Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM

Jelle Don, Serge Fehr, Christian Majenz and Christian Schaffner

DTU Technical University of Denmark

CWI

QuSoft Research Center for Quantum Software

Universiteit Leiden The Netherlands

Universiteit van Amsterdam

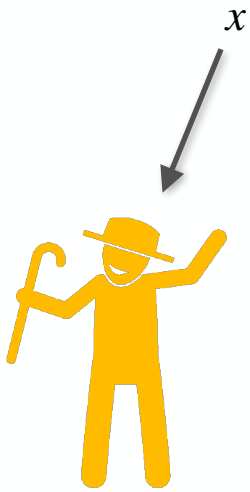
Outline

- The Problem
- Our Results
- Commit-and-Open Protocols
- The QROM extractor
- Main Result
- The CHFL21 Framework
- Improved Unruh Transform

The Problem

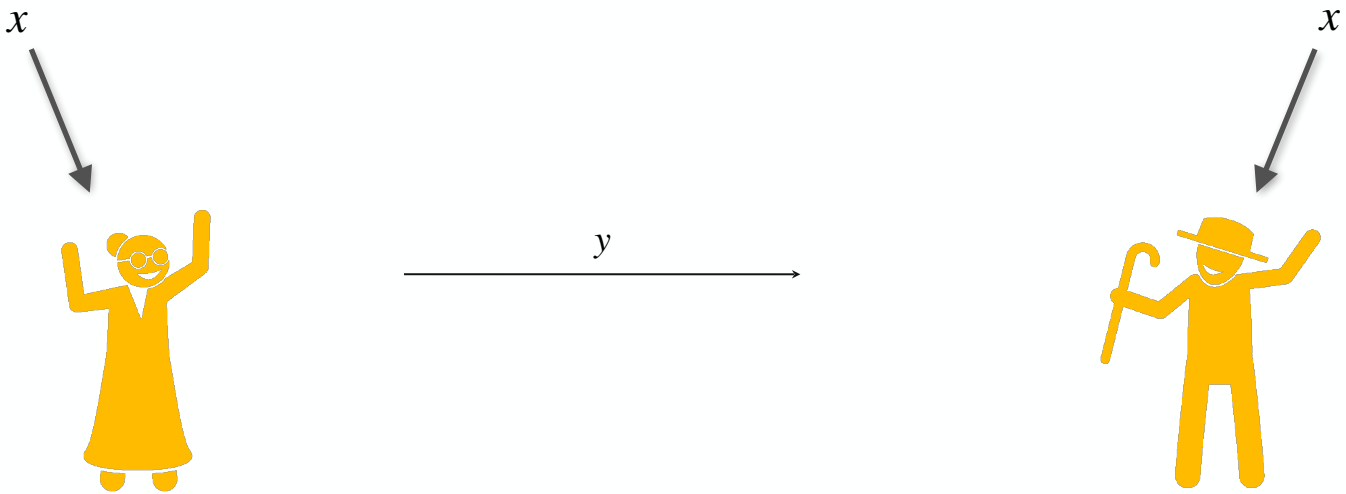
Are there Fiat-Shamir NIZKs/DSS with a tight security proof?

Σ-protocols & Fiat-Shamir



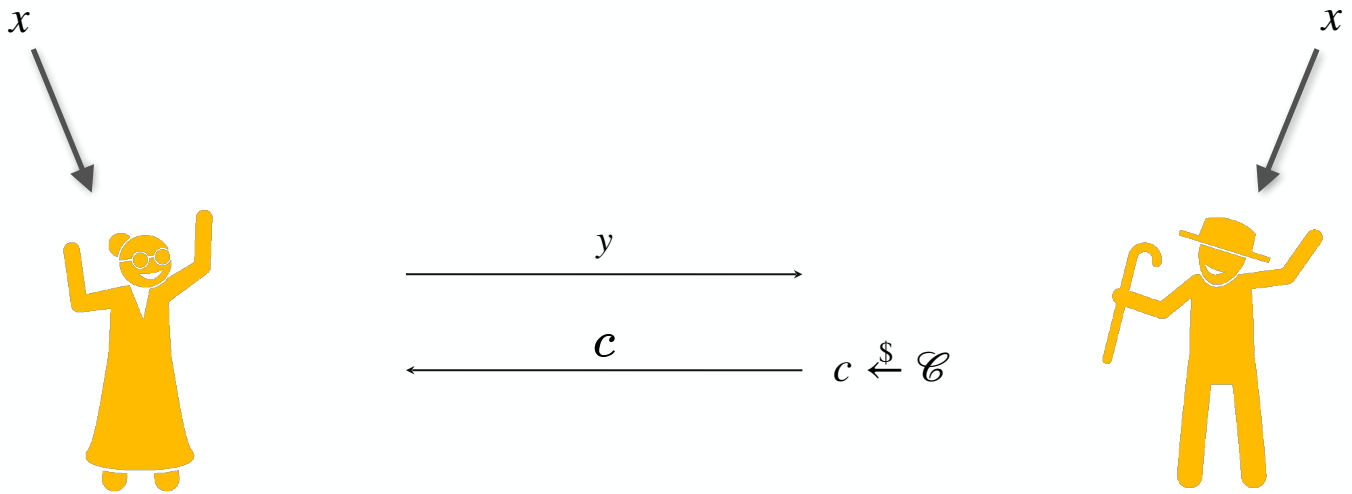
$x \in \mathscr{L}$, witness relation R

Σ-protocols & Fiat-Shamir



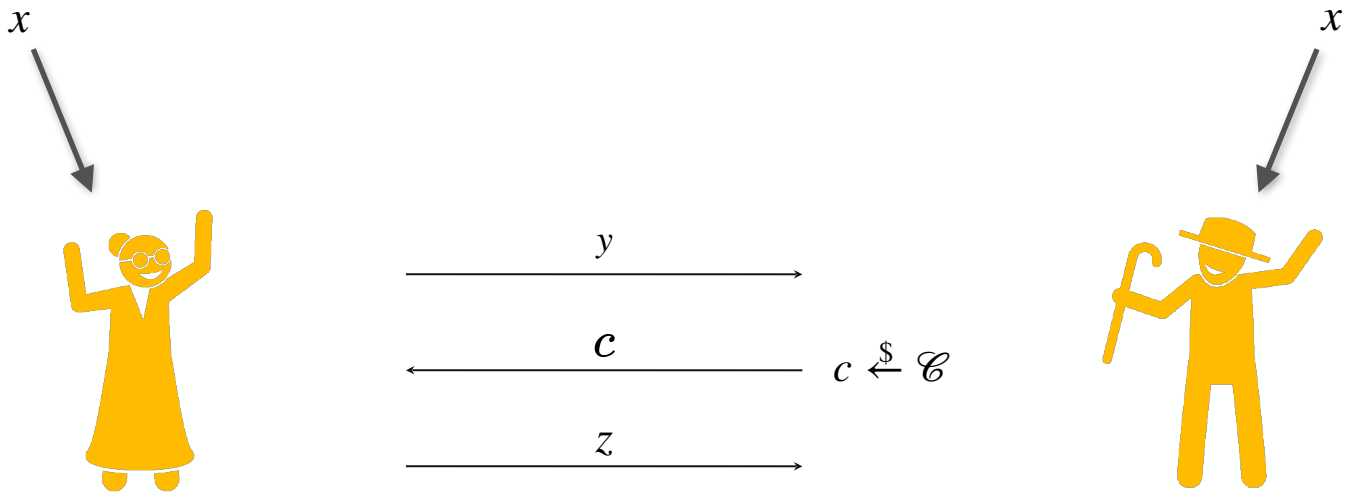
$x \in \mathscr{L}$, witness relation R

Σ-protocols & Fiat-Shamir



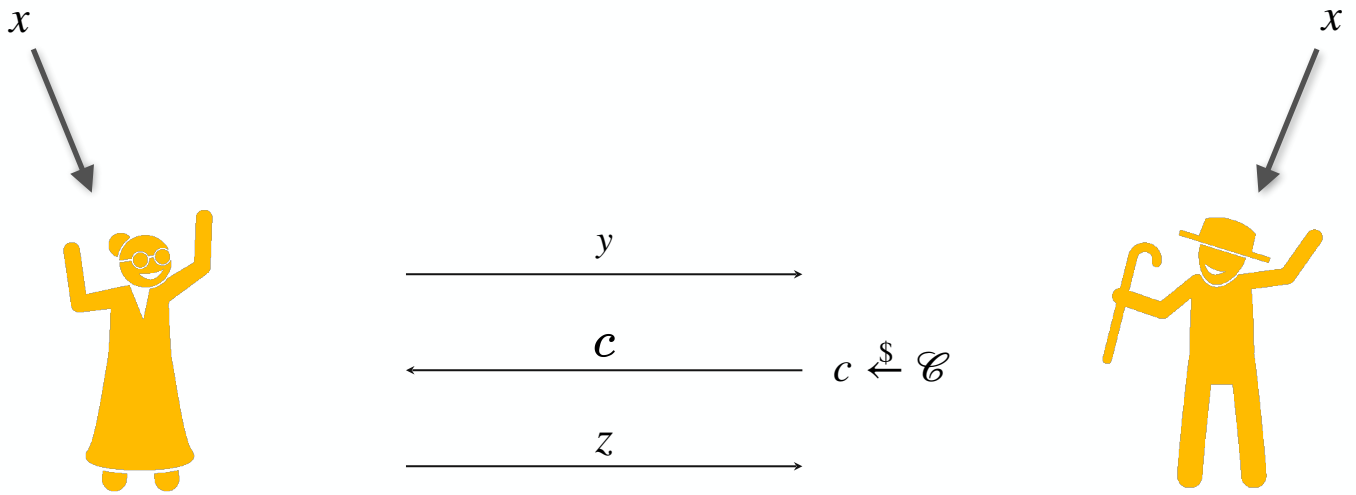
$x \in \mathscr{L}$, witness relation R

Σ-protocols & Fiat-Shamir



$x \in \mathscr{L}$, witness relation R

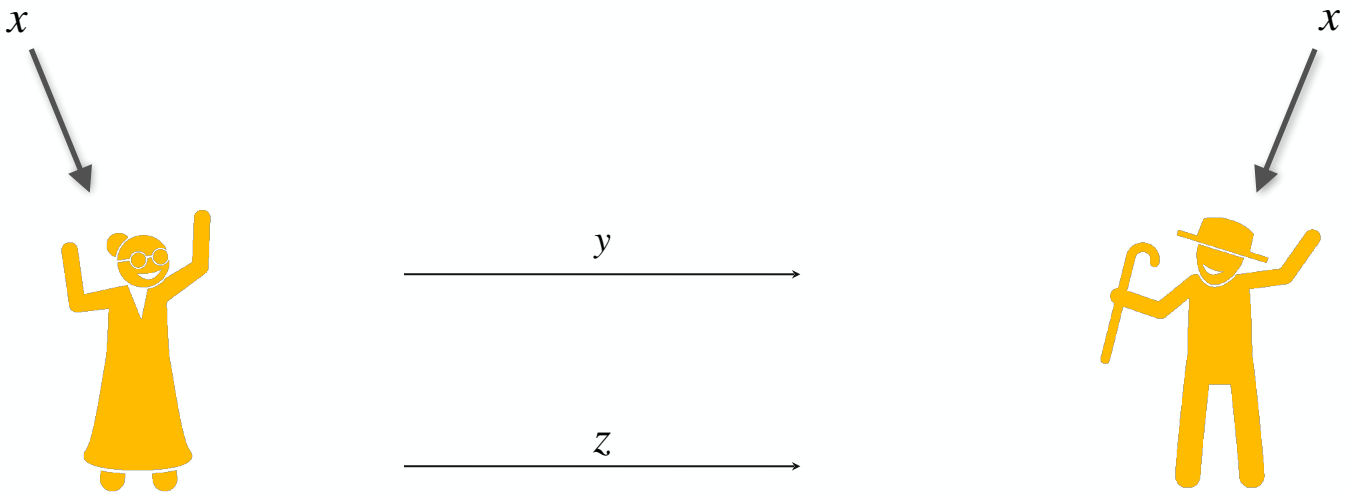
Σ-protocols & Fiat-Shamir



$x \in \mathscr{L}$, witness relation R

$V(x, y, c, z) \in \{\text{accept}, \text{reject}\}$

Σ-protocols & Fiat-Shamir

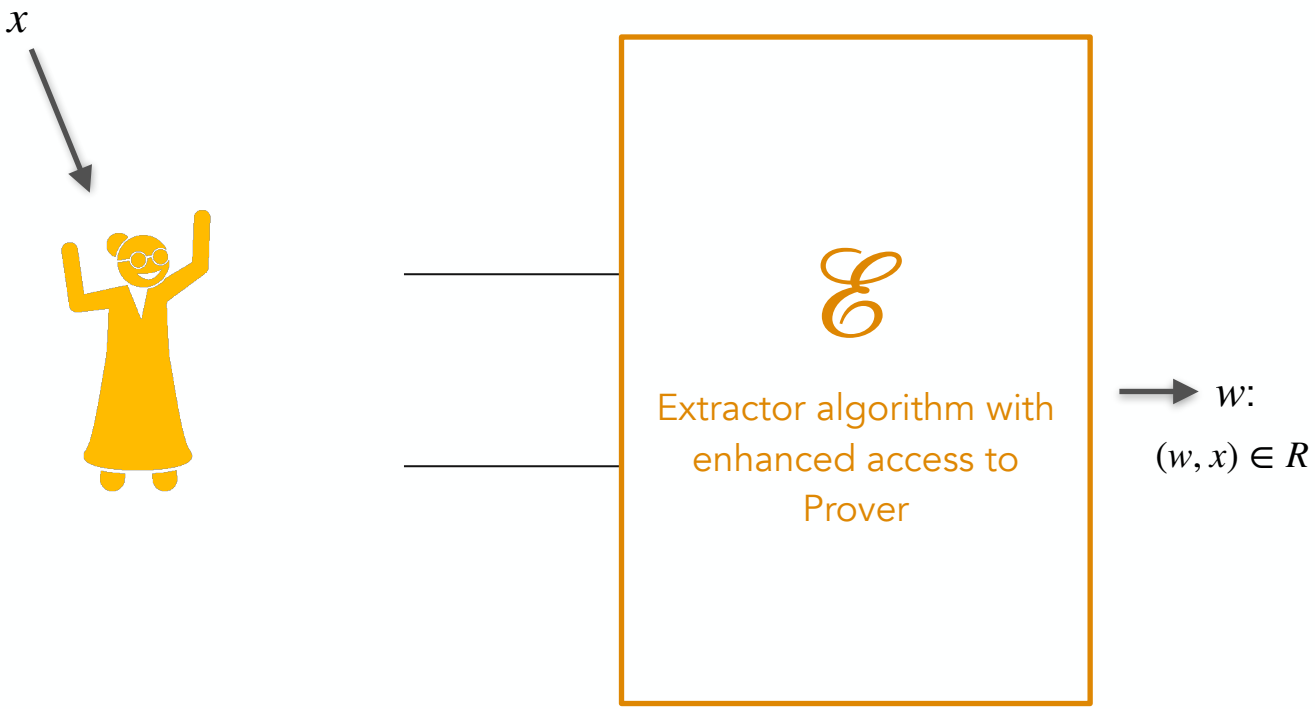


$x \in \mathscr{L}$, witness relation R

$V(x, y, c, z) \in \{\text{accept}, \text{reject}\}$

Fiat-Shamir: $c := H(x, y)$

Extractability



Extractability

FS of…	Prover success probability	Extractor success probability
Arbitrary Σ, ROM	p	p^2/q or p/q
Commit-and-Open, ROM	p	p-$negl_q(n)$
Arbitrary Σ, QROM	p	p^3/q^6 or p/q^2
Commit-and-Open, QROM	p	p/q^2

Σ-protocols with collapsingness

q=number of (Q)RO queries

n=security parameter

Extractability

FS of…	Prover success probability	Extractor success probability
Arbitrary Σ, ROM	p	p^2/q or p/q
Commit-and-Open, ROM	p	p-$negl_q(n)$
Arbitrary Σ, QROM	p	p^3/q^6 or p/q^2
Commit-and-Open, QROM	p	p/q^2

Σ-protocols with collapsingness

q=number of (Q)RO queries

n=security parameter

Our Results

Online-extractability for some Fiat-Shamir-NIZKs in the QROM

Results

We…

- construct an online extractor for the Fiat-Shamir transform of commit-and-open protocols in the QROM
- extend the technique to Merkle-tree commitments
- modularize and improve the Unruh transform
- apply our result to the Picnic signature scheme

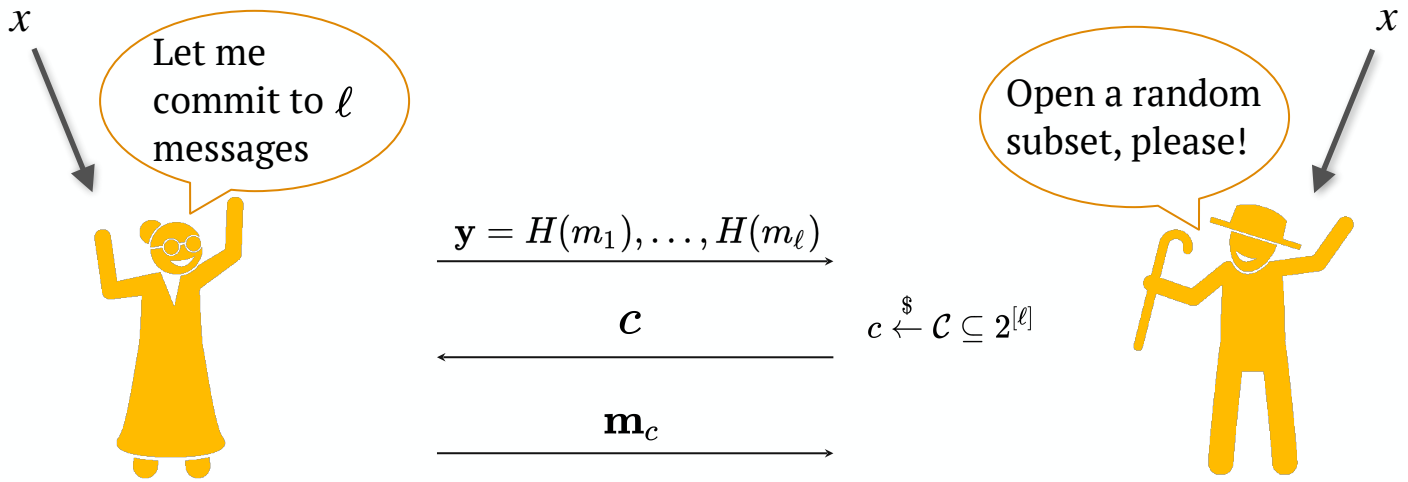
Related work

- Chailloux (eprint ’21): same result, but under scheme-specific assumption
- Chiesa, Manohar, Spooner (TCC ’19): Analysis of a specific SNARG construction.
  - Quite similar to our Merkle tree commitment result
  - Was somehow missed in the analysis of, e.g, Picnic until now

Commit-and-Open Protocols

A special class of Σ-protocols

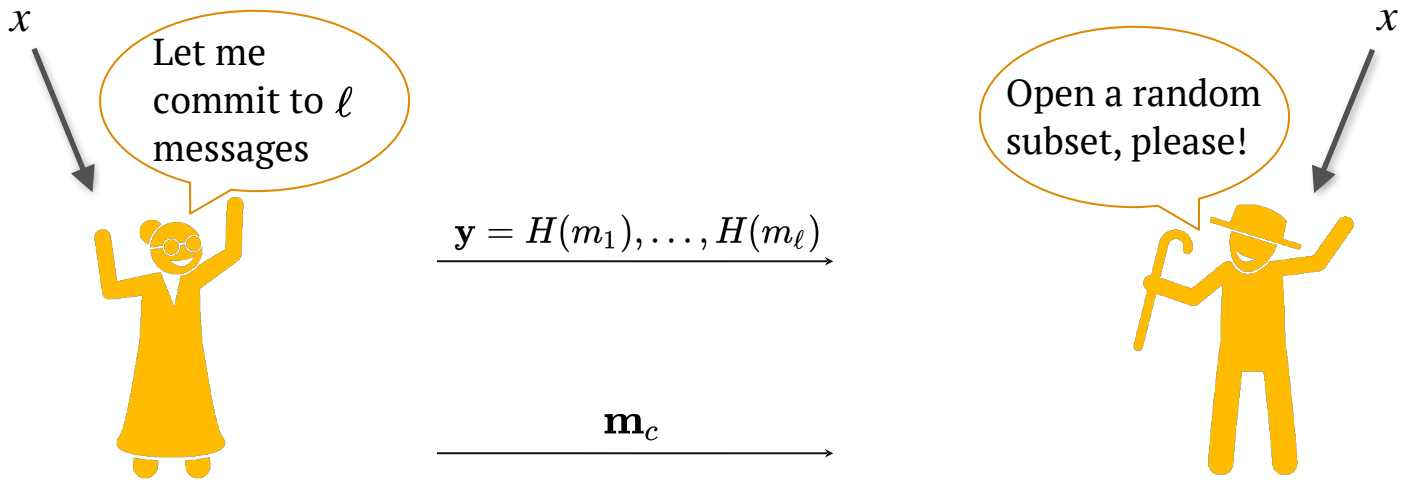
Commit-and-Open (C&O) Protocols



$x \in \mathscr{L}$, witness relation R

$V(x, \mathbf{m}_c) \in \{\text{accept}, \text{reject}\}$
$\forall i \in c : H(m_i) = y_i$

Commit-and-Open (C&O) Protocols



$x \in \mathscr{L}$, witness relation R

Fiat-Shamir: $c := H(x, \mathbf{y})$

$V(x, \mathbf{m}_c) \in \{\text{accept}, \text{reject}\}$
$\forall i \in c : H(m_i) = y_i$

Merkle tree commitments with octopus opening

- First message in C&O protocols: $H(m_1), \ldots, H(m_\ell)$
- Third message: $(m_i)_{i \in c}$ for $c \subset \{1,...,\ell\}$

Merkle tree commitments with octopus opening

- First message in C&O protocols: $H(m_1), \ldots, H(m_\ell)$
- Third message: $(m_i)_{i \in c}$ for $c \subset \{1,...,\ell\}$

$\Rightarrow$ Any commitment allowing for opening a subset of messages works

Merkle tree commitments with octopus opening

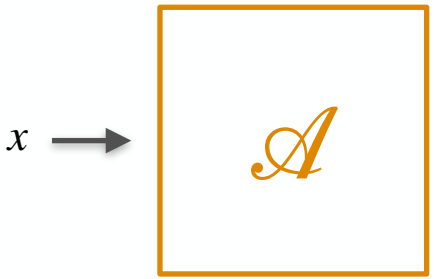
- First message in C&O protocols: $H(m_1), \ldots, H(m_\ell)$
- Third message: $(m_i)_{i \in c}$ for $c \subset \{1,...,\ell\}$

$\Rightarrow$ Any commitment allowing for opening a subset of messages works

In Picnic: Merkle tree commitment

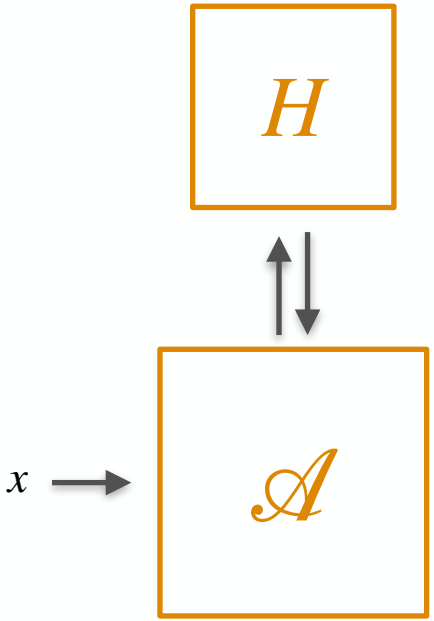
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



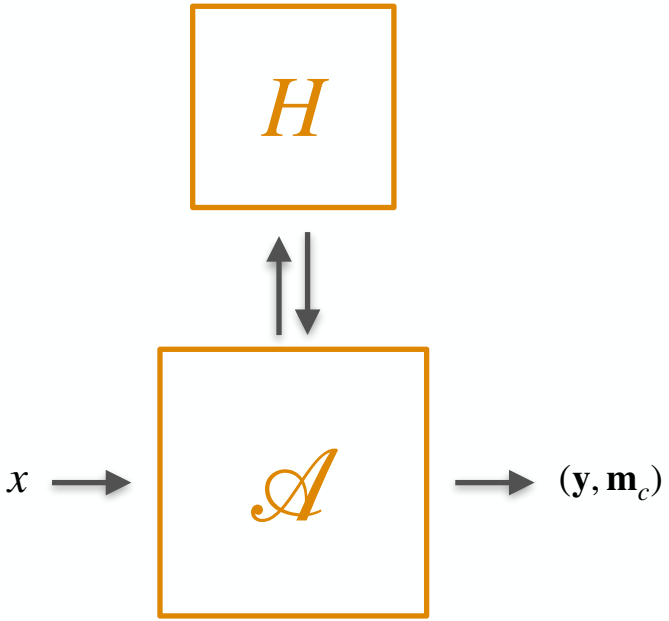
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



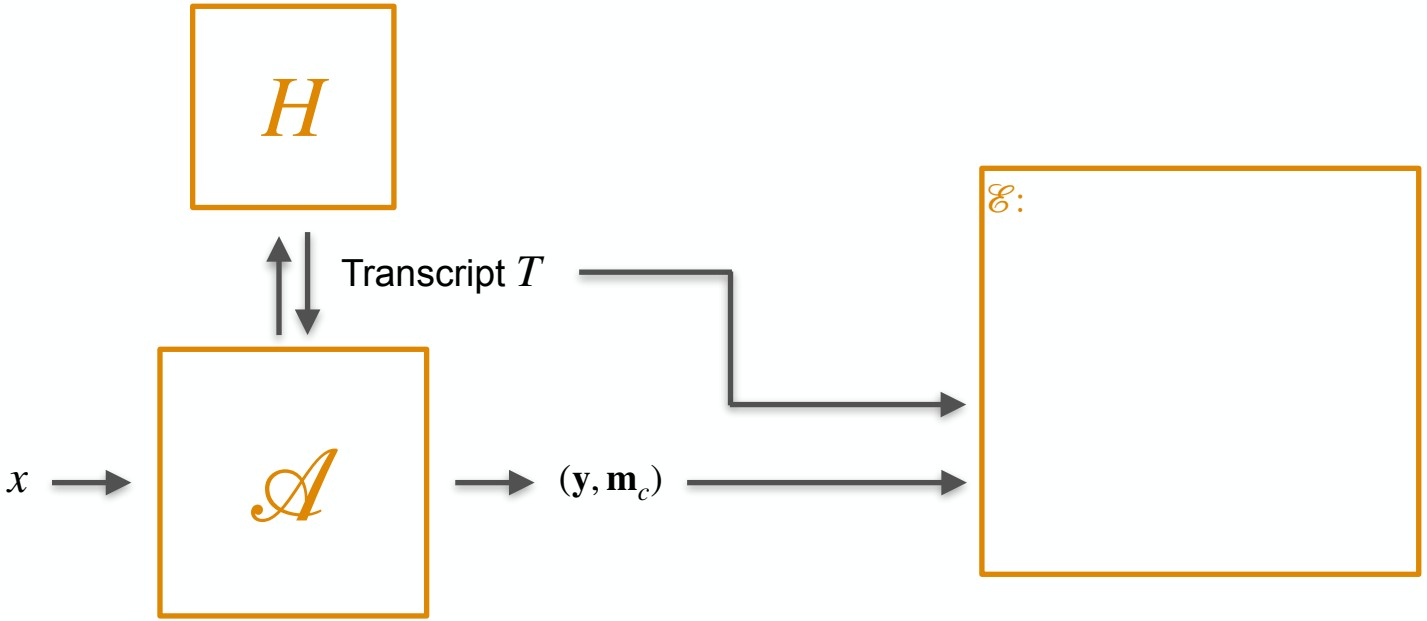
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



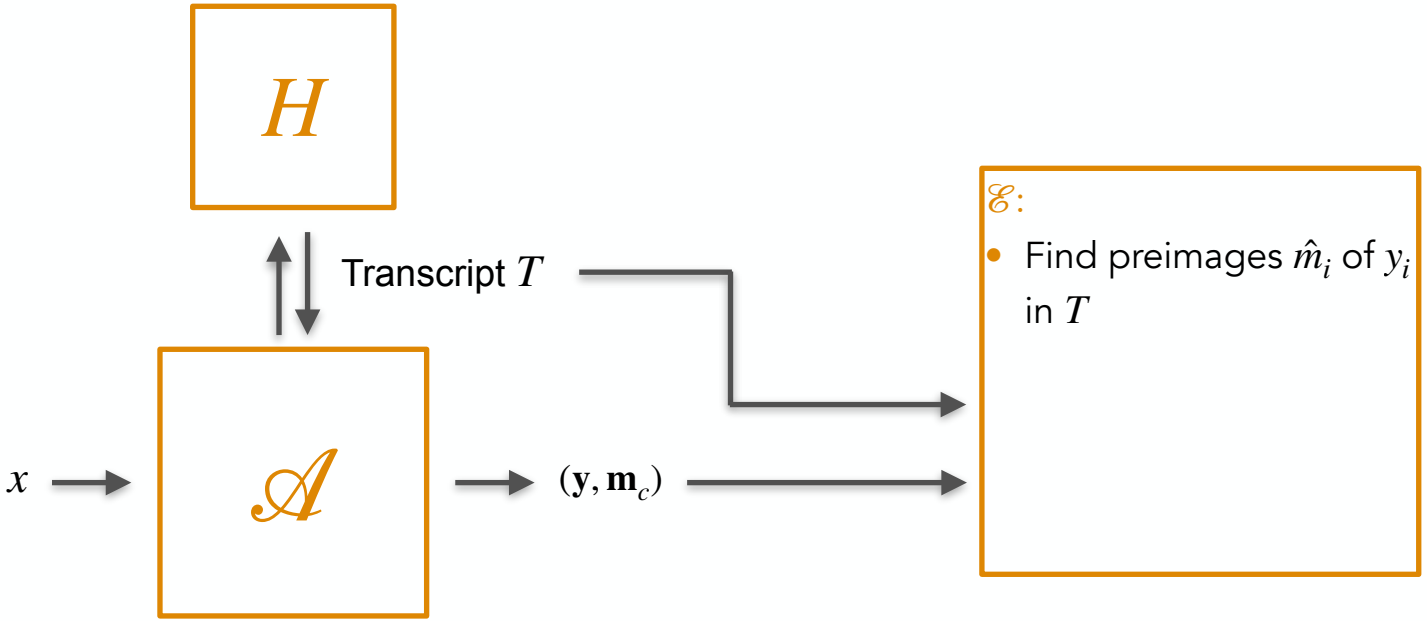
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



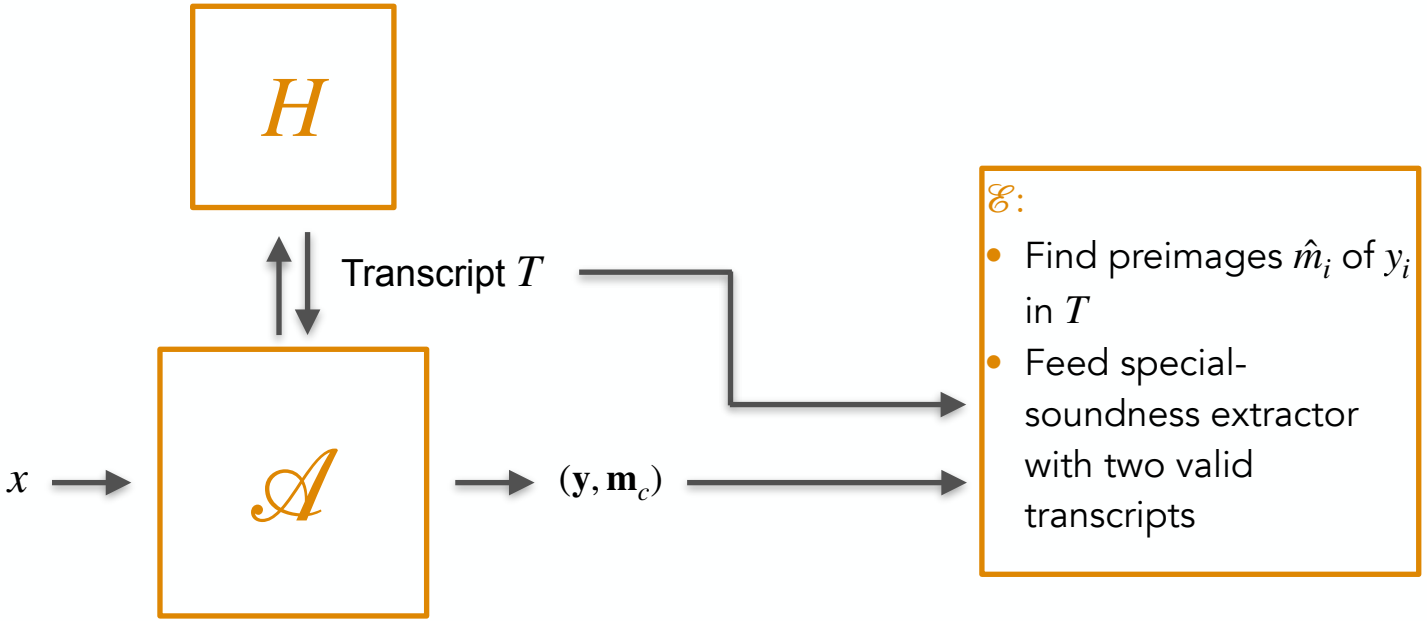
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



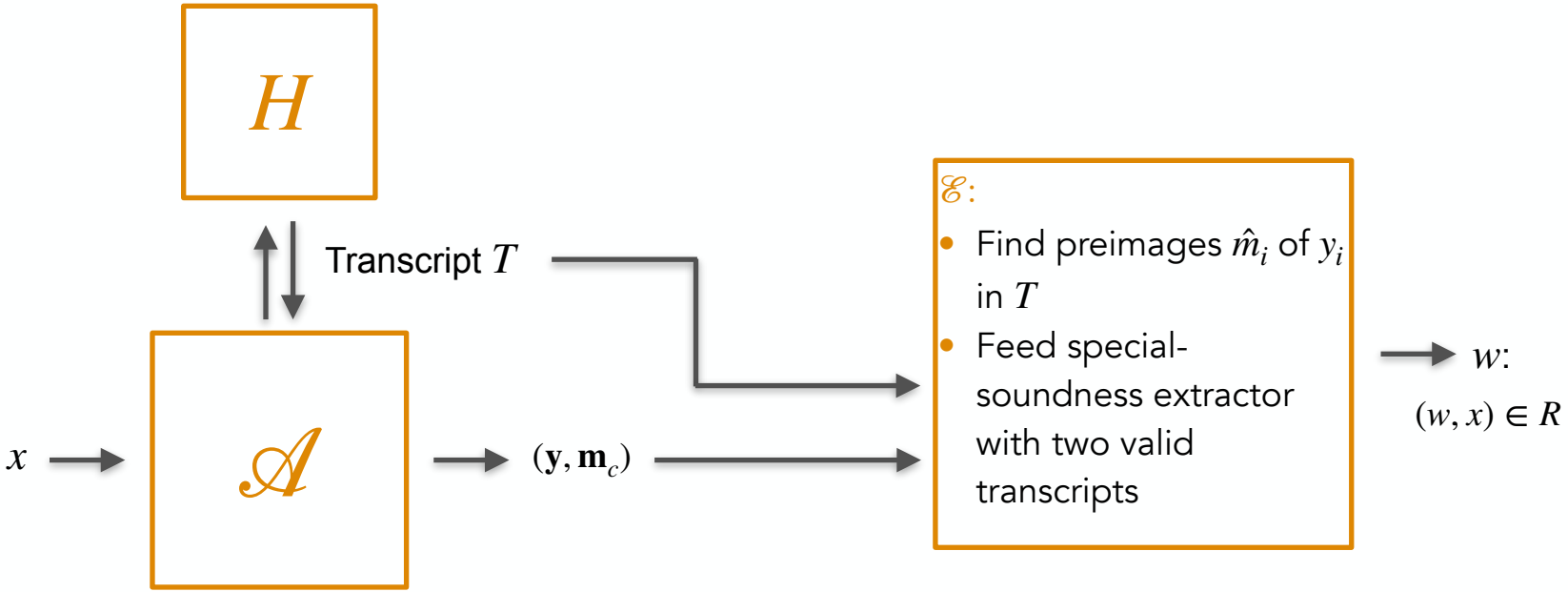
Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol

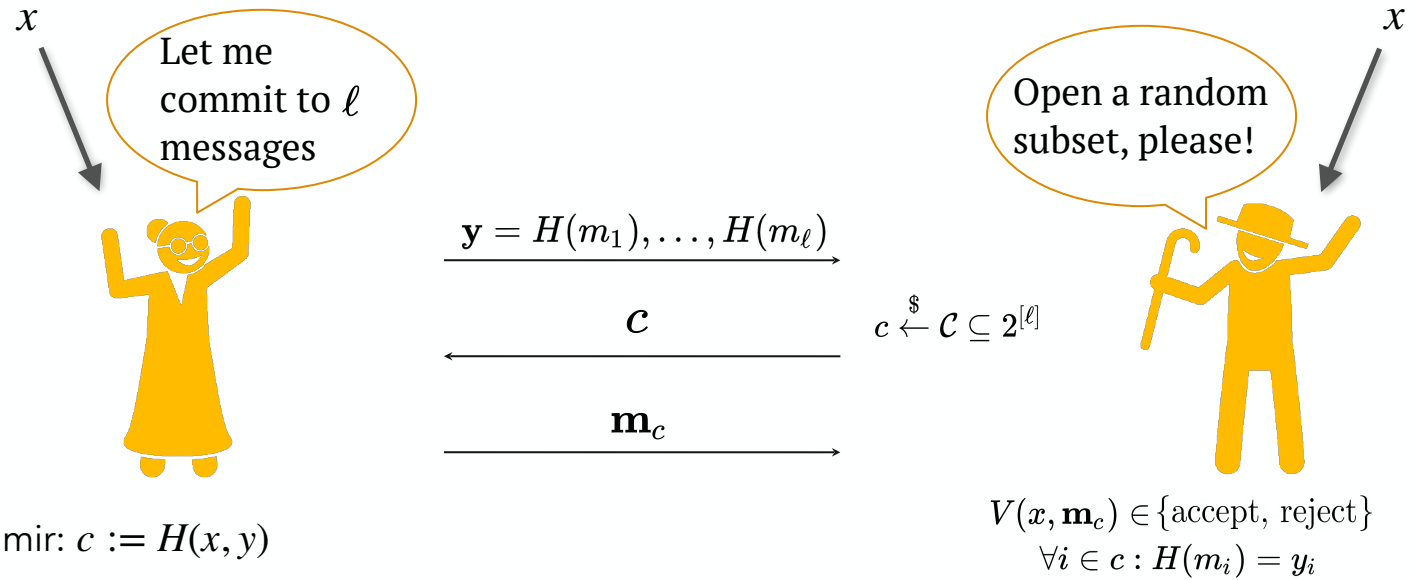


Online-Extractability in the ROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



Why does it work?

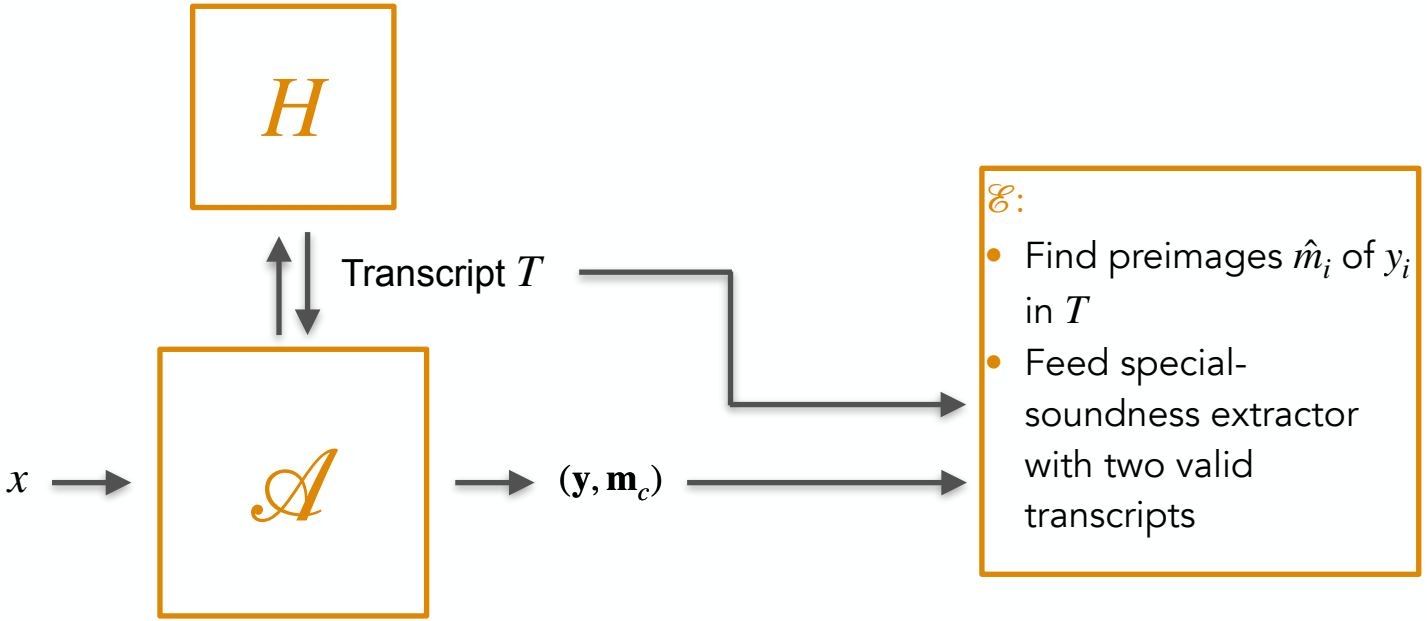


Fiat-Shamir: $c := H(x, y)$

It's (usually) easy to produce $\mathbf{y}$ and a valid $\mathbf{m}_c$ for **one** value of c….

Why does it work?

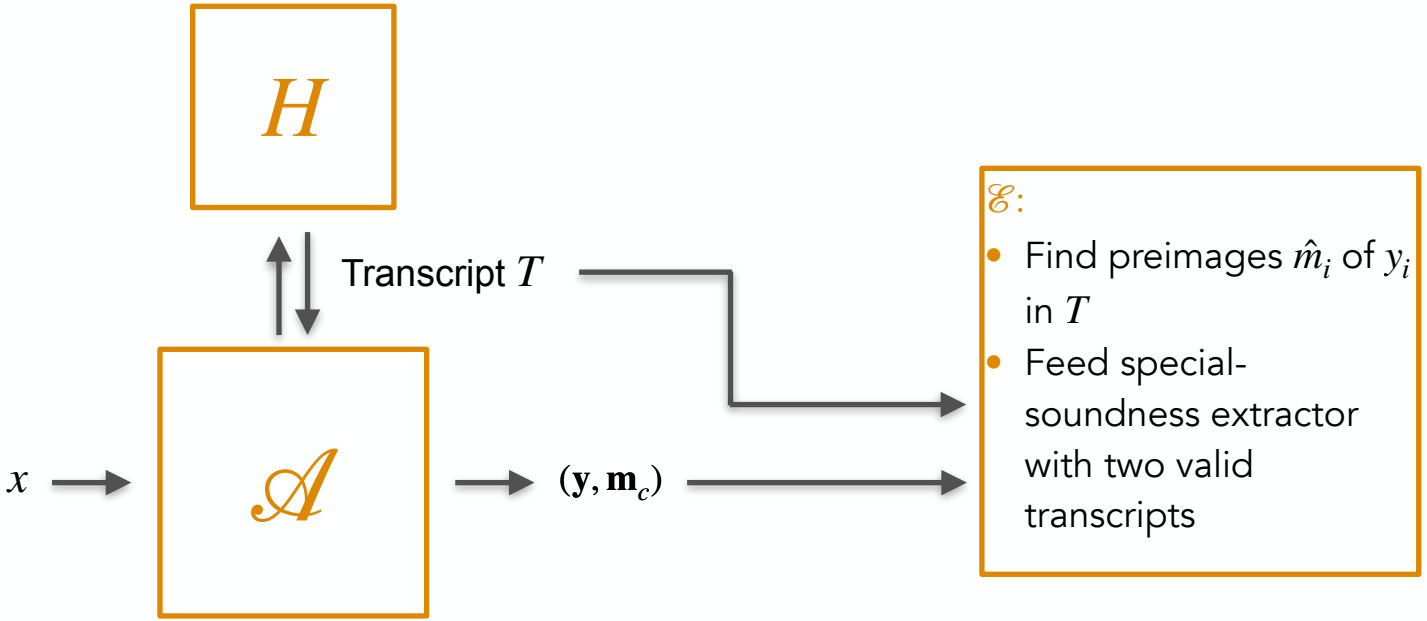
$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



Why does it work?

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol

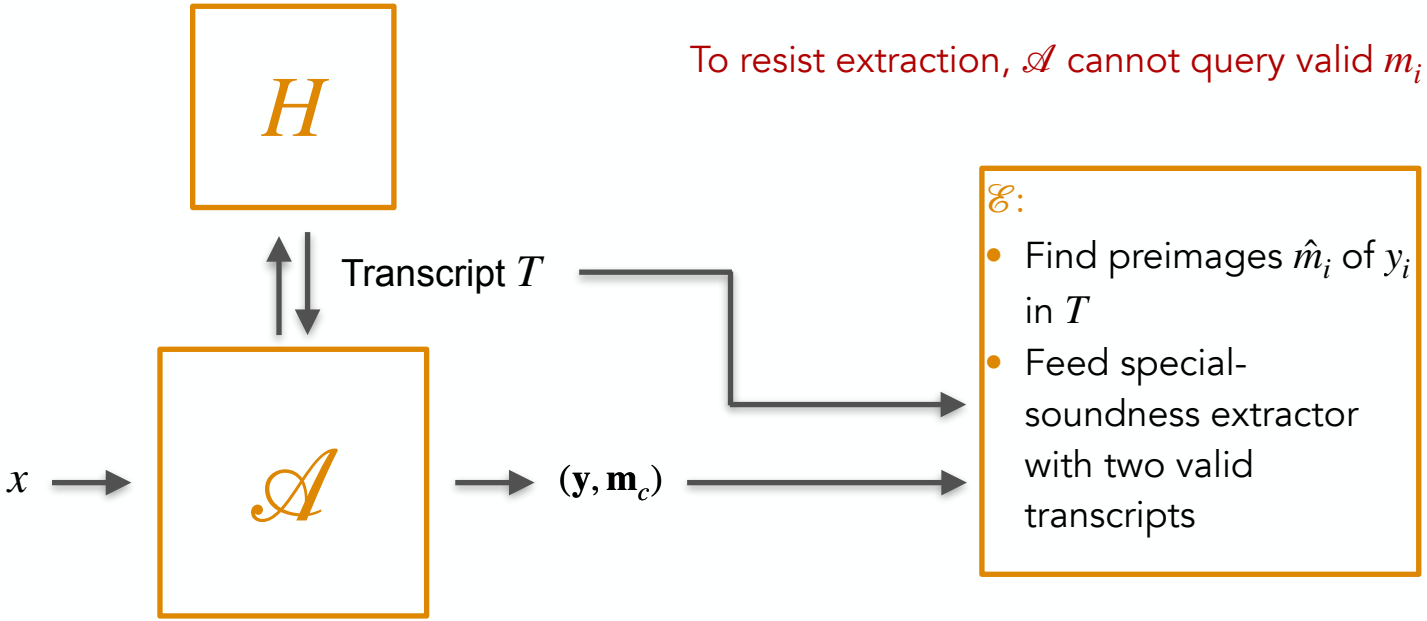
For simplicity: $\mathscr{C}$ = subsets of size r



Why does it work?

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol

For simplicity: $\mathscr{C}$ = subsets of size r



Why does it work?

$\mathscr{A}$ that succeeds such that $\mathscr{E}$ does not needs to perform an "artificial" oracle search task:

Problem: *Find valid* $\left(\mathbf{y}, \mathbf{m}_{H(x,\mathbf{y})}\right)$ *without querying any valid* m *such that* $H(m) = y_i$ *for some* $i \notin H(x, \mathbf{y})$

Why does it work?

$\mathscr{A}$ that succeeds such that $\mathscr{E}$ does not needs to perform an "artificial" oracle search task:

Problem: *Find valid* $\left(\mathbf{y}, \mathbf{m}_{H(x,\mathbf{y})}\right)$ *without querying any valid* m *such that* $H(m) = y_i$ *for some* $i \notin H(x, \mathbf{y})$

This is a hard oracle search task!

Extractability

FS of…	Prover success probability	Extractor success probability
Arbitrary Σ, ROM	p	p^2/q or p/q
Commit-and-Open, ROM	p	p-negl$_q$(n)
Arbitrary Σ, QROM	p	p^3/q^6 or p/q^2
Commit-and-Open, QROM	p	p/q^2

Σ-protocols with collapsingness

q=number of (Q)RO queries

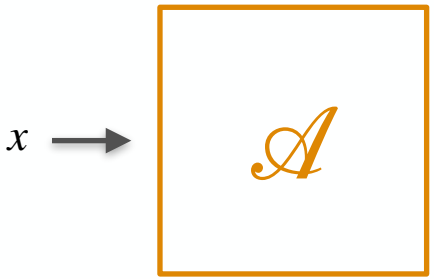
n=security parameter

The QROM extractor

“Just use a compressed oracle!”

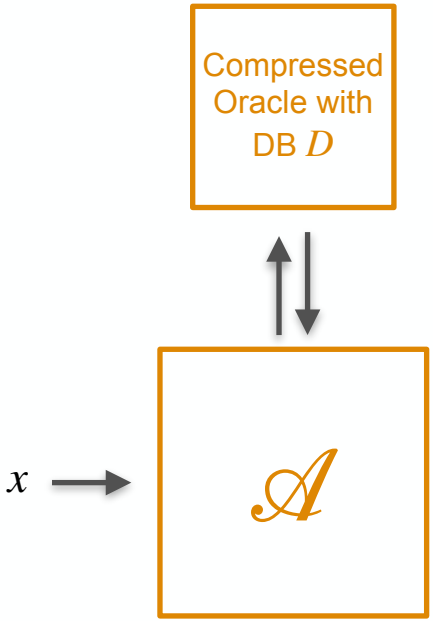
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



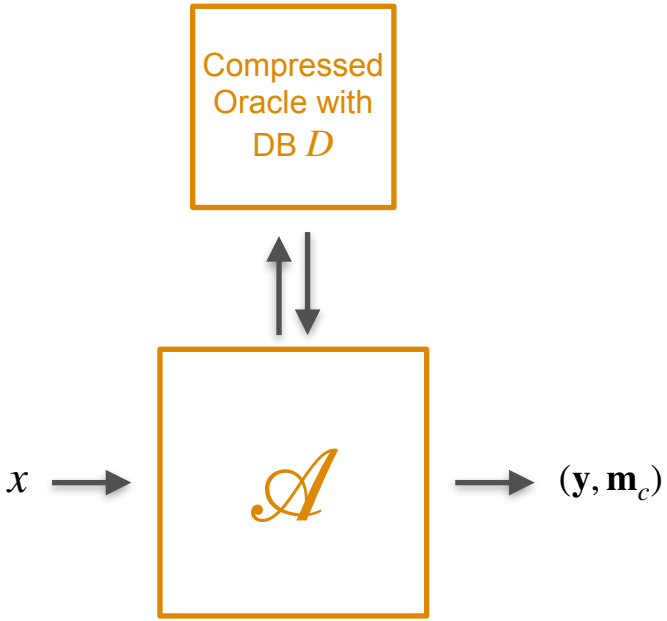
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



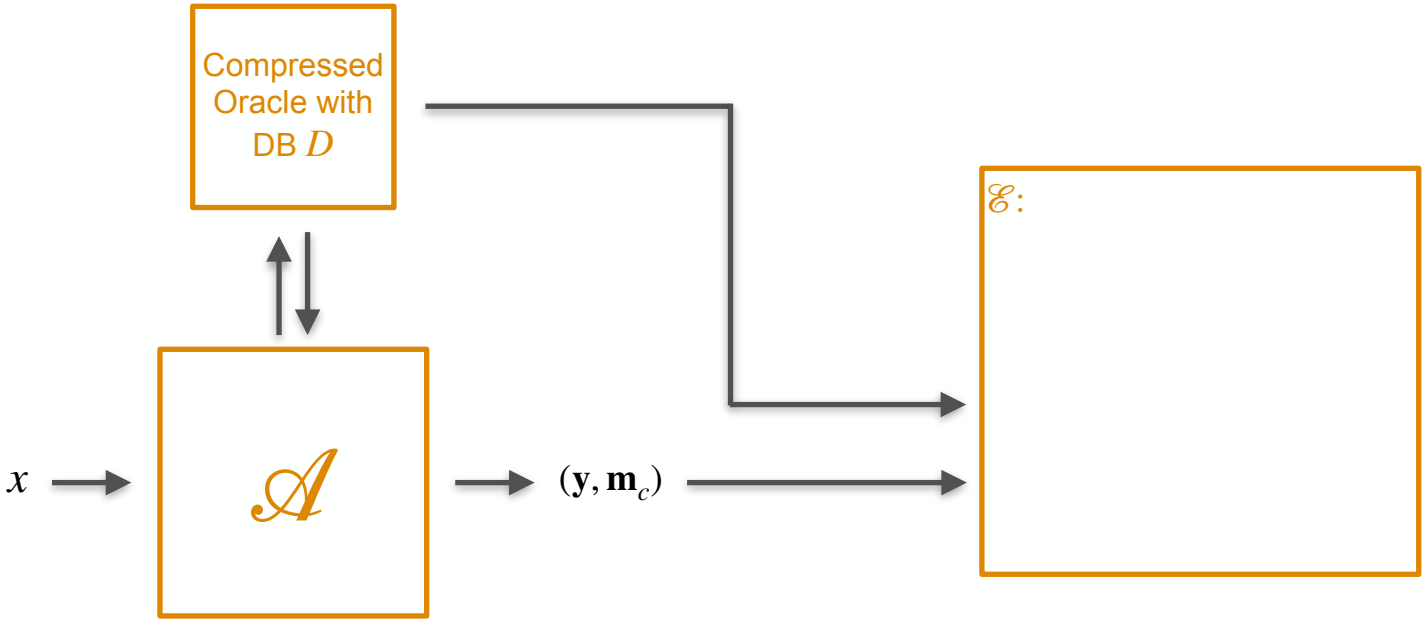
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



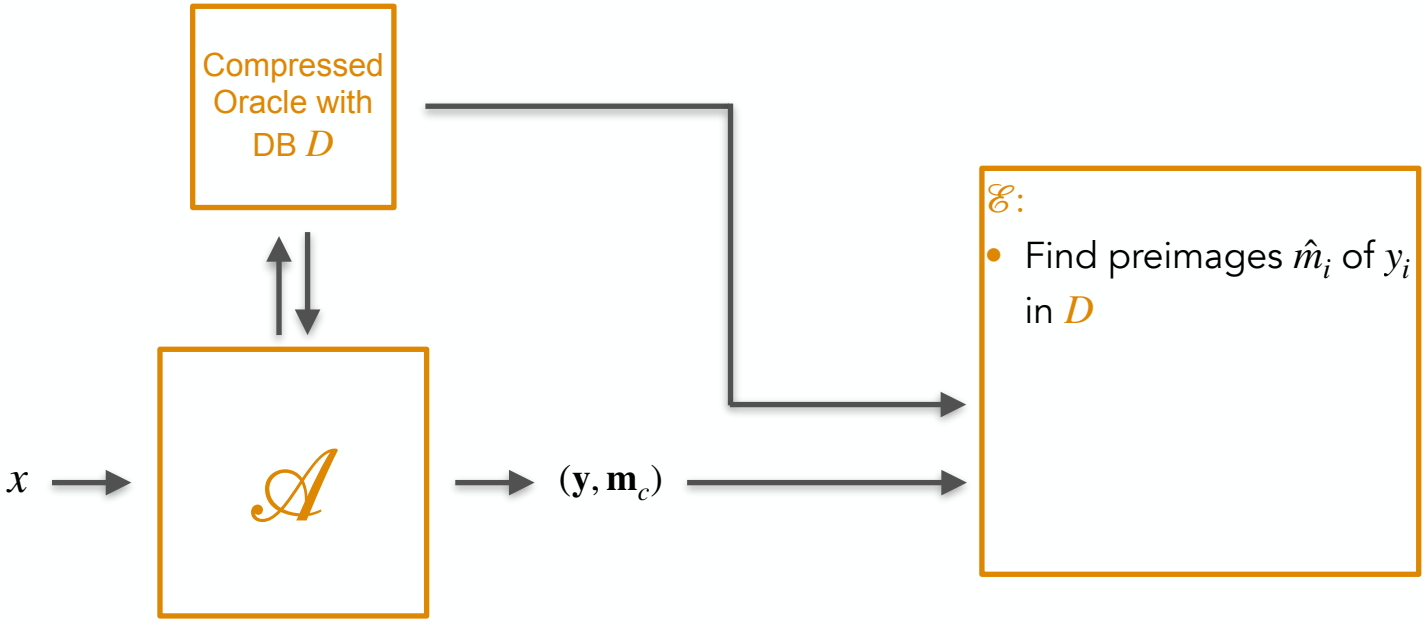
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



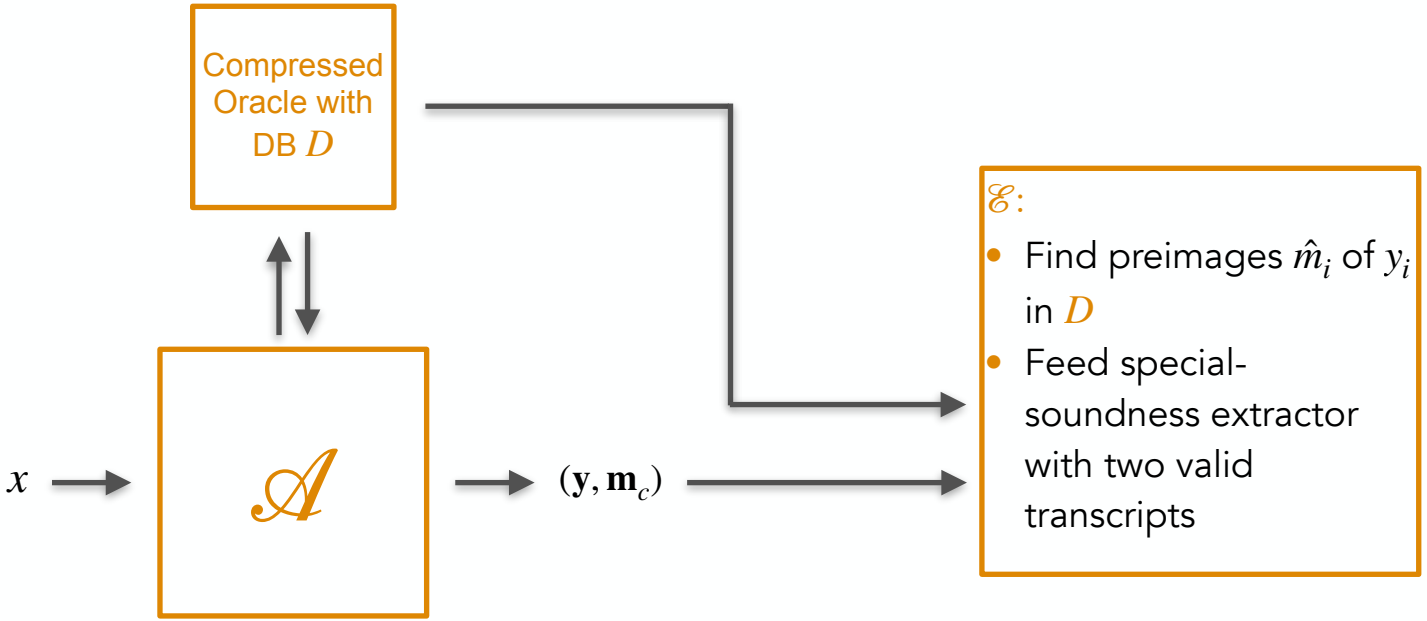
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



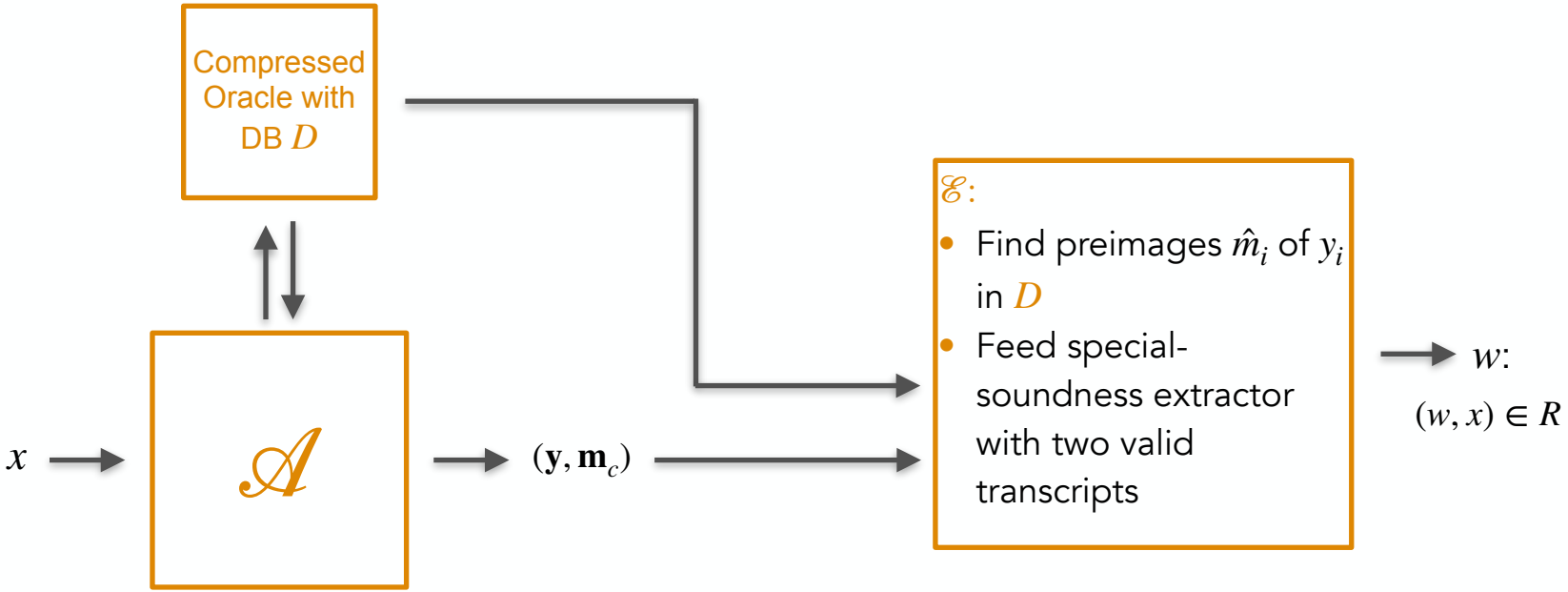
Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



Online-Extractability in the QROM

$\mathscr{A}$: Adversary against FS transform of special-sound C&O protocol



Why does it work?

$\mathscr{A}$ that succeeds such that $\mathscr{E}$ does not needs to perform an "artificial" compressed-oracle search task:

Problem: *Find valid* $\left(\mathbf{y}, \mathbf{m}_{D(x,\mathbf{y})}\right)$ *such that* (m, y_i) *for valid* m *is not in the database* D *for* $i \notin D(x, \mathbf{y})$.

Why does it work?

$\mathscr{A}$ that succeeds such that $\mathscr{E}$ does not needs to perform an "artificial" compressed-oracle search task:

Problem: *Find valid* $\left(\mathbf{y}, \mathbf{m}_{D(x,\mathbf{y})}\right)$ *such that* (m, y_i) *for valid* m *is not in the database* D *for* $i \notin D(x, \mathbf{y})$.

Query lower bounds for compressed oracles: plenty.

Why does it work?

$\mathscr{A}$ that succeeds such that $\mathscr{E}$ does not needs to perform an "artificial" compressed-oracle search task:

Problem: *Find valid* $\left(\mathbf{y}, \mathbf{m}_{D(x,\mathbf{y})}\right)$ *such that* (m, y_i) *for valid* m *is not in the database* D *for* $i \notin D(x, \mathbf{y})$.

Query lower bounds for compressed oracles: plenty.

But not if the predicate needs to read the compressed oracle database!

Main Result

Online-extractability in the QROM via artificial compressed-oracle tasks

Main Theorem

Theorem (Don, Fehr, M, Schaffner 22, informal): *For the FS transformation of a C&O protocol with any of a very general class of special-soundness-like properties there exists an online extractor that extracts a witness whenever the prover succeeds, except with negligible error, in the QROM.*

This also works in case a Merkle tree commitment is used.

Main Theorem

Theorem (Don, Fehr, M, Schaffner 22, informal): *For the FS transformation of a C&O protocol with any of a very general class of special-soundness-like properties there exists an online extractor that extracts a witness whenever the prover succeeds, except with negligible error, in the QROM.*

This also works in case a Merkle tree commitment is used.

For the proof, we generalize the compressed-oracle query lower bound framework of Chung, Fehr, Huang, Liao (Eurocrypt ’21).

Result: Online-extractability of NIZK from C&O

FS of…	Prover success probability	Extractor success probability
Arbitrary Σ, ROM	p	p^2/q or p/q
Commit-and-Open, ROM	p	p-negl$_q$(n)
Arbitrary Σ, QROM	p	p^3/q^6 or p/q^2
Commit-and-Open, QROM	p	**p-negl$_q$(n)**

Σ-protocols with collapsingness

q=number of (Q)RO queries

n=security parameter

Application: Picnic

Picnic: Fiat-Shamir DSS based on the MPC-in-the-Head paradigm

Application: Picnic

Picnic: Fiat-Shamir DSS based on the MPC-in-the-Head paradigm

- Provably secure in the QROM, based on security of the underlying block cipher (and a couple more primitives)

Application: Picnic

Picnic: Fiat-Shamir DSS based on the MPC-in-the-Head paradigm

- Provably secure in the QROM, based on security of the underlying block cipher (and a couple more primitives)
- Previously: Very much non-tight security proof with both power loss, q^c loss

Application: Picnic

Picnic: Fiat-Shamir DSS based on the MPC-in-the-Head paradigm

- Provably secure in the QROM, based on security of the underlying block cipher (and a couple more primitives)
- Previously: Very much non-tight security proof with both power loss, q^c loss
- Our result ⇒ multiplicatively tight reduction, additive error terms essentially match collision- and preimage attacks on hash function.

The CFHL21 Framework

A query lower bound framework for oracle search tasks

Query lower bounds for compressed oracles

Lemma (Zhandry '18): *If there's no pair $(x, y) \in R$ in the compressed oracle database, the oracle algorithm can't output such a pair.*

Query lower bounds for compressed oracles

Lemma (Zhandry '18): *If there's no pair* $(x, y) \in R$ *in the compressed oracle database, the oracle algorithm can't output such a pair.*

Generalizes to relations on tuples of input-output pairs. Write $D \in R$

⇒ Bounds for (multi)collision, space-time trade-offs, chain-of-values,…

Query lower bounds from transition capacities (TCs)

Query lower bounds from transition capacities (TCs)

- Classical TC: Maximum probability that a fresh pair (x, y) with random y puts D into R

Query lower bounds from transition capacities (TCs)

- Classical TC: Maximum probability that a fresh pair (x, y) with random y puts D into R
- Quantum TC: Maximum amplitude that the compressed oracle unitary converts $D \notin R$ into $D \in R$

Query lower bounds from transition capacities (TCs)

- Classical TC: Maximum probability that a fresh pair (x, y) with random y puts D into R
- Quantum TC: Maximum amplitude that the compressed oracle unitary converts $D \notin R$ into $D \in R$

Theorem (Chung, Fehr, Huang, Liao, Eurocrypt '21, very informal): *There's a closed-form quantum query bound for the task of satisfying a relation R with input-output pairs of a QRO in terms of the quantum TC.*

Removing one technical restriction allows application to our artificial search task!

Improved Unruh transform

Any Σ-protocol can become a C&O protocol!

Unruh Transform

- Less efficient than FS, but first NIZK provably secure in the QROM
- Online extractable, can be applied to any sigma-protocol
- Prover commits to a response for every possible challenge
- Requires length preserving hash for the commitment

$$a, y_i := H(z_i||r_i)_{i \in \mathcal{C}}$$

$$c = i \qquad c \xleftarrow{\$} \mathcal{C}$$

$$z_i, r_i$$

$$V(x, a, z_i) \in \{\text{accept}, \text{reject}\}$$
$$H(z_i||r_i) = y_i$$

Unruh Transform

- Less efficient than FS, but first NIZK provably secure in the QROM
- Online extractable, can be applied to any sigma-protocol
- Prover commits to a response for every possible challenge
- Requires length preserving hash for the commitment

$$a, y_i := H(z_i||r_i)_{i \in \mathcal{C}}$$

$$c = i \qquad c \xleftarrow{\$} \mathcal{C}$$

$$z_i, r_i$$

$$V(x, a, z_i) \in \{\text{accept}, \text{reject}\}$$
$$H(z_i||r_i) = y_i$$

It's a C&O protocol!

Unruh Transform

- Less efficient than FS, but first NIZK provably secure in the QROM
- Online extractable, can be applied to any sigma-protocol
- Prover commits to a response for every possible challenge
- ~~Requires length preserving hash for the commitment~~
- Can use Merkle tree commitment

$$a, y_i := H(z_i||r_i)_{i \in \mathcal{C}} \rightarrow$$

$$\leftarrow c = i \quad c \xleftarrow{\$} \mathcal{C}$$

$$\rightarrow z_i, r_i$$

$$V(x, a, z_i) \in \{\text{accept}, \text{reject}\}$$
$$H(z_i||r_i) = y_i$$

Summary

- We give the first tight QROM reduction of Fiat-Shamir NIZKs for the subclass of C&O protocols
- The reduction works on Merkle-C&O
- ⇒Tight QROM reduction for the Picnic signature scheme
- More efficient Unruh transform

The End!

Questions?