Online-Extractability in the Quantum Random-Oracle Model

Jelle Don, Serge Fehr, Christian Majenz and Christian Schaffner

CWI

QuSoft
Research Center for Quantum Software

Universiteit Leiden
The Netherlands

DTU
Technical University of Denmark

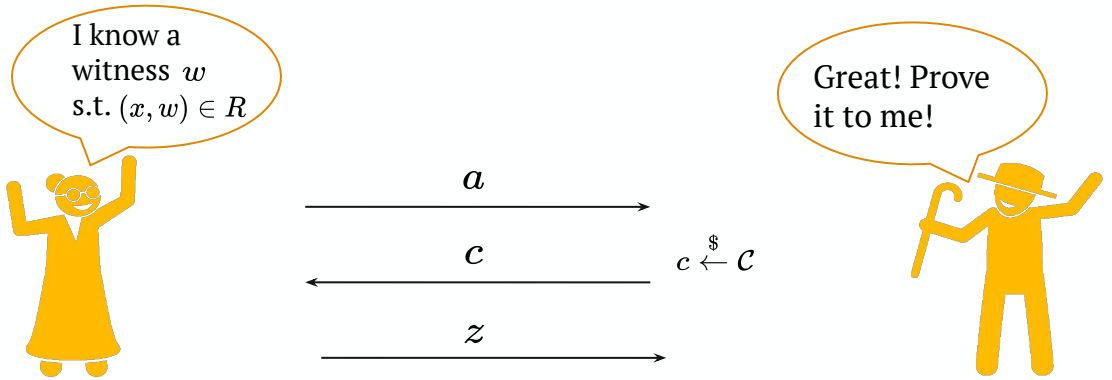
Universiteit van Amsterdam

Extraction (in cryptography)

- $\mathcal{A}$ sends messages depending on some secret s
- In an honest execution, s remains secret
- An extractor algorithm with ‘enhanced access’ to $\mathcal{A}$ can obtain s

Examples of extraction

- (Zero-knowledge) proofs of knowledge



- Extractable commitments
- CCA-security of encryption or KEM's

Straight-line and on-the-fly

- Straight-line
  - Single run vs. rewinding
  - Better loss factor/runtime

- On-the-fly
  - Extraction happens during execution vs. afterwards
  - Necessary for CCA-security extraction

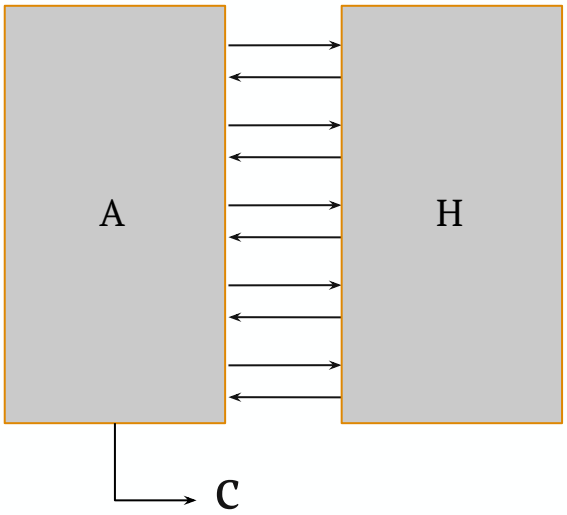
- Straight-line + On-the-fly = online extractability

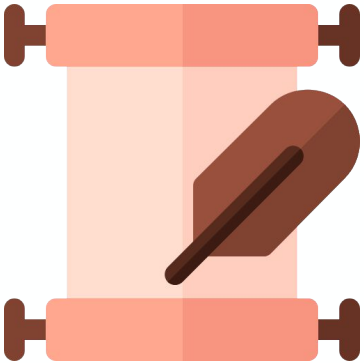
Enhanced access

- Rewinding
  - Proofs of knowledge, zero-knowledge proofs
- Trapdoor
  - Extractable commitments
- Random-Oracle Model (ROM)
  - Hash-based commitments, commit-and-open protocols, CCA security
- Quantum Random-Oracle Model?

Example: Hash-based commitment (ROM)

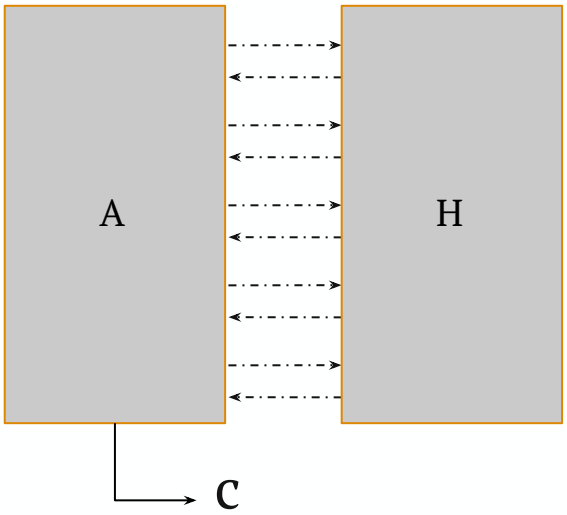
- A commits to s with c = H(x) for x = s||r, where r is random
- The extractor searches for x' s.t. H(x')=c in the transcript





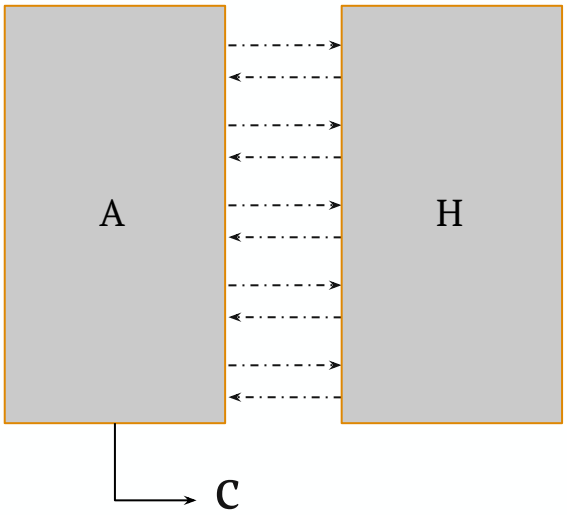
Example: Hash-based commitment (QROM)

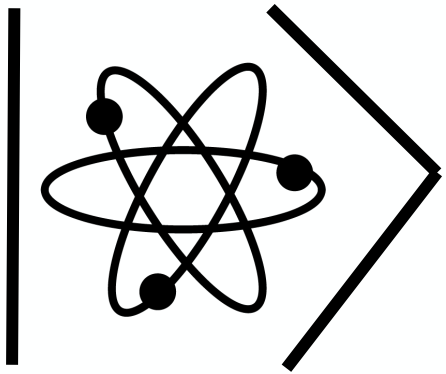
- A commits to s with c = H(x) for x = s||r, where r is random
- ~~The extractor searches for x s.t. H(x)=c in the transcript~~



Example: Hash-based commitment (QROM)

- A commits to s with c = H(x) for x = s||r, where r is random
- The extractor performs a measurement on the oracle state?





[Zha19]

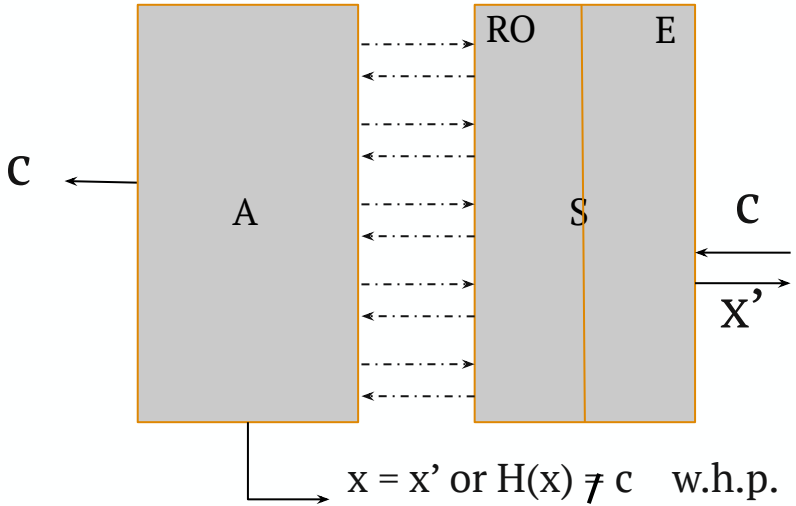
Technical core of our result

- We bound the norm of the commutator [M,O] of a suitable extraction measurement and the compressed oracle unitary

- The bound is negligible in the output size of the oracle, hence
  - We can move the measurement to the end of the run
  - Introducing a measurement at the end does not affect the view of the adversary
  - The adversary does not notice the measurement

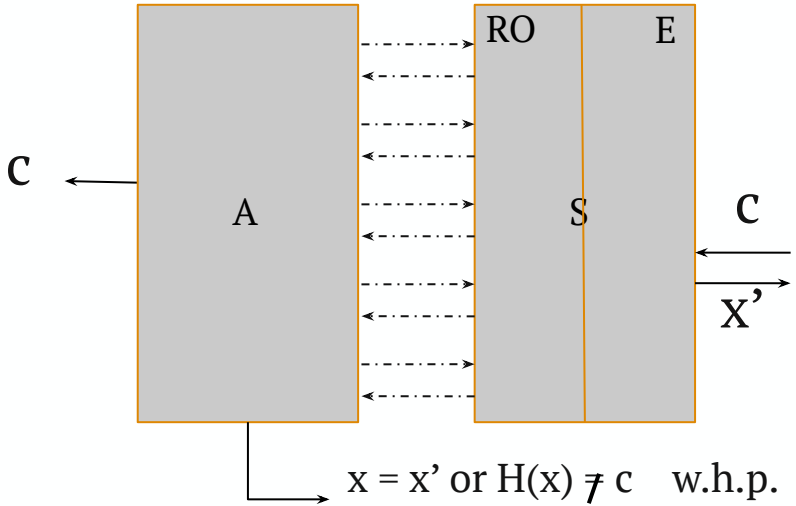
Our main result

- There exists a simulator S with RO interface and Extraction interface s.t. for every bounded query algorithm A we have:



Our main result

- There exists a simulator S with RO interface and Extraction interface s.t. for every bounded query algorithm A we have:

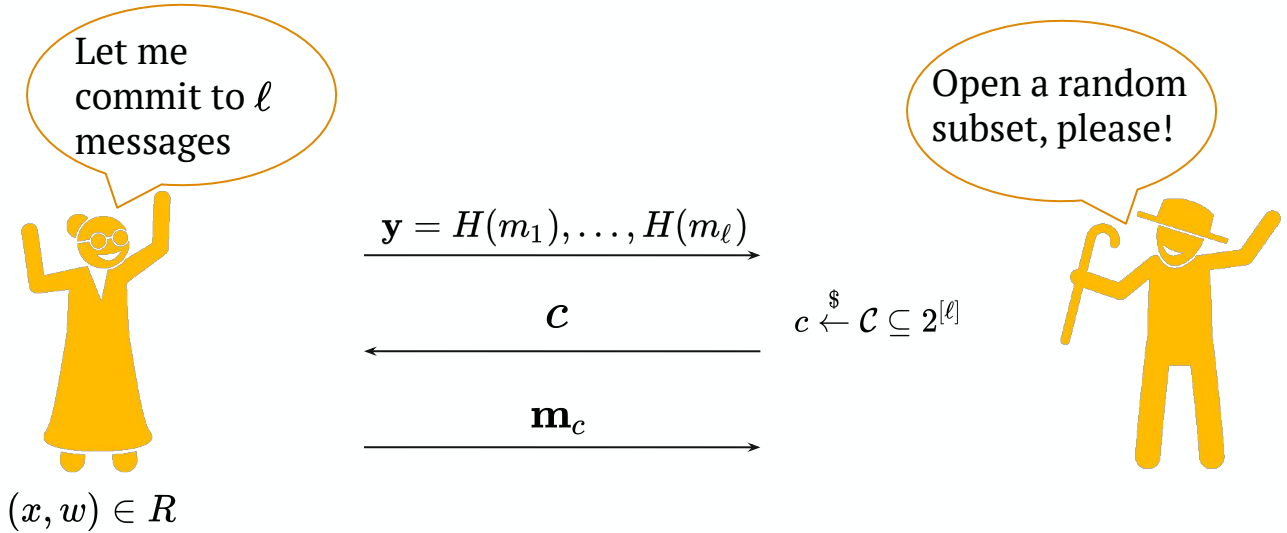


This example: c = H(x)

More general: t = f(x,H(x))

for f(x,y) with the property that there are not too many y's s.t. f(x,y)=t

Application: Commit-and-Open Protocols



Application: Commit-and-Open Protocols

- We show tight online-extractability of generic C&O protocols
  - Without ‘collapsingness’ or ‘unique responses’
  - Previous techniques incurred a cubic loss
- Used in the popular MPC-in-the-head paradigm
- Underlying the NIST post-quantum signature candidate PICNIC
  - PICNIC uses a *Fiat-Shamir-transformed* C&O protocol
  - Proven tightly secure in follow-up work [DFMS22]

Application: Fujisaki-Okamoto transform

- We give the first complete post-quantum security proof of the textbook FO-transform
  - Session key derived as H(m) instead of H(m,c)
  - No “key confirmation hash”
  - Works for FO with “explicit rejection”
- Used in many of the NIST KEM candidates

Summary

- We lift a powerful extraction method from the ROM to the QROM
  - That works straight-line and on-the-fly
- We give the first tight reduction of commit-and-open protocols
- We give the first post-quantum analysis of textbook FO
- If the adversary outputs t and promises an x s.t. f(x,H(x)) = t
  - We can extract it online

Thank you for listening

Questions?