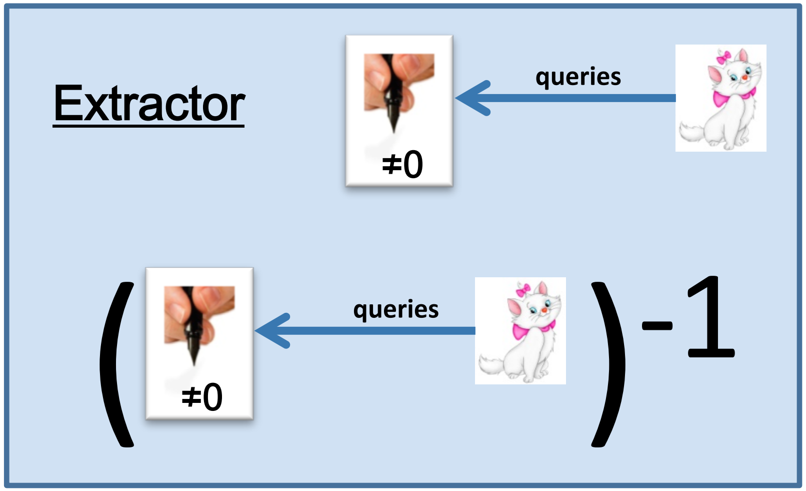
Caveat: No candidates for injective OWFs known.

Using extractors (I)



Shouldn't happen

Proof:

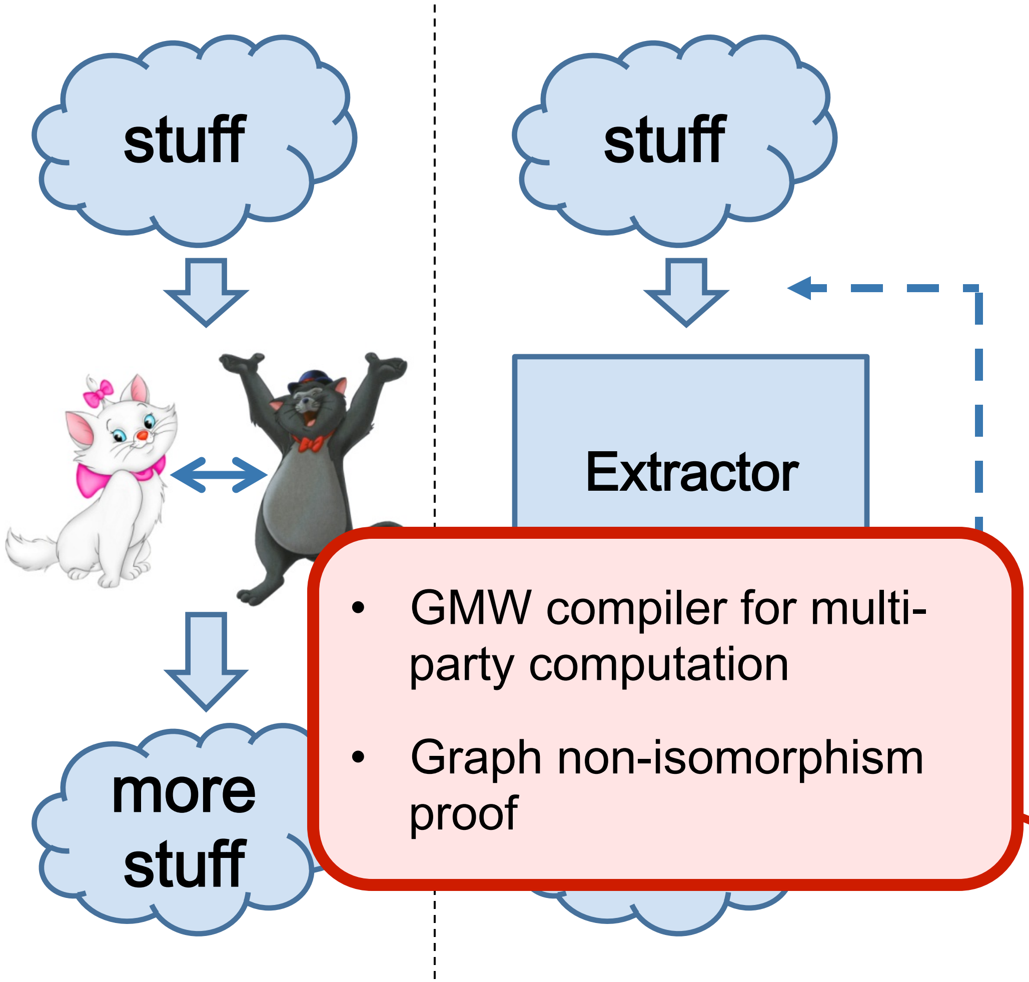


→ Sig(0)

OPEN PROBLEM

Extractor finds Sig(0),
given only Sig(≠0) and $(\mathrm{Sig}(\neq 0))^{-1}$
⇒
~~contradiction~~

Using extractors (II)



- GMW compiler for multi-party computation
- Graph non-isomorphism proof

- Success prob. too low
- Repeat.

- Quantum?
- Watrous? No!
- Success prob. not indep. of state.

OPEN PROBLEM

Conclusions

- ZK and proof of knowledge
  → New challenges in quantum case
- Solved in basic settings, many unsolved issues
  (Challenge: Graph non-isomorphism is ZK)
- Same problems likely to occur in more complex settings
  (e.g., multiparty computation)

I thank for your attention

Logo soup

European Union
European Social Fund

Investing in your future

ARCHIMEDES

DoRa

European Union
Regional Development Fund

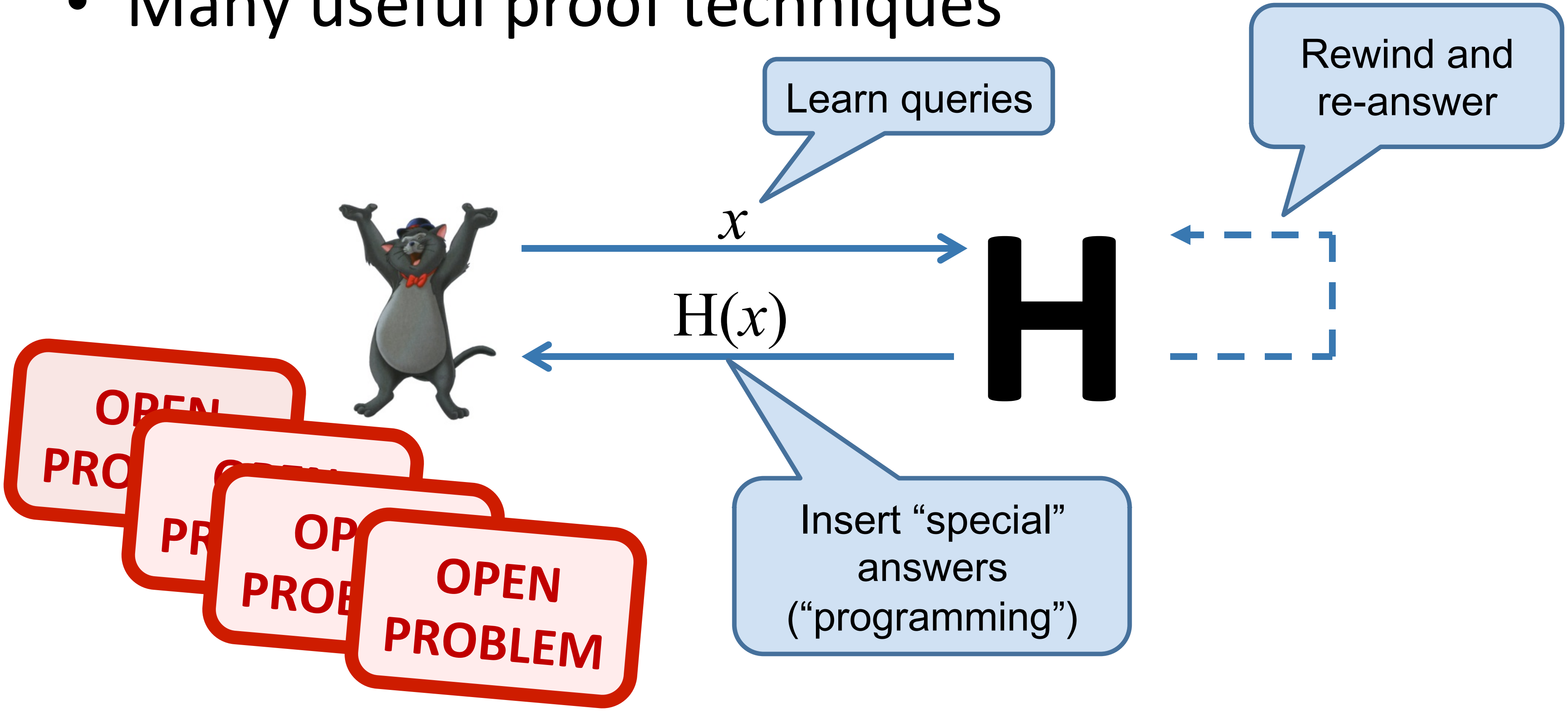
Investing in your future

EXCS
ESTONIAN COMPUTING

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

Random Oracles

- Model hash function as **random function H**
- Many useful proof techniques



Learn queries

Rewind and re-answer

Insert “special” answers (“programming”)

Limited programming of RO

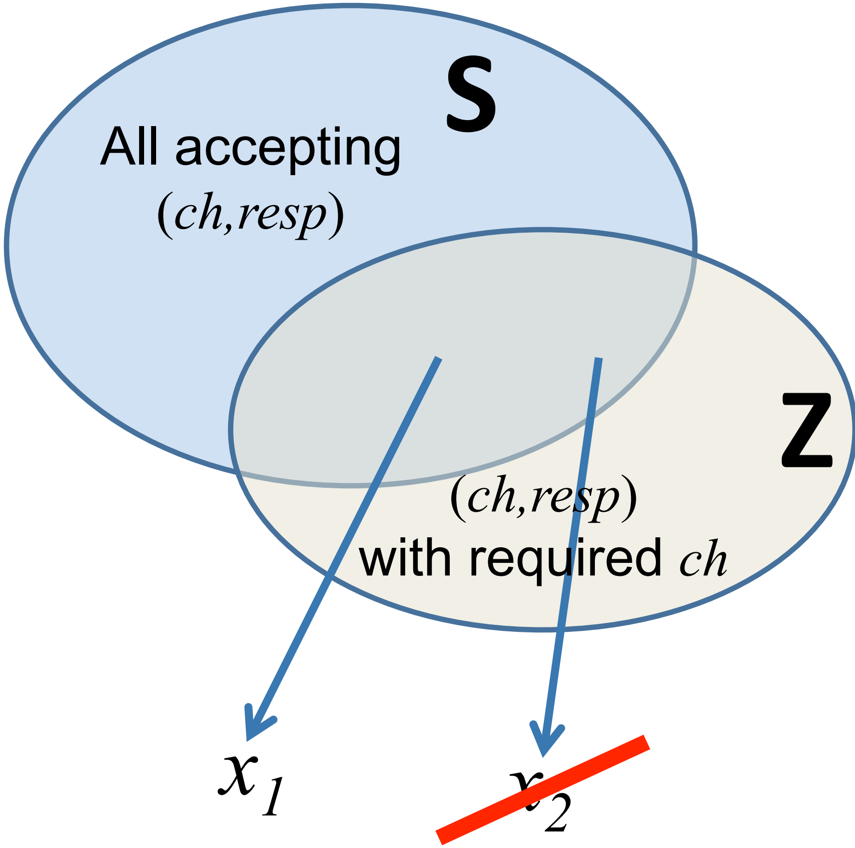
- Want to give answer $\mathrm{H}(x)=y_{special}$
- Don’t know which x is queried

- Solution: Put $y_{special}$ in many (not too many) images of H
- With noticeable probability:
  Exactly one query hits $y_{special}$
- Even works quantumly [Zhandry 12]

WORK IN PROGRESS!

Necessity of strict soundness

- Given a set S
- can encode it as a quantum state $|\Psi\rangle$
- s.t. for any set Z
- you find one $x_1 \in S \cap Z$
- but not two $x_1, x_2 \in S$


S
All accepting
$(ch,resp)$
Z
$(ch,resp)$
with required ch
x_1
~~x_2~~