

# Quantum Attacks on Classical Proof Systems

## The Hardness of Quantum Rewinding

Dominique Unruh

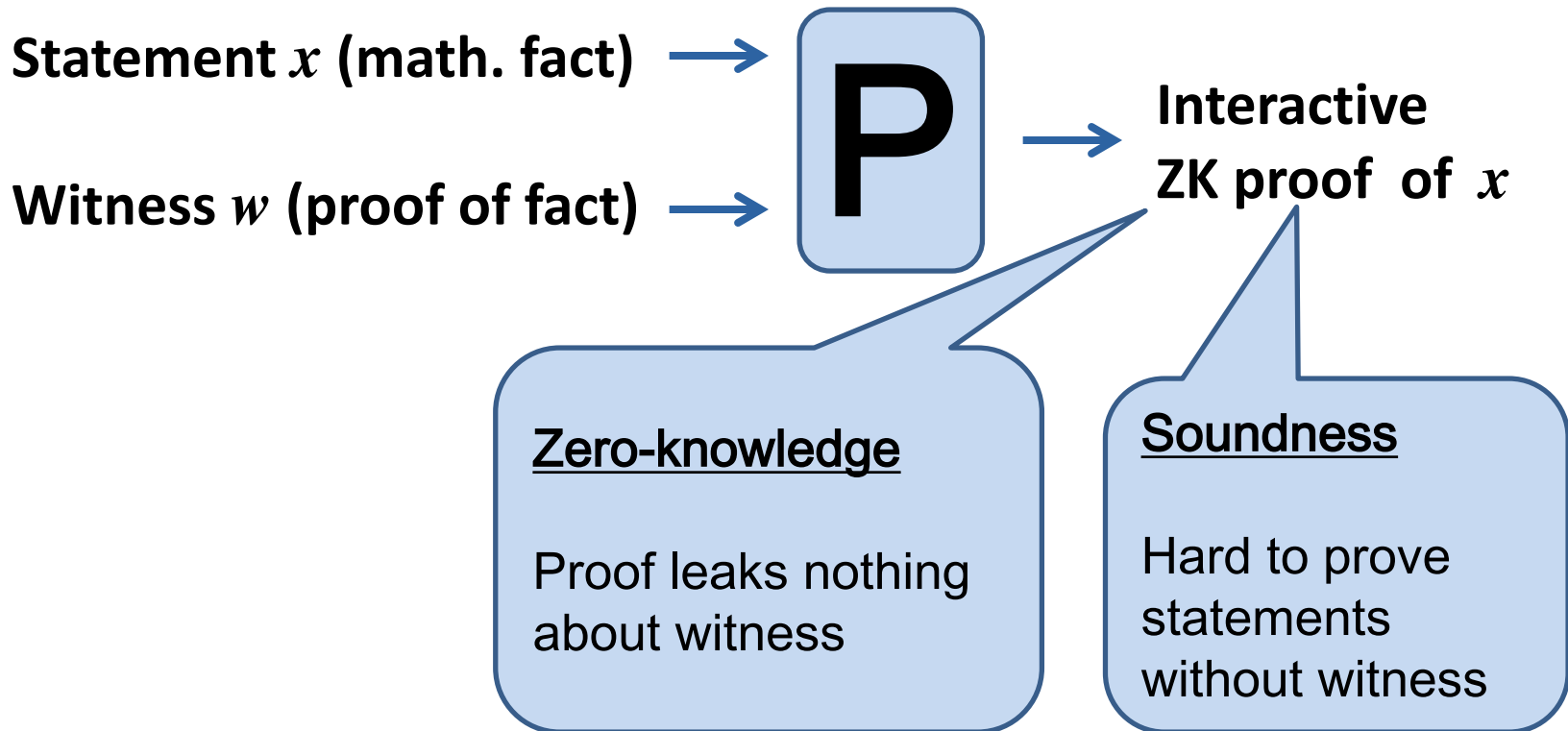
University of Tartu

With Andris Ambainis, Ansis Rosmanis

# Classical Crypto

**(Quick intro.)**

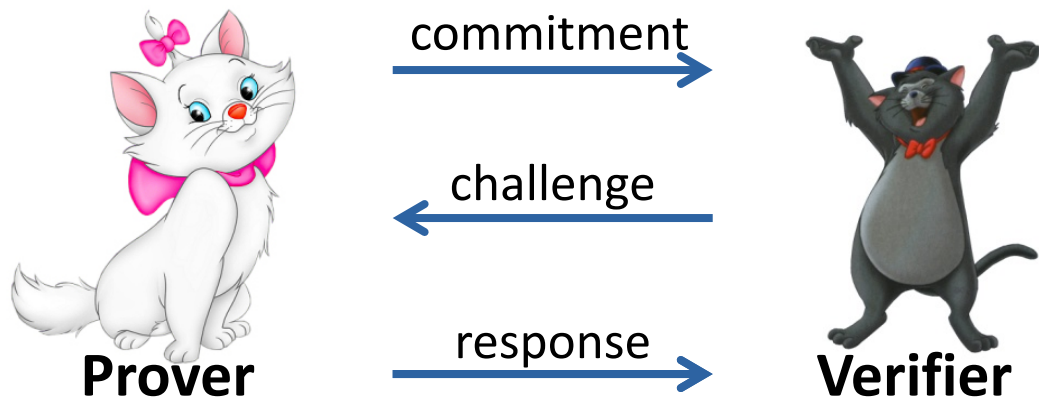
# Zero-knowledge proofs (of knowledge)



**Uses:** Proving honest behavior, drosophilia of crypto, ...

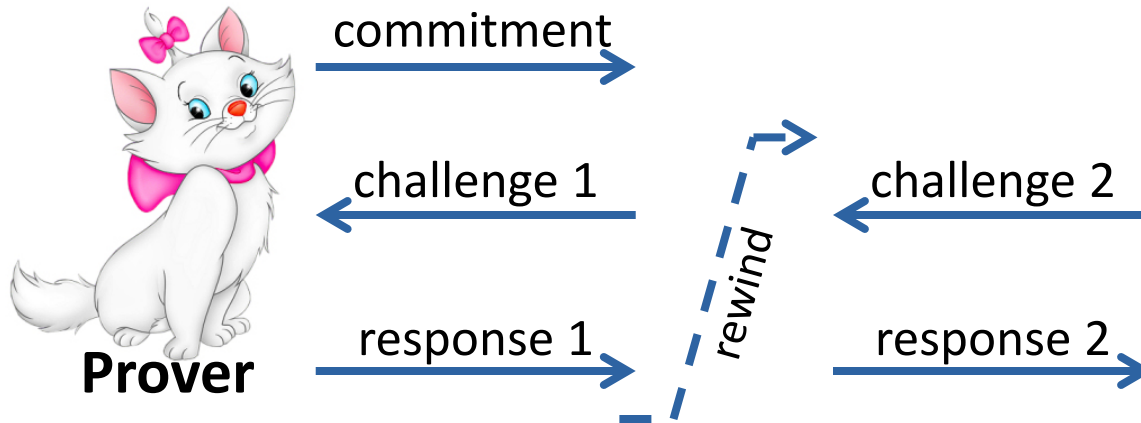
# Towards efficient ZK: Sigma protocols

---



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

# Proving soundness



**Special soundness** → We extract the witness  
 → Correct proof implies knowledge of witness

**Classical security easy.**

# Quantum!

**But if adversary has a  
quantum computer?**

# Impossibility result

---

There is a sigma-protocol

- with special soundness
- that is not sound

(Relative to some oracle.)

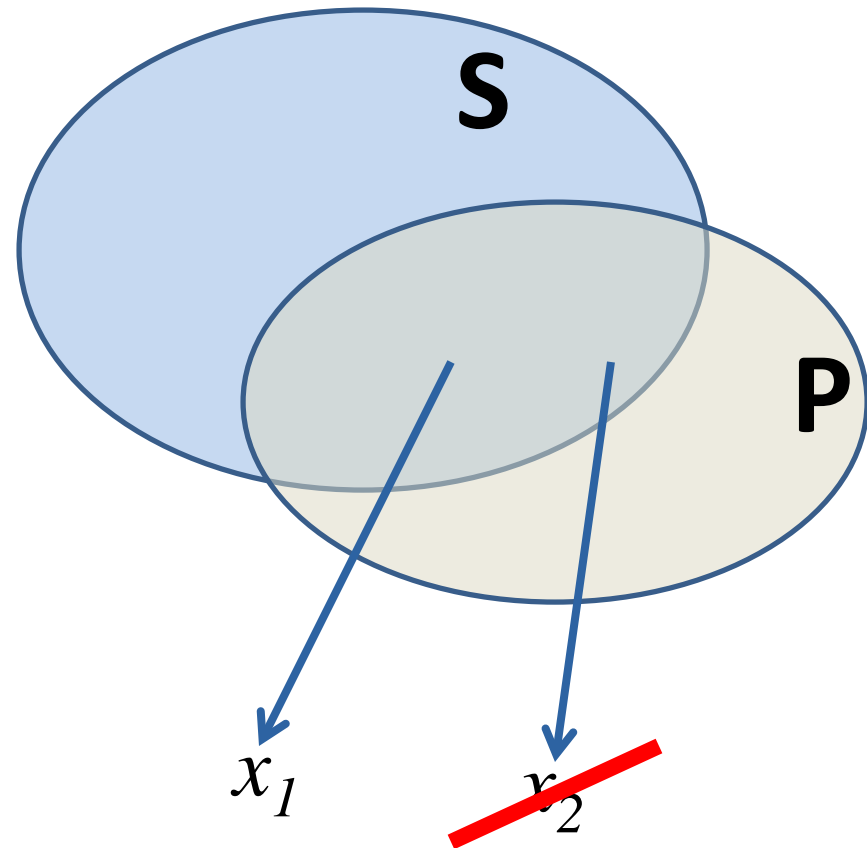
## Consequence:

A classically secure sigma-protocol  
may be quantum insecure\*

\* See terms and conditions for oracle-separations

# The “pick-one trick” (simplified)

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



[Up to some constraints]



# Pick-one trick: Finding $x_1 \in S \cap P$

## Grover's algorithm

- Create

$$|\Psi\rangle := \sum_x |x\rangle$$

- Repeatedly apply:

$$I - 2|\Psi\rangle\langle\Psi|$$

and stuff.

- Get:  $x \in P$

## Picking $x_1$

- Create

$$|\Psi\rangle := \sum_{x \in S} |x\rangle$$

- Repeatedly apply:

$$I - 2|\Psi\rangle\langle\Psi|$$

and stuff.

- Get:  $x \in P \cap S$

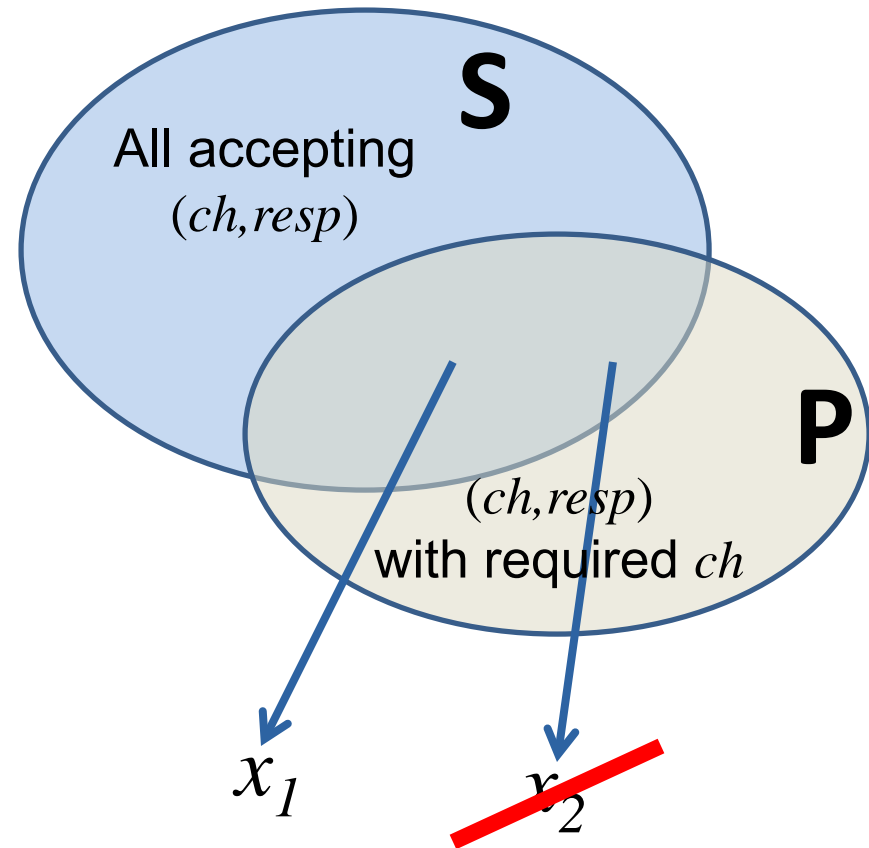
## Pick-one trick: Not finding $x_1, x_2 \in S$

---

- $x_1, x_2 \in S$  hard to find.
- Even with oracle for  $I - 2|\Psi\rangle\langle\Psi|$ .
- Assuming  $S$  is a random set.
- Query complexity problem.
- Proved using Ambainis' "adversary method"

# Breaking sigma-protocols

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



# No quantum secure sigma protocols?

---

- No: under extra conditions, they are secure  
[Watrous 2006, Unruh 2012]
- But general security unlikely under same assumptions as classical



# Other results

---

Same technique (pick-one trick) gives impossibilities for:

- Computationally-sound proofs
- Fiat-Shamir's NIZK proofs/signatures
- Fischlin's NIZK proofs
- Commitments

# Open problems

---

- Can we do it without oracles?  
[Aaronson, Christiano 2012]?
- Under what conditions are sigma-protocols et al. secure?
- Alternative constructions that are secure?

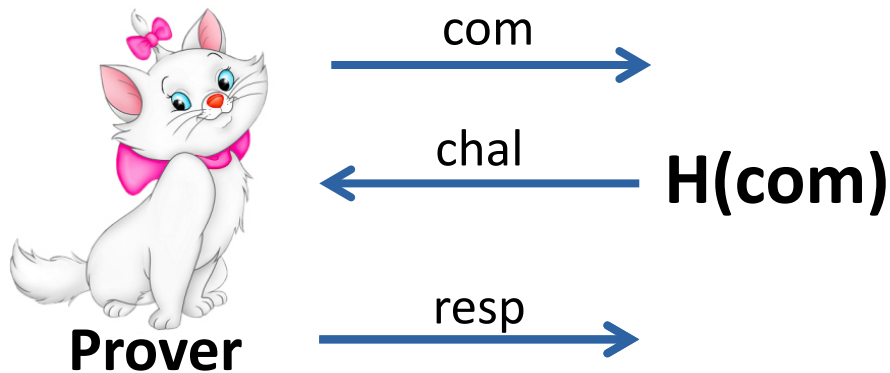
# I thank for your attention



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

# NIZK with random oracles

## Fiat-Shamir



- NIZK consists of com, chal, resp
- Prover can't cheat: H is like a verifier
- Security-proof: Rewinding

## Fischlin

Fix com

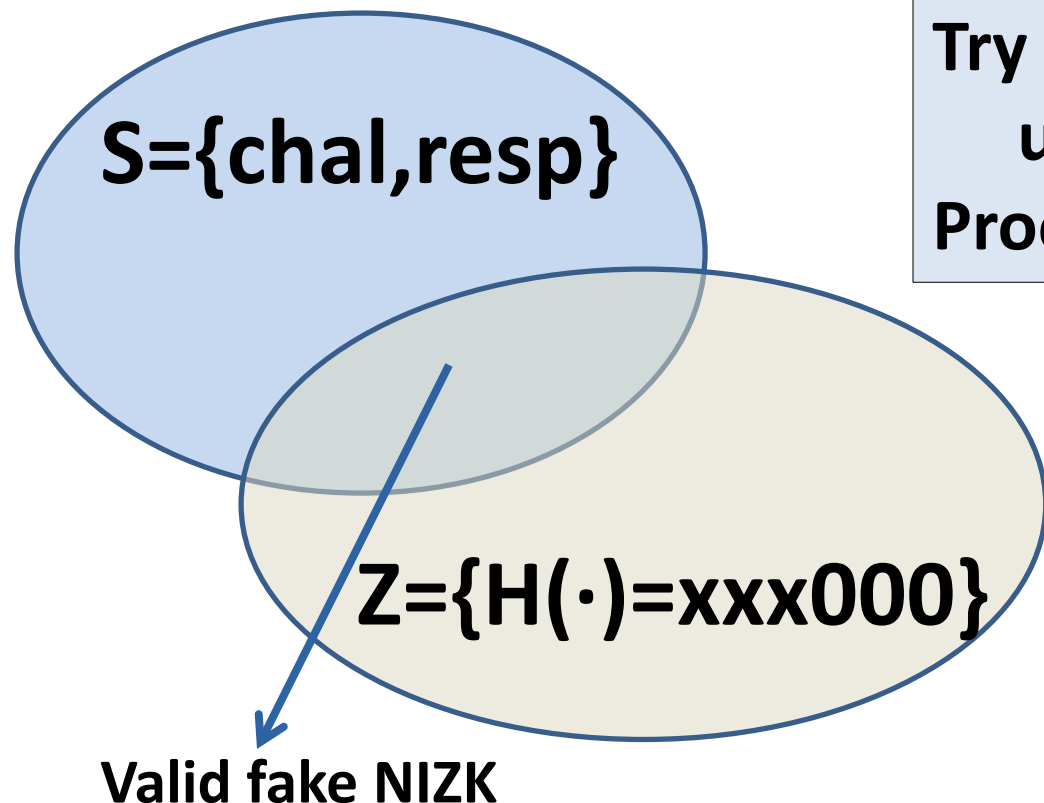
Try different chal, resp  
until  $H(\text{chal}, \text{resp}) = \text{xxx000}$

**Proof** := com, chal, resp

- Need to query several chal, resp
- Implies existence of witness



# Attacking Fischlin



**Fix com**

**Try different chal, resp**

**until  $H(\text{chal, resp}) = \text{xxx000}$**

**Proof = com, chal, resp**

**Without knowing witness!**

**(Because we have only one S-element)**

**[Fiat-Shamir attacked similarly]**

# How does “one-pick trick” work?

---

- Grover: Quantum algorithm for searching
- Observation:
  - First step of Grover produces a state encoding the search space
- This state (plus modified Grover) implements “one-pick trick”
- Hard part: Prove “can’t find two  $x_1, x_2 \in S$ ”