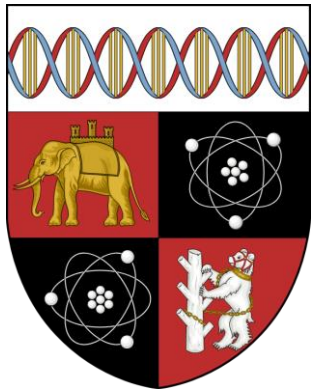
Feistel Tools: Reprogramming and Query-Recording for QRPs

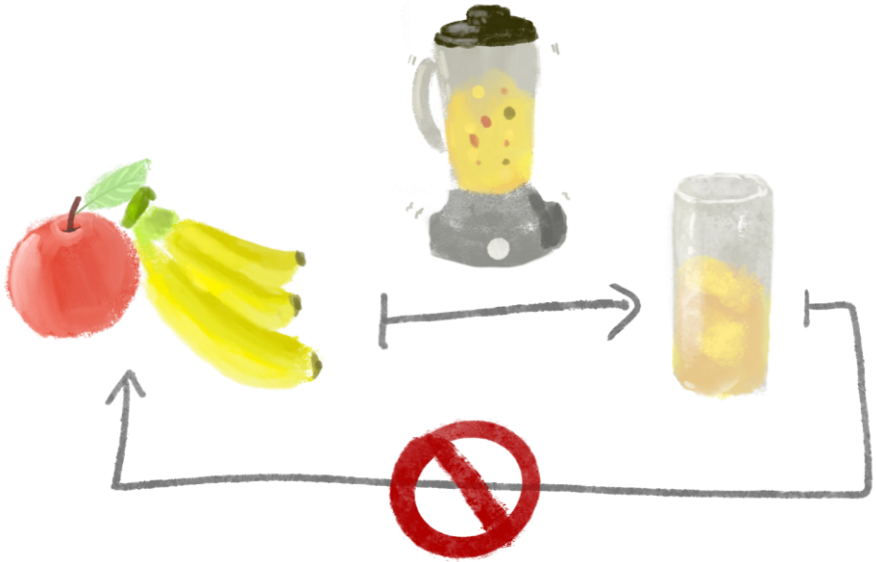
Yu-Hsuan Huang, Andreas Hülsing,
Varun Maram, Silvia Ritsch, Abishanka Saha



Illustrations/slides due to Yu-Hsuan, Silvia, ChatGPT, and online meme generator.

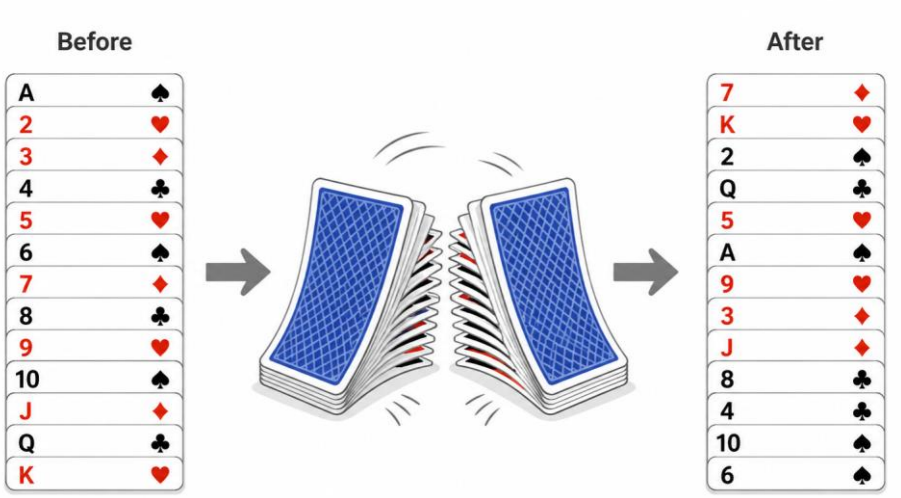
Symmetric Primitives...

One-Way Functions:
Easy to evaluate, hard to invert.



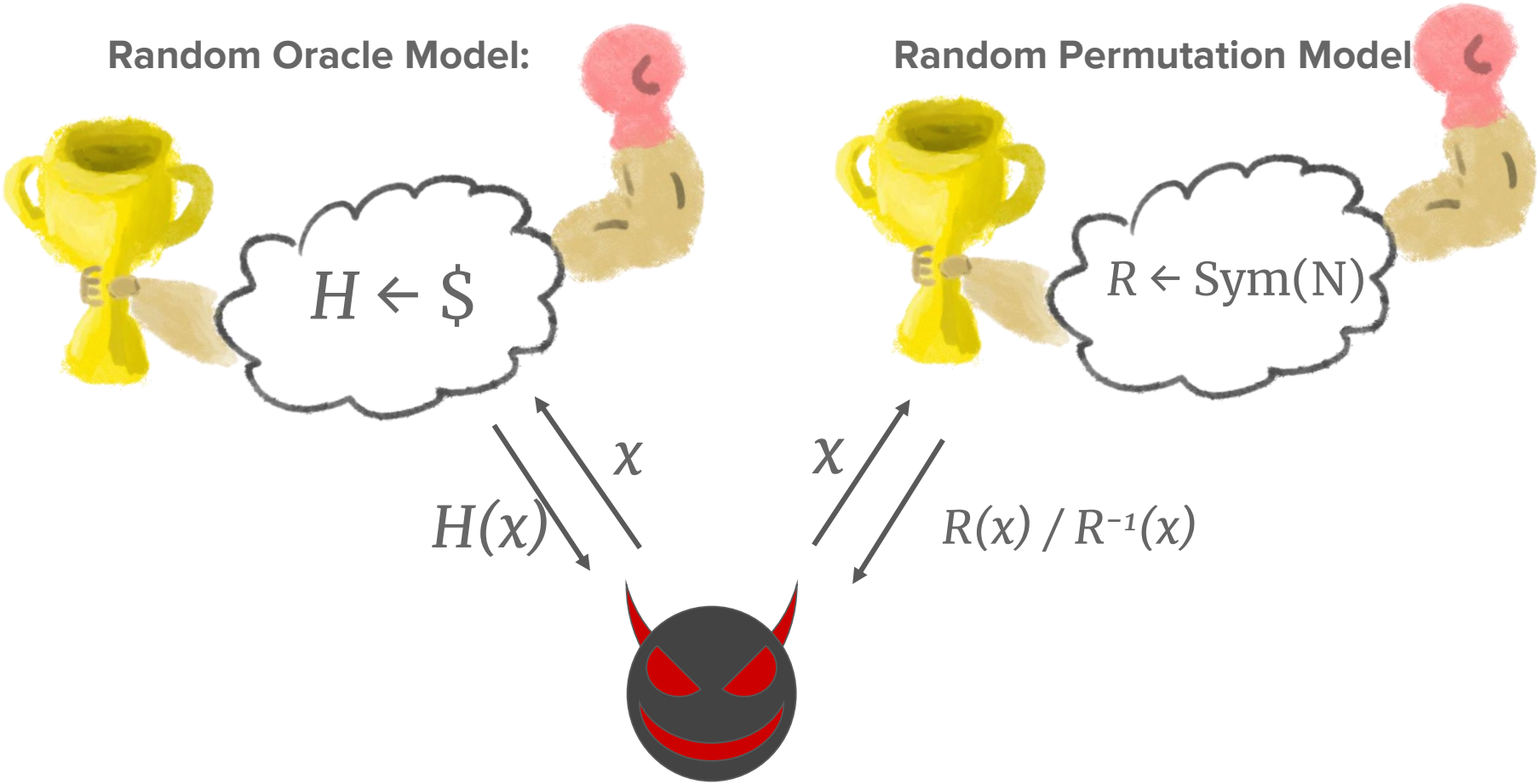
hash function, compression function ...

Permutations:
Easy to evaluate, often easy to invert.

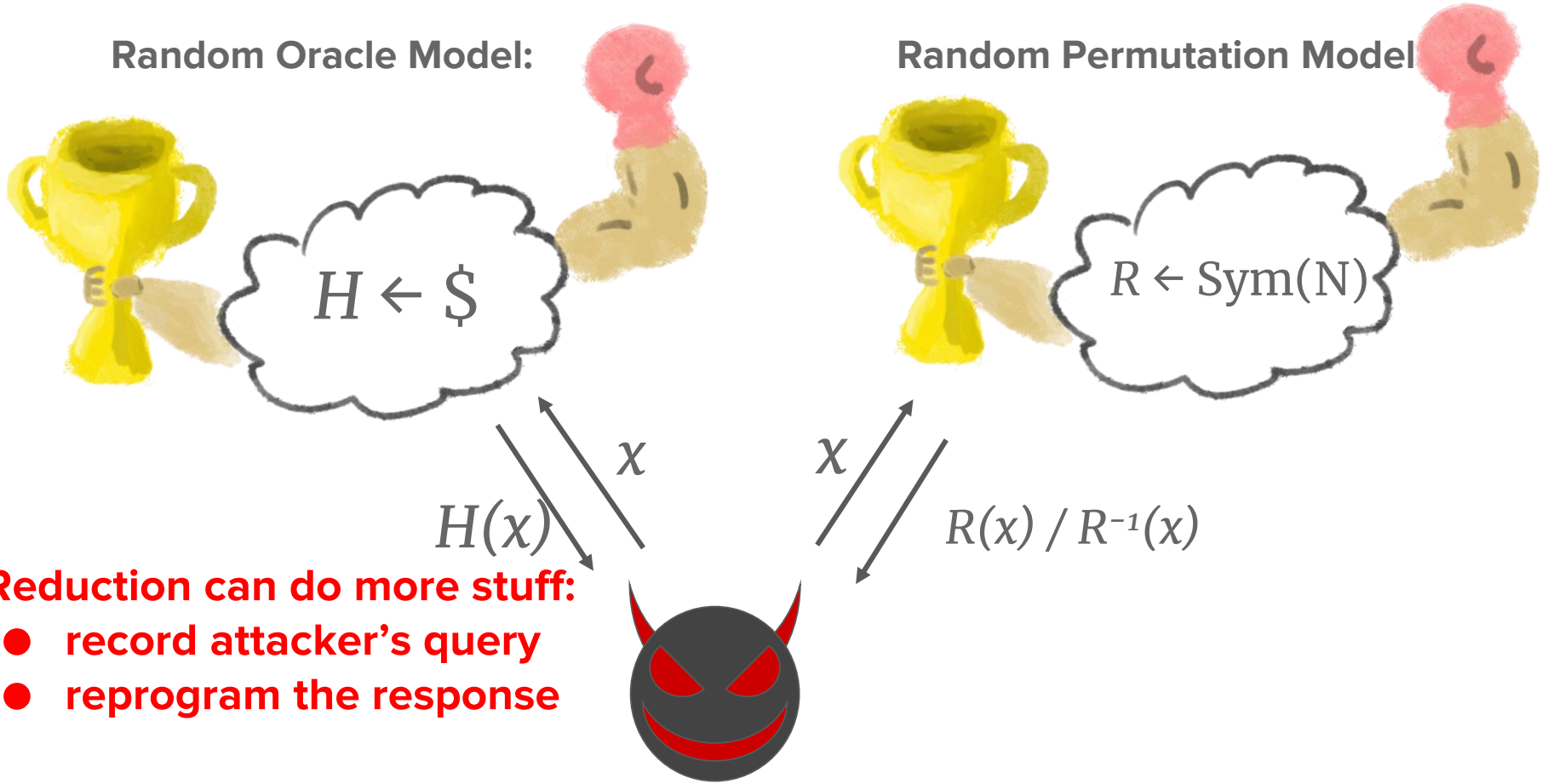


(fixed key) block cipher, round of sponge ...

Symmetric Primitives...



Symmetric Primitives...



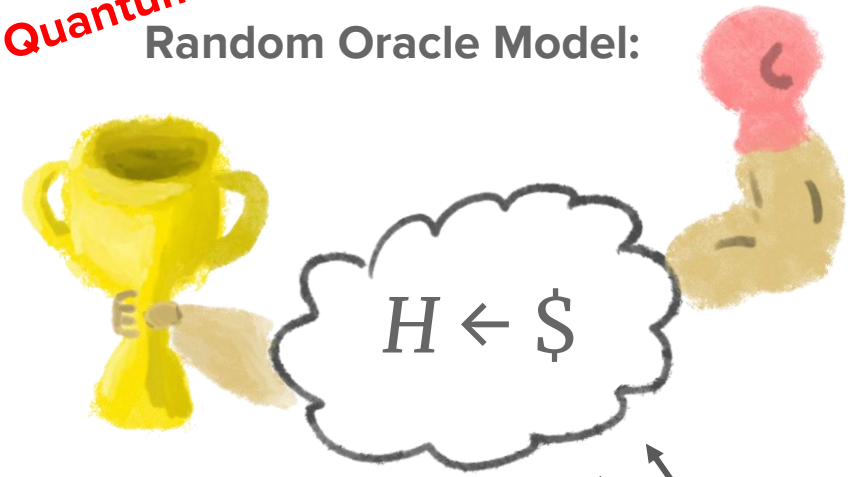
Reduction can do more stuff:

- **record attacker's query**
- **reprogram the response**

Symmetric Primitives...

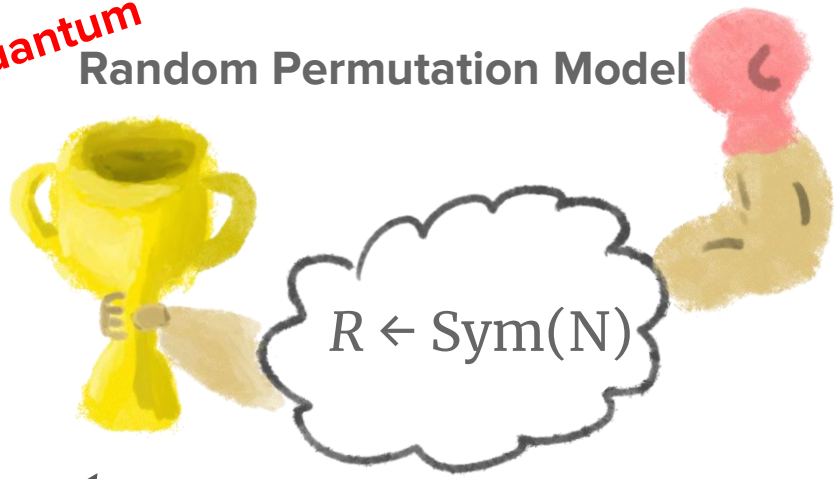
Quantum

Random Oracle Model:



Quantum

Random Permutation Model



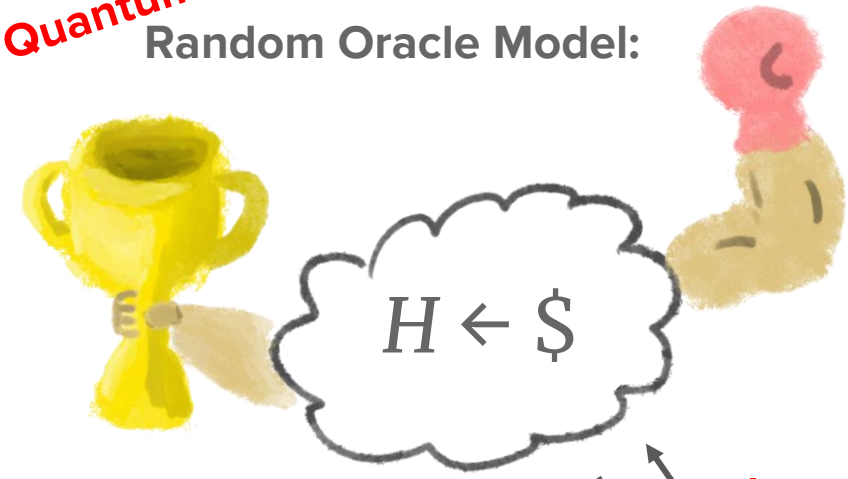
$|x\rangle$ $|x\rangle$

$|H(x)\rangle$ $|R(x)\rangle$ / $|R^{-1}(x)\rangle$

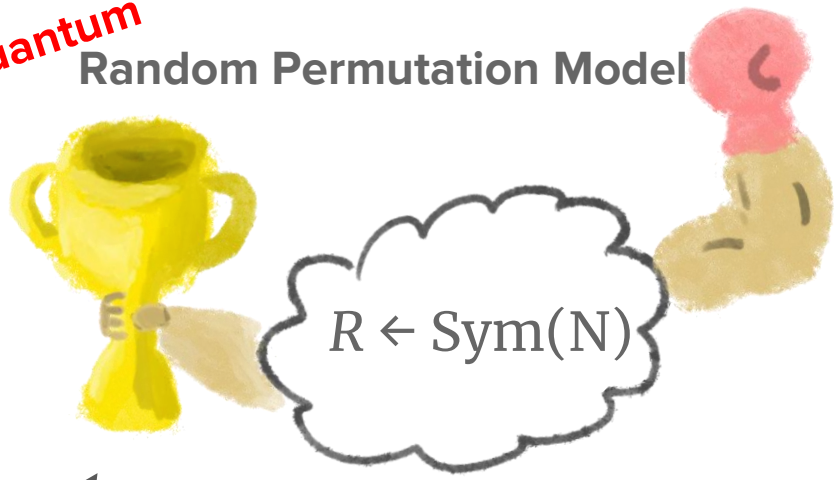
- record attacker's query?
- reprogram the response?

Symmetric Primitives...

Quantum Random Oracle Model:



Quantum Random Permutation Model



$|x\rangle$ $|x\rangle$

$|H(x)\rangle$ $|R(x)\rangle$ / $|R^{-1}(x)\rangle$

No cloning theorem?

- record attacker's query?
- reprogram the response?

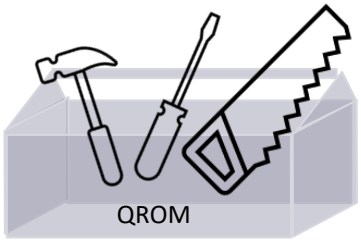
superposition response?

The Gap in Existing Toolboxes

Quantum Random Oracle Model:

Rich QROM toolbox:

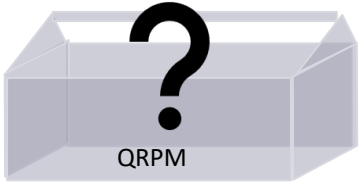
- **Query recording**
- **many flavours of reprogramming:**
  - **measure and reprogram**
  - **one-way to hiding**
  - **adaptive reprogramming**
- **Techniques for auxiliary inputs**
- **many more…**



Quantum Random Permutation Model:

Not a lot is known for QRPM:

- **Almost no, or very restricted, query recording** [MMW24]
- **Some reprogramming tools proven via tailored approach** [ABKM21, CHLYY25]
- **Almost no auxiliary-input techniques**



The Gap in Existing Toolboxes

Quantum Random Oracle Model:

Quantum P…om Permutation Model:

Rich QROM …

- Query reco…
- …
  - mea…
  - adaptive re…
- Techniques for auxiliary inpu…
- many more…

…via

…21, CHLYY25]

…auxiliary …chniques

This work: a generic lifting of QROM tools → QRPM tools!

Concurrent: compressed permutation oracle, albeit with a big loss [Carolan25]

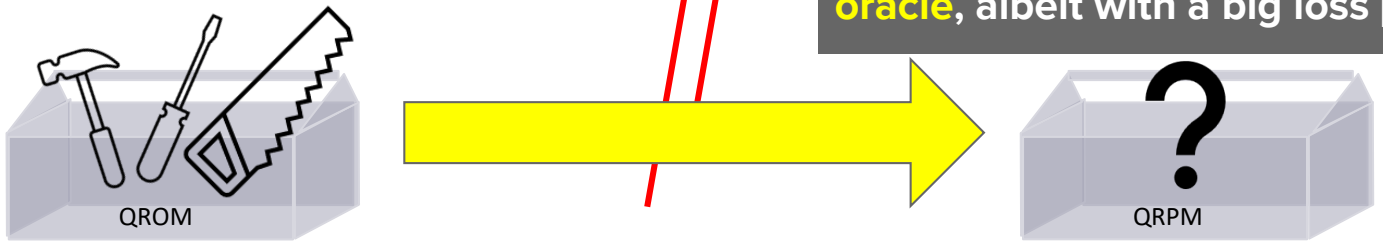


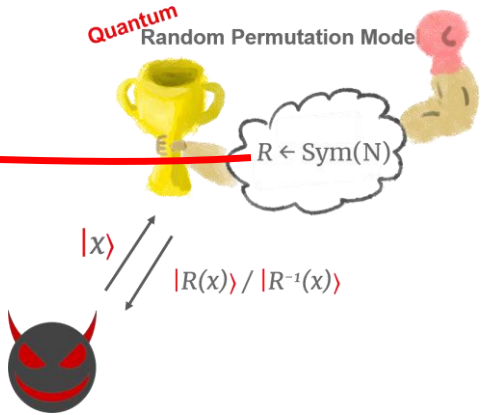
Table of Contents

Core Idea

Generically lifting
QROM tools → QRPM tools!

Functions → Permutations

simulate using
random functions?

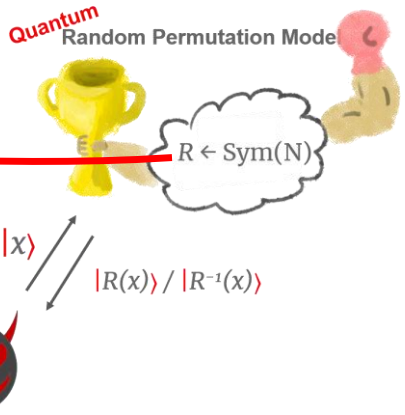


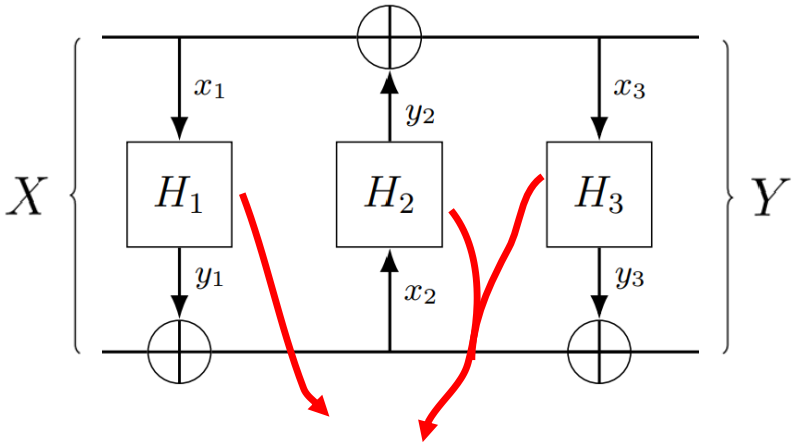
Core Idea

Generically lifting QROM tools → QRPM tools!

Functions ⟹ **Permutations**

[3-round Feistel]





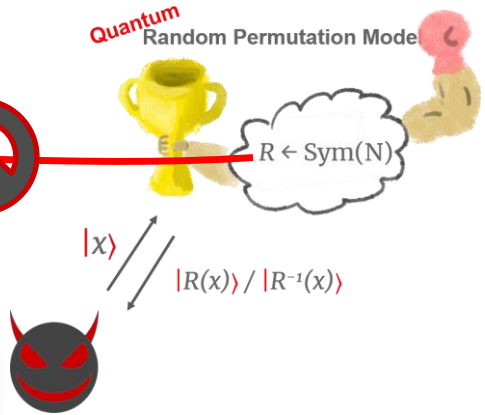
random functions

Core Idea

Generically lifting
QROM tools → QRPM tools!

Functions → Permutations

[3-round Feistel]



Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation

Hidenori Kuwakado
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

Masakatu Morii
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

***Abstract*—No polynomial classical algorithms can distinguish between the 3-round Feistel cipher with internal permutations and a random permutation. It means that the 3-round Feistel cipher with internal permutations is secure against any chosen plaintext attack on the classical computer. This paper shows that there exists a polynomial quantum algorithm for distinguishing them. Hence, the 3-round Feistel cipher with internal permutations may be insecure against a chosen plaintext attack on a quantum computer. This distinguishing problem is an instance that can be efficiently solved by exploiting the quantum parallelism. The proposed algorithm is the first application of Simon's algorithm to cryptographic analysis.**

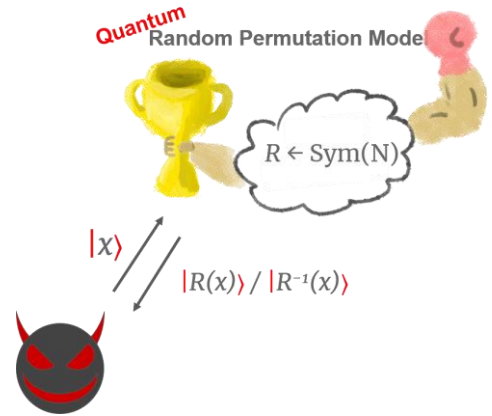
Precisely speaking, we discuss the (in)distinguishability of the unitary operator for computing the Feistel cipher from the unitary operator for computing the random permutation. Since the Feistel cipher is a classical cipher, one may think that the comparison of unitary operators is meaningless. However, if quantum computers are inexpensively realized in feature, then even classical ciphers will be implemented on quantum computers. In such a situation, an adversary will have access to the unitary operator instead of the classical oracle. Hence, it is significant to study the (in)distinguishability in the context of quantum algorithms.

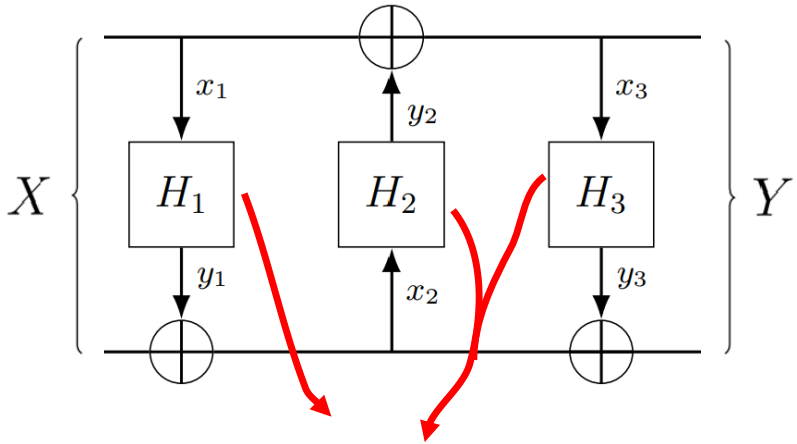
Core Idea

Generically lifting
QROM tools → QRPM tools!

Functions → Permutations

[3-round Feistel]





random functions

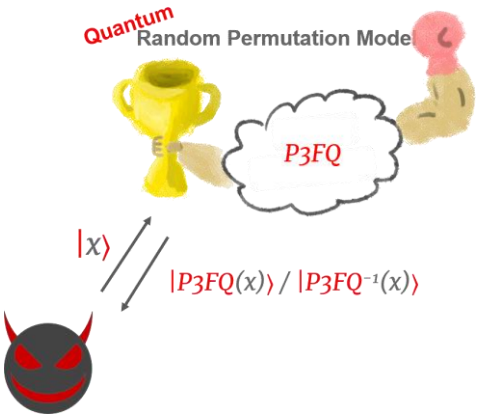
Core Idea

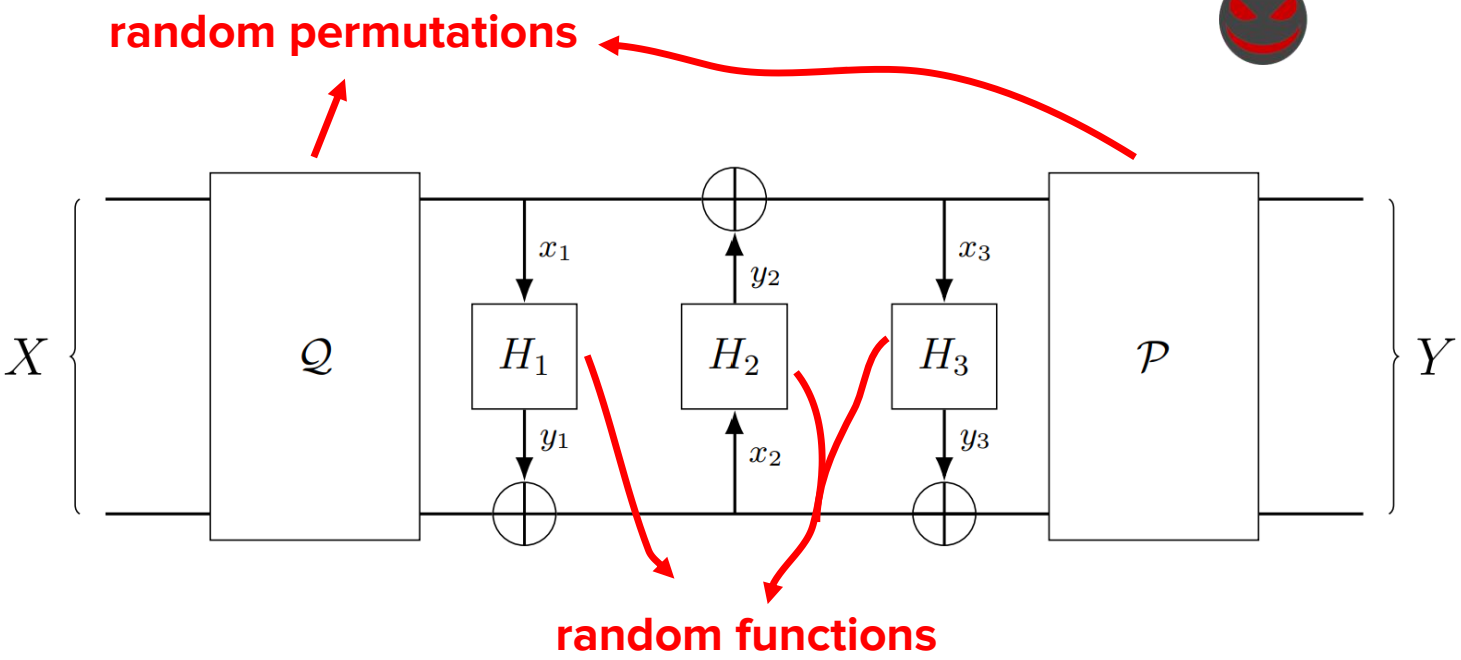
Generically lifting
QROM tools → QRPM tools!

Functions → Permutations

P3FQ

$$Y = P \circ [3\text{-round Feistel}] \circ Q(X)$$





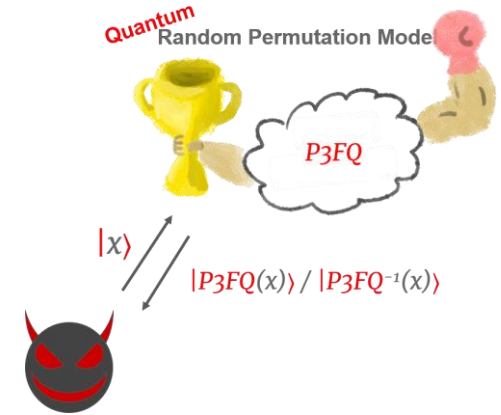
Core Idea

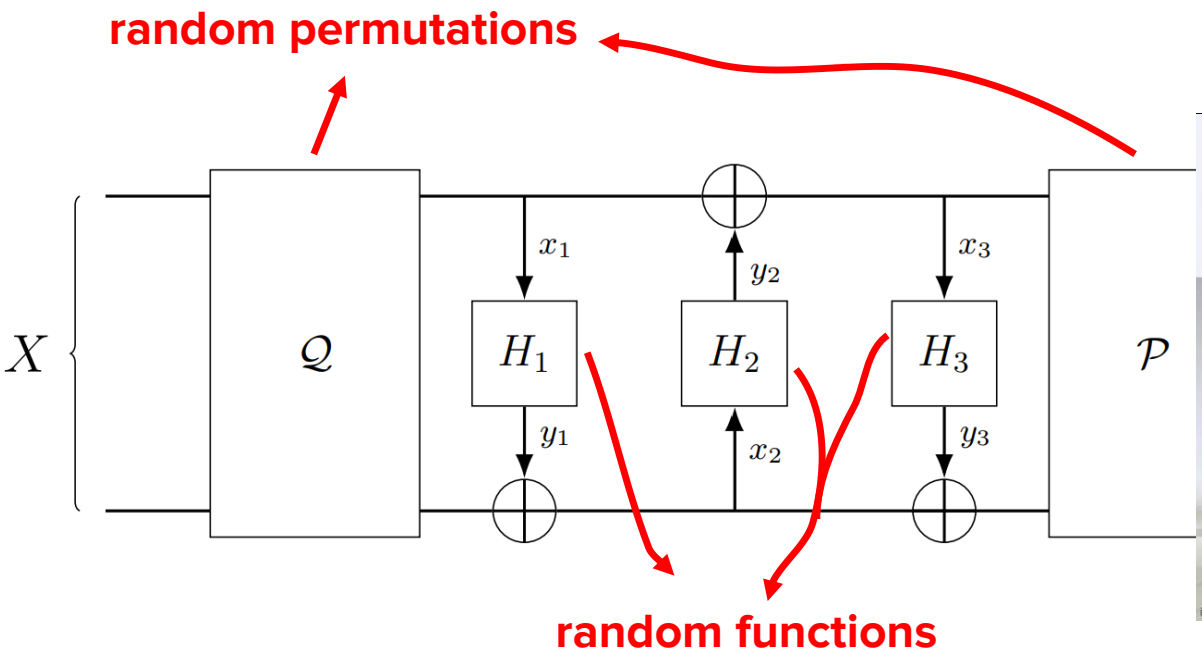
Generically lifting
QROM tools → QRPM tools!

Functions → Permutations

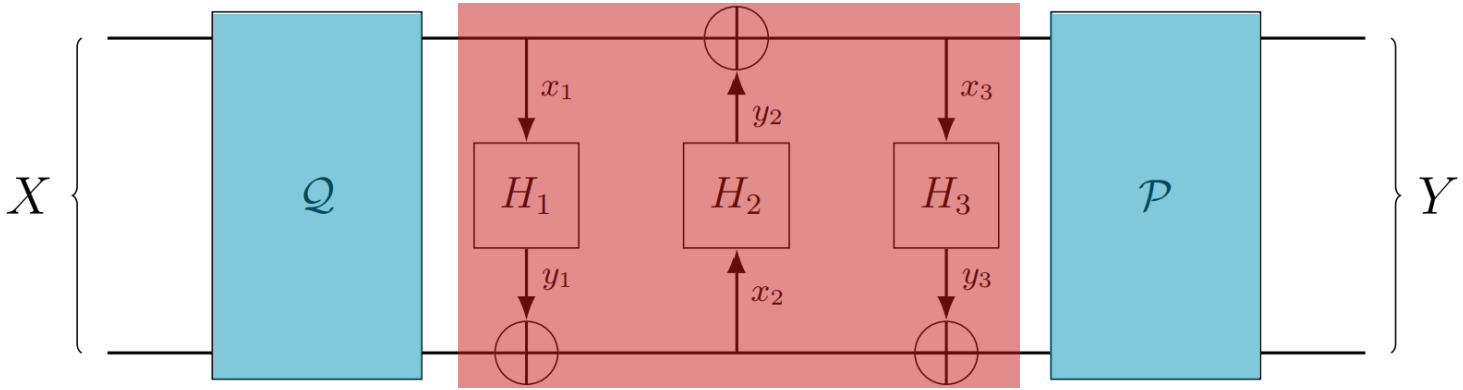
P3FQ

$$Y = P \circ [3\text{-round Feistel}] \circ Q(X)$$





Core Idea



Outer random permutations:

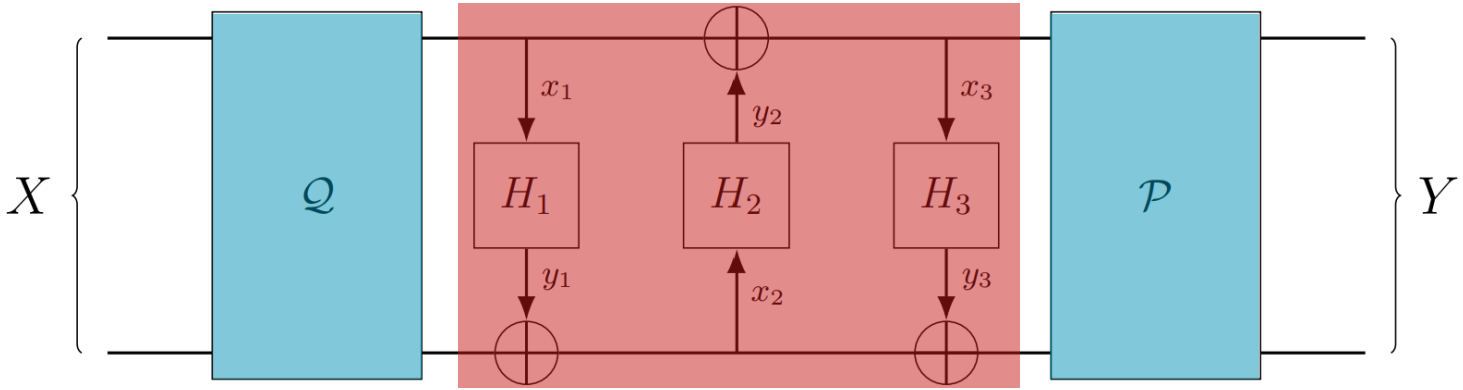
- **provide indistinguishability**
- **hide internal Feistel, and hide each other.**

Inner random oracles smuggle QROM tools:

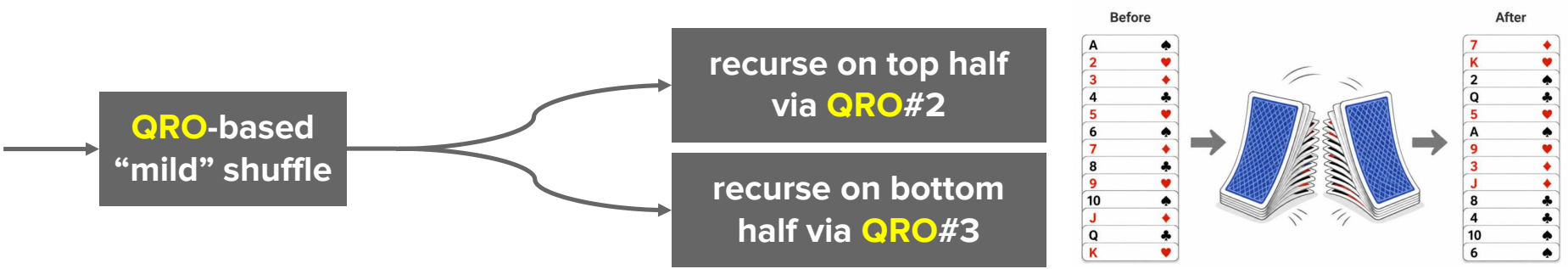
- **reprogramming**
- **query recording, etc.**

Core Idea

Also: ∃ efficient (stateful) simulation

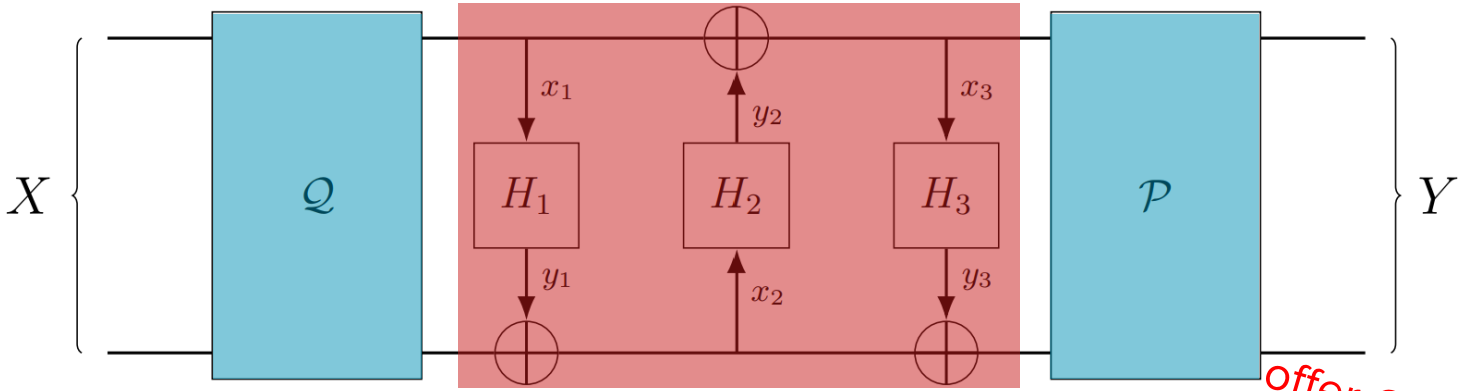


1. **QRO simulation** via Zhandry's compressed oracle technique
2. **QRP simulation** via the "mix-and-cut" technique:



Core Idea

Also: ∃ efficient (stateful) simulation



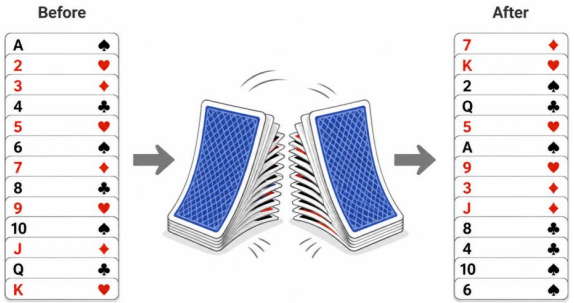
offer QROM tools

1. **QRO simulation** via Zhandry's compressed oracle technique
2. **QRP simulation** via the "mix-and-cut" technique:

QRO-based "mild" shuffle

→ **recurse on top half via QRO#2**

→ **recurse on bottom half via QRO#3**



Liftable QROM Techniques

How to Record Quantum Queries, and Applications to Quantum Indifferentiability

Abstract. The quantum random oracle model (QROM) has become the standard model in which to prove the post-quantum security of random-oracle-based constructions. Unfortunately, none of the known proof techniques allow the reduction to record information about the adversary's queries, a crucial feature of many classical ROM proofs, including all proofs of indifferentiability for hash function domain extension.
In this work, we give a new QROM proof technique that overcomes

Liftable QROM Techniques

How to Record Quantum Queries, and Applications to Quantum Indifferentiability

Abstract. The quantum random oracle model (QROM) has become the standard model in which to prove the post-quantum security of
unately, none of the known
d information about the ad-
ssical ROM proofs, including
ion domain extension.
technique that overcomes

Tight adaptive reprogramming in the QROM

Alex B. Grilo[1], Kathrin Hövelmanns[2], Andreas Hülsing[3], and Christian Majenz[4]

[1] Sorbonne Université, CNRS, LIP6, France
[2] Ruhr-Universität Bochum, Germany
[3] Eindhoven University of Technology, The Netherlands
[4] Centrum Wiskunde & Informatica and QuSoft, Amsterdam, The Netherlands
authors-qrom-reprog@huelsing.net

Abstract. The random oracle model (ROM) enjoys widespread popularity, mostly because it tends to allow for *tight* and *conceptually simple* proofs where provable security in the standard model is elusive or costly. While being the adequate replacement of the ROM in the post-quantum security setting, the quantum-accessible random oracle model (QROM) has thus far failed to provide these advantages in many settings. In this work, we focus on *adaptive reprogrammability*, a feature of the ROM enabling tight and simple proofs in many settings. We show that the straightforward quantum-accessible generalization of adaptive reprogramming is

Liftable QROM Techniques

How to Record Quantum Queries, and Applications to Quantum Indifferentiability

Abstract.
the standa

Tight adaptive reprogramm

Alex B. Grilo[1], Kathrin Hövelmanns[2], Andreas

[1] Sorbonne Université, CNRS
[2] Ruhr-Universität Bochun
[3] Eindhoven University of Technolo
[4] Centrum Wiskunde & Informatica and QuSof
authors-qrom-reprog@hue

Abstract. The random oracle model (ROM) enjoys w
tends to allow for *tight* and *conceptually simple* proofs
model is elusive or costly. While being the adequate
quantum security setting, the quantum-accessible ra
far failed to provide these advantages in many settin
reprogrammability, a feature of the ROM enabling tight and simple proofs in many settings. We show that the straightforward quantum-accessible generalization of adaptive reprogramming is

Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model*

Jelle Don[1,2], Serge Fehr[1,3,4], Christian Majenz[2,4], and Christian Schaffner[2,4]

[1] Centrum Wiskunde & Informatica (CWI), Amsterdam, Netherlands
[2] Institute for Logic, Language and Computation, University of Amsterdam, Amsterdam, Netherlands
[3] Mathematical Institute, Leiden University, Netherlands
[4] QuSoft, Amsterdam, Netherlands
jelle.don@cwi.nl, serge.fehr@cwi.nl, c.majenz@uva.nl, c.schaffner@uva.nl

Abstract. The famous Fiat-Shamir transformation turns any public-coin three-round interactive proof, i.e., any so-called Σ-protocol, into a non-interactive proof in the random-oracle model. We study this transformation in the setting of a *quantum adversary* that in particular may query the random oracle in quantum superposition.
Our main result is a generic reduction that transforms any quantum dishonest prover attacking the Fiat-Shamir transformation in the quantum random-oracle model into a similarly successful quantum dishonest prover attacking the underlying Σ-protocol (in the standard model). Applied to the standard soundness and proof-of-knowledge definitions, our reduction implies that both these security properties,

Liftable QROM Techniques

Tight adaptive reprog

Alex B. Grilo[1], Kathrin Hövelmanns[2], .

[1] Sorbonne Universit
[2] Ruhr-Universitä
[3] Eindhoven University of
[4] Centrum Wiskunde & Informatica a
authors-qrom-re

Abstract. The random oracle model (ROM) tends to allow for *tight* and *conceptually simpl* model is elusive or costly. While being the a quantum security setting, the quantum-acce far failed to provide these advantages in ma *reprogrammability*, a feature of the ROM enab show that the straightforward quantum-access

r Transformation
-Oracle Model*

[2,4], and Christian Schaffner[2,4]

, Amsterdam, Netherlands
y of Amsterdam, Amsterdam, Netherlands
iversity, Netherlands
therlands
z@uva.nl, c.schaffner@uva.nl

y public-coin three-round interactive proof, n the random-oracle model. We study this in particular may query the random oracle

y quantum dishonest prover attacking the model into a similarly successful quantum standard model). Applied to the standard implies that both these security properties,

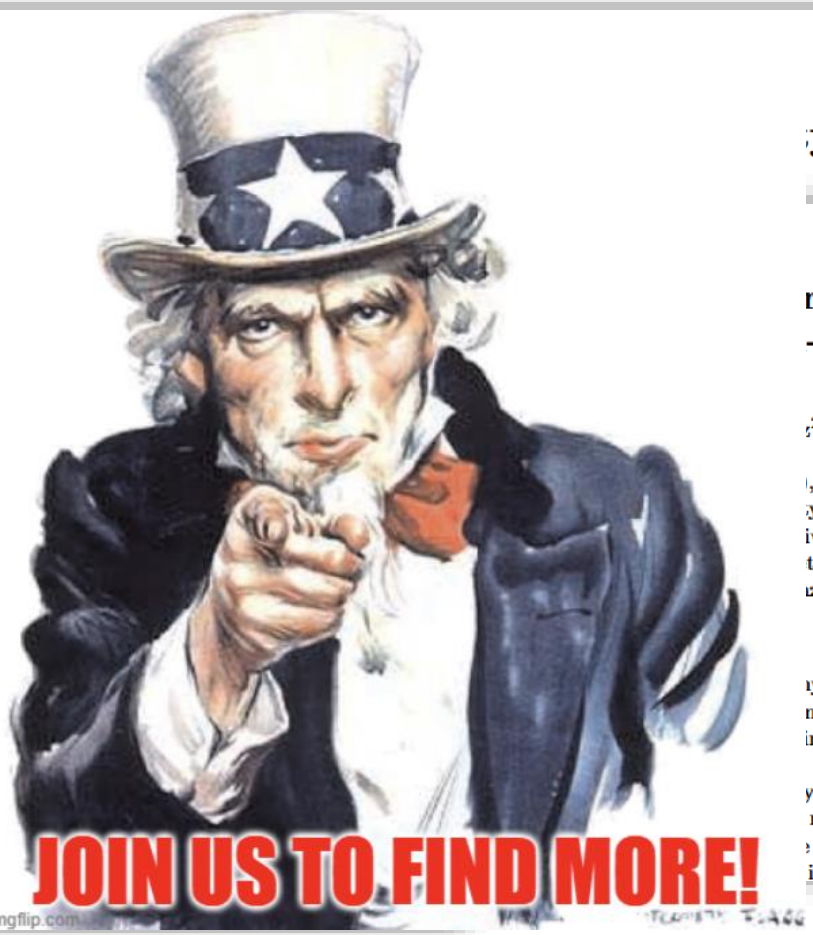
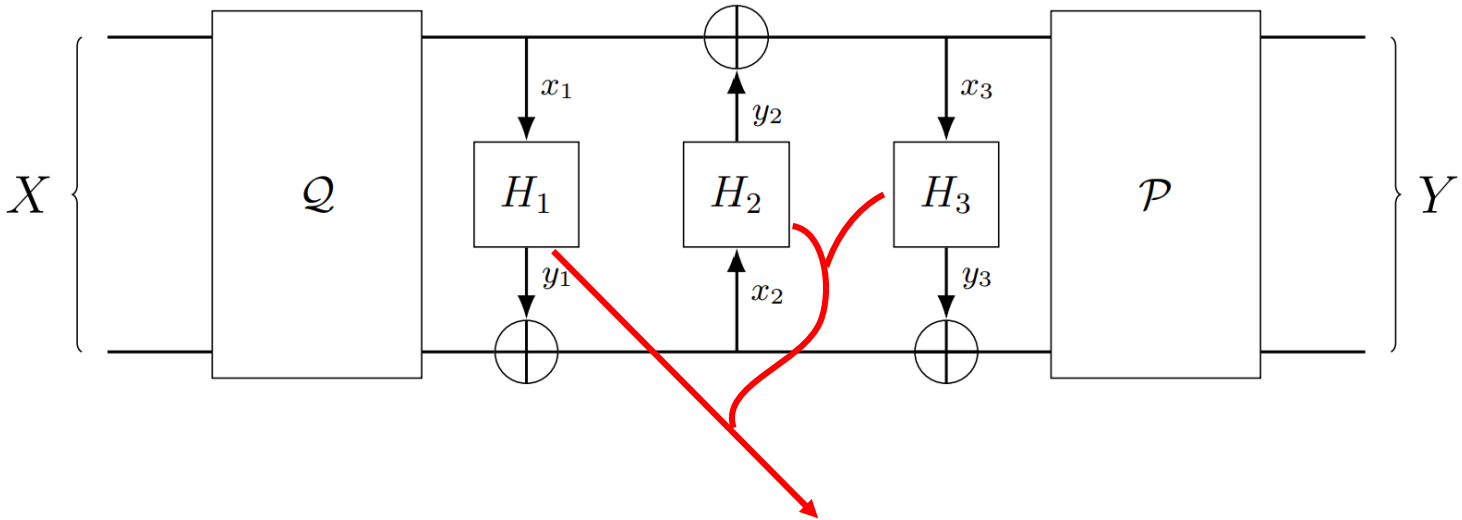


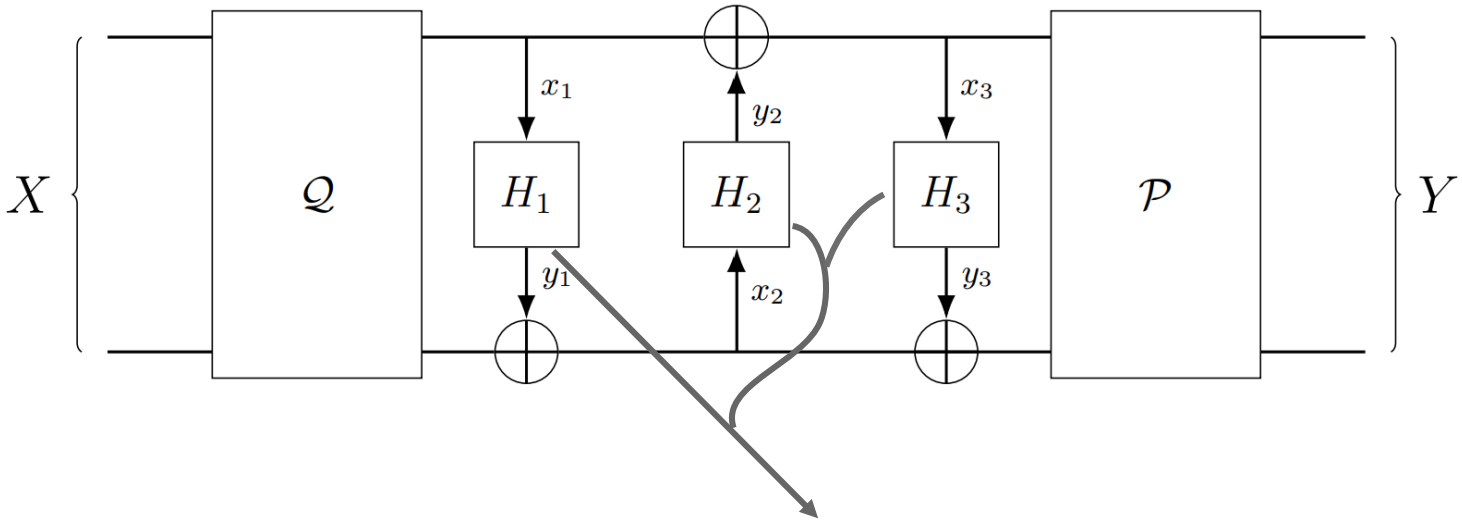
Table of Contents

Lifting Query Recording



Compressed oracle: record H_1, H_2, H_3 queries

Lifting Query Recording

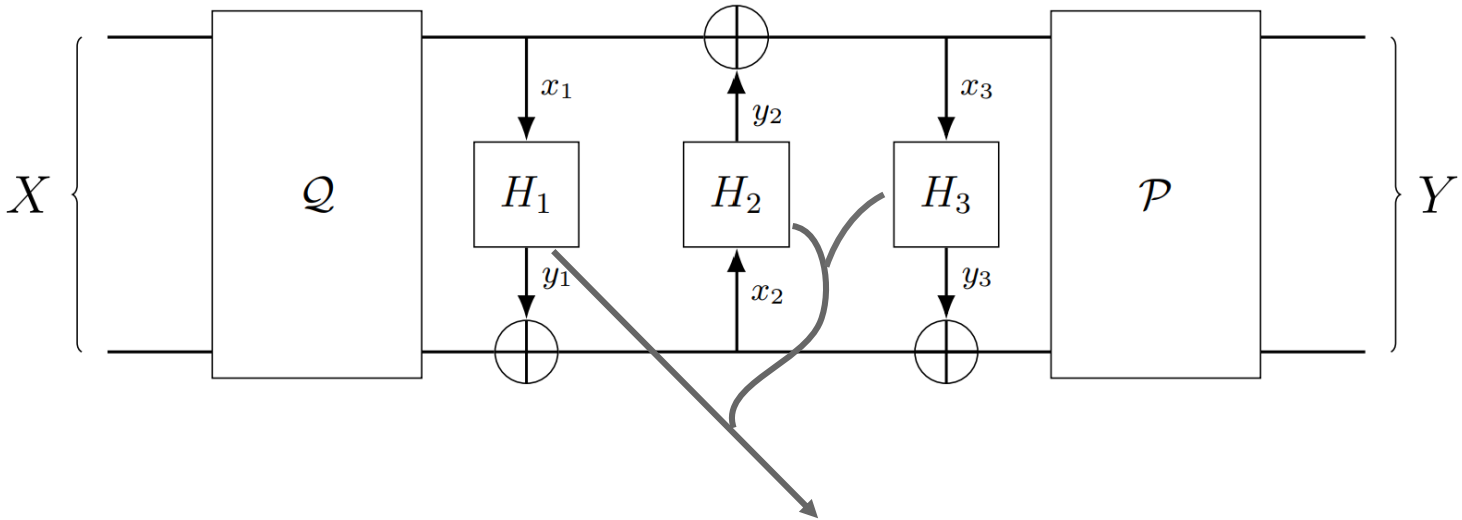


Compressed oracle: record H_1, H_2, H_3 queries

For P3FQ: record (X, Y) if ∃ "consistent chain":

$Q(X) = (x_1 , y_1 \oplus x_2)$ and $P(x_3 , x_2 \oplus y_3) = Y$ and $x_1 \oplus x_3 = y_2$

Lifting Query Recording



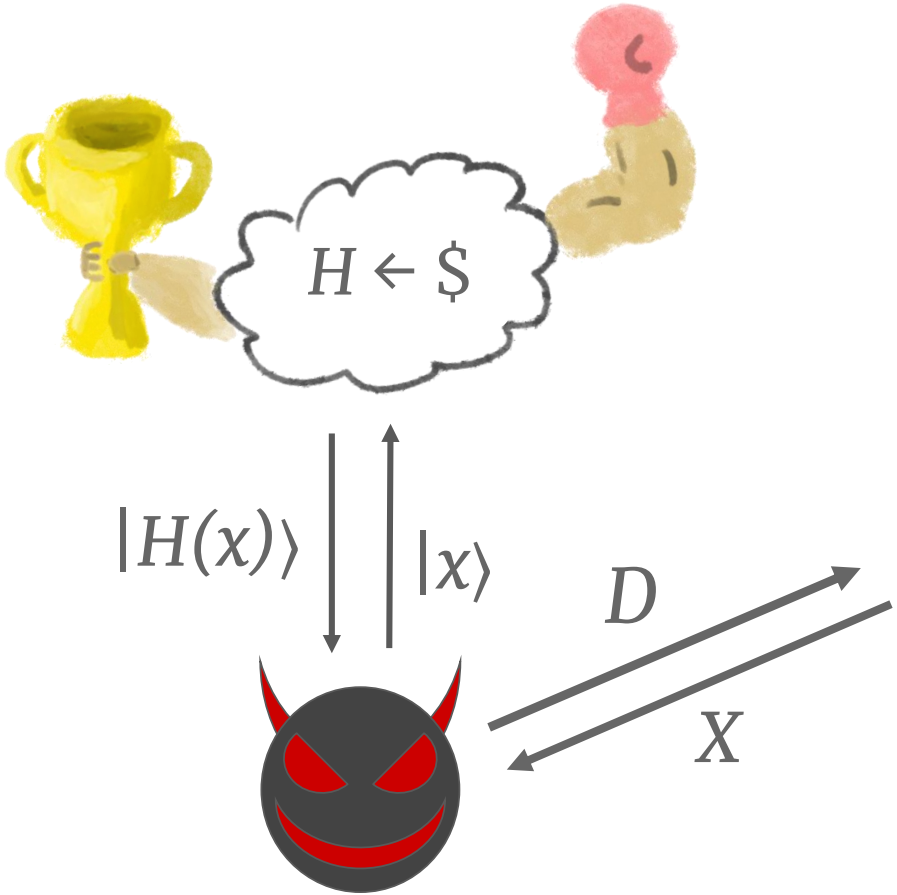
Compressed oracle: record H_1, H_2, H_3 queries

For P3FQ: record (X, Y) if ∃ "consistent chain":
$Q(X) = (x_1, y_1 \oplus x_2)$ and $P(x_3, x_2 \oplus y_3) = Y$ and $x_1 \oplus x_3 = y_2$

We **recover existing lower bounds**: double-sided zero search, i.e., find $R(x, 0^n) = (y, 0^n)$
and **obtain new lower bounds**: finding k > q input-output pairs of $R(\cdot)$ in q queries

Table of Contents

Lifting Adaptive Reprogramming



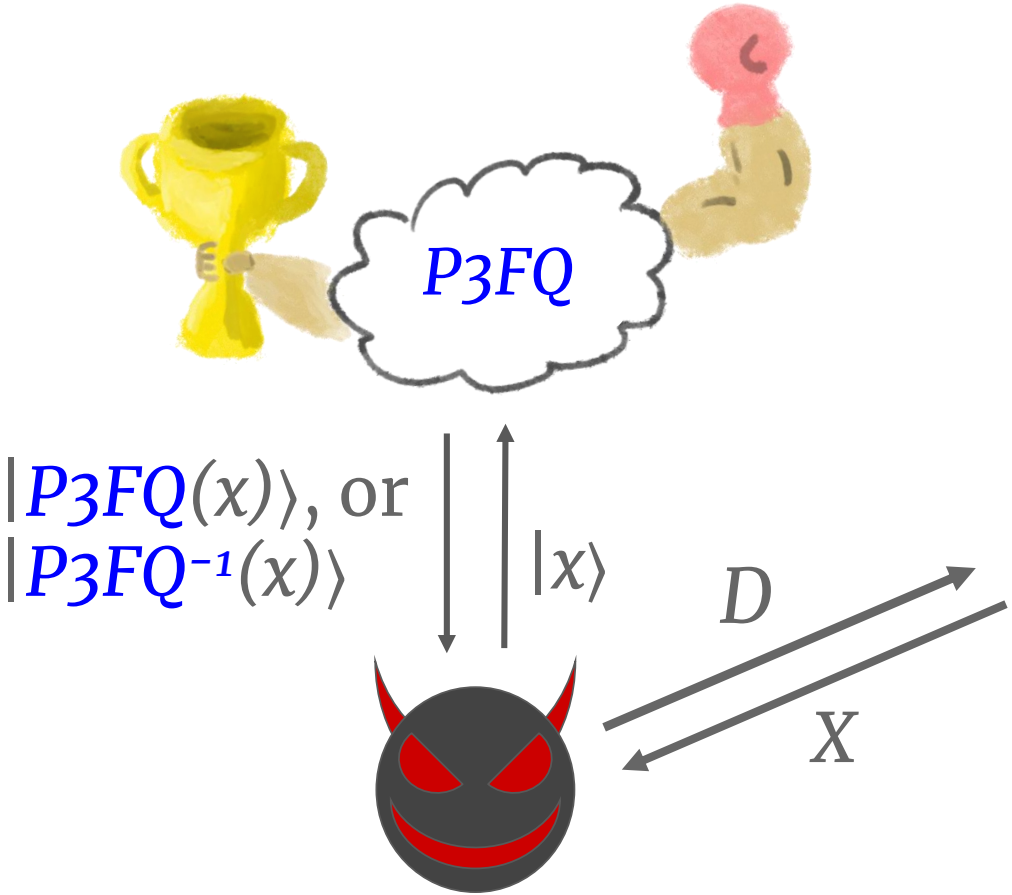
[GHHM21] theorem: Indistinguishable for D with high min-entropy.

$No\ Prog(D)$
1. $X \leftarrow D$

or ≈

$Prog(D)$
1. $X \leftarrow D$
2. $H(X) := \$$

Lifting Adaptive Reprogramming



Our lifting theorem:
Indistinguishable for D with high min-entropy.

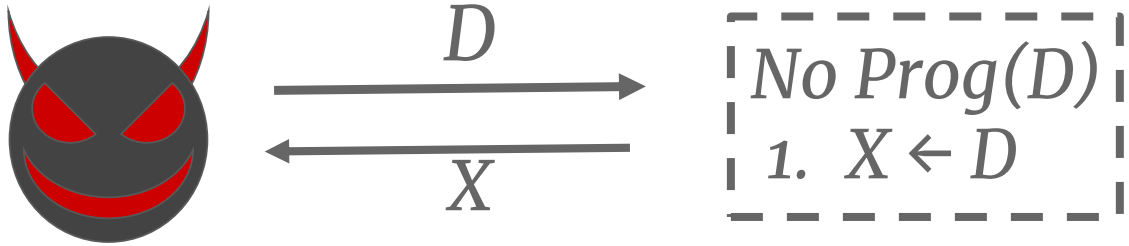
No Prog(D)
1. $X \leftarrow D$

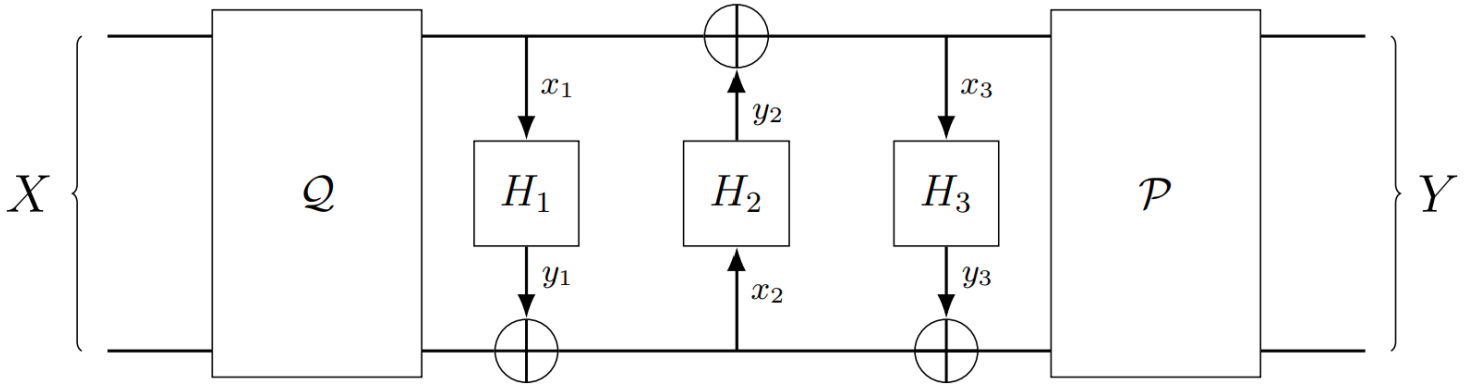
or ≈

Prog(D)
1. $X \leftarrow D$
2. *"P3FQ(X) := $"*

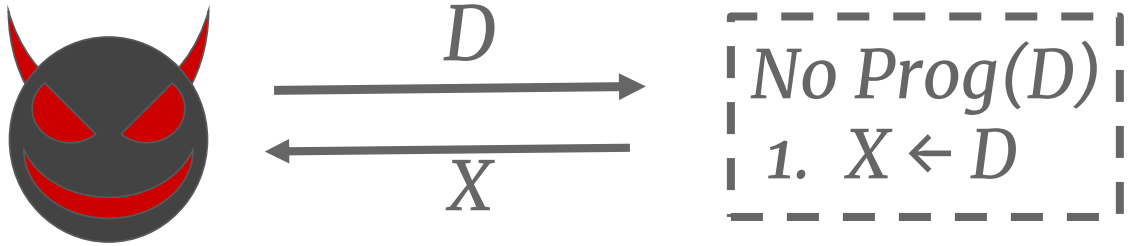
Interlude

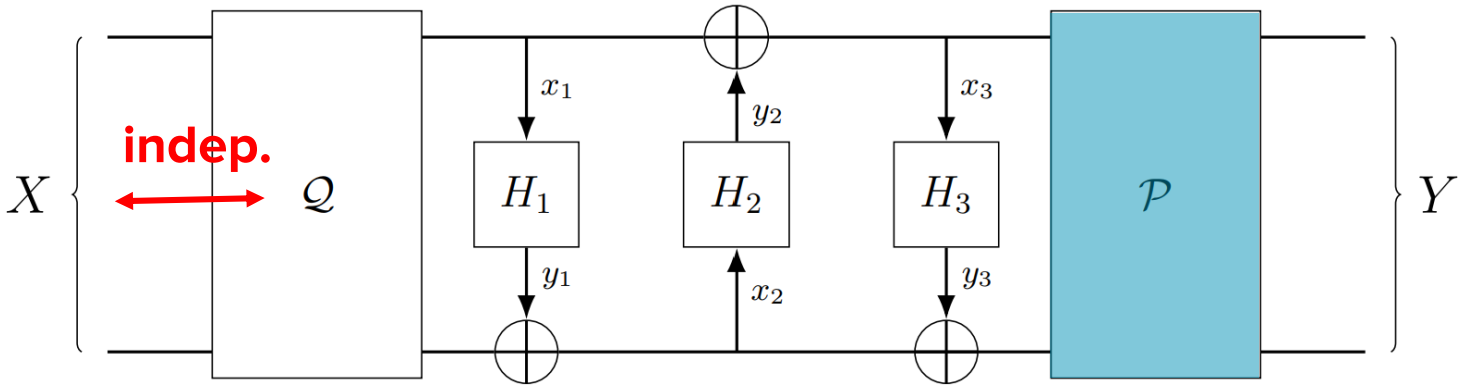
Lifting Adaptive Reprogramming





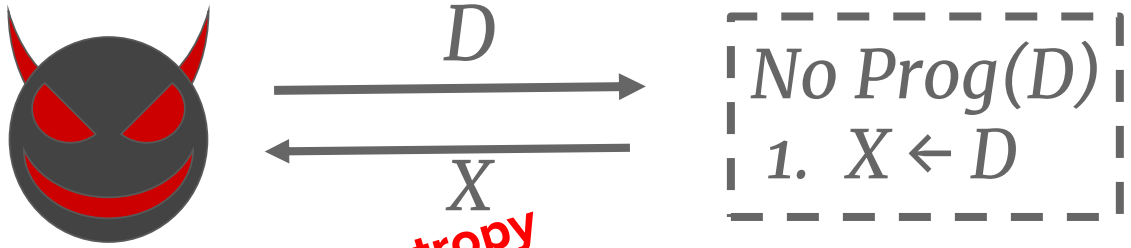
Lifting Adaptive Reprogramming

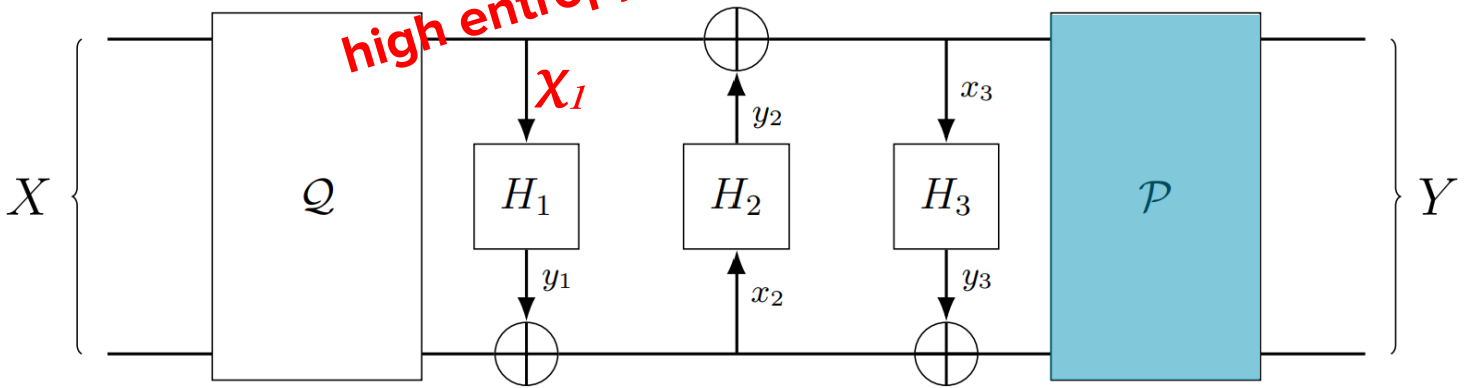




P is masking Q ⇒ X is indep. of Q

Lifting Adaptive Reprogramming

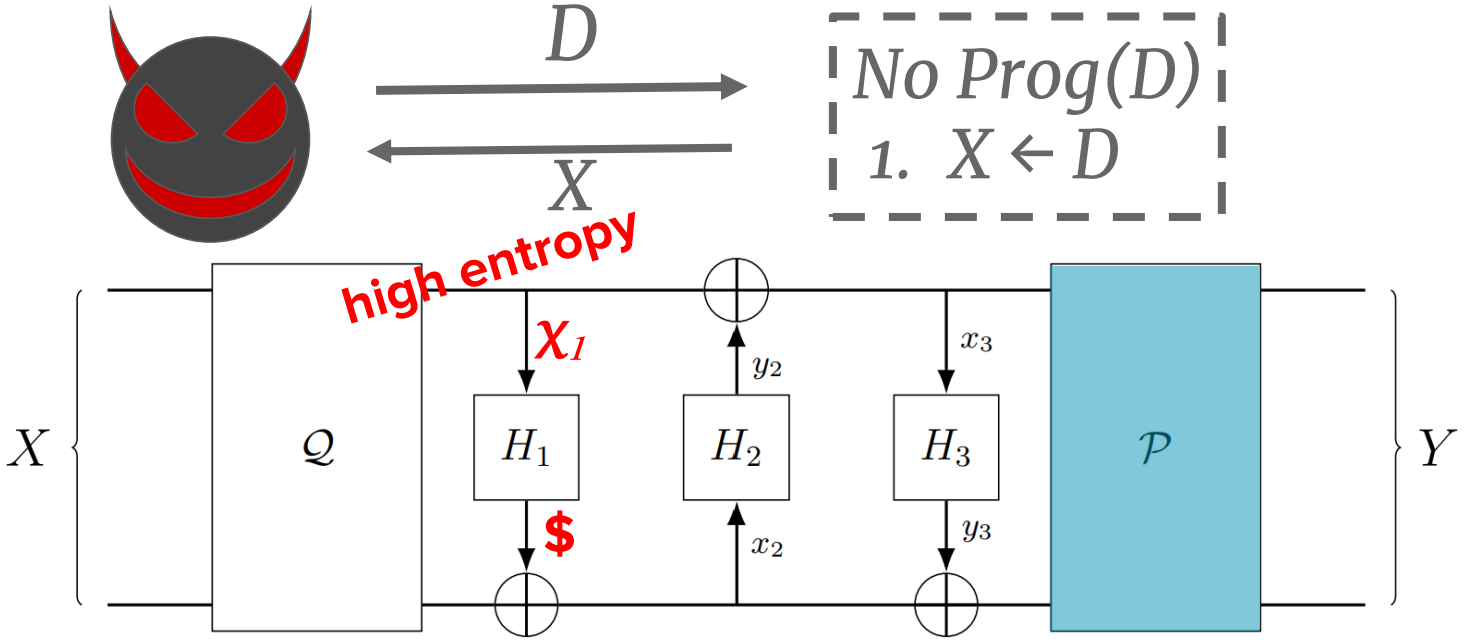




P is masking Q ⇒ X is indep. of Q

⇒ $H_\infty(\ x_1$:= left wire of $Q(X) \mid Q\ ) \approx H_\infty(X)$

Lifting Adaptive Reprogramming

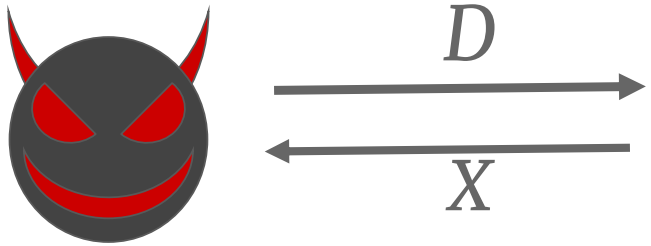


P is masking Q ⇒ X is indep. of Q

⇒ $H_\infty(\ x_1$:= left wire of $Q(X) \mid Q\ ) \approx H_\infty(X)$

⇒ apply [GHHM21] for "$H_1(x_1)$:= $"

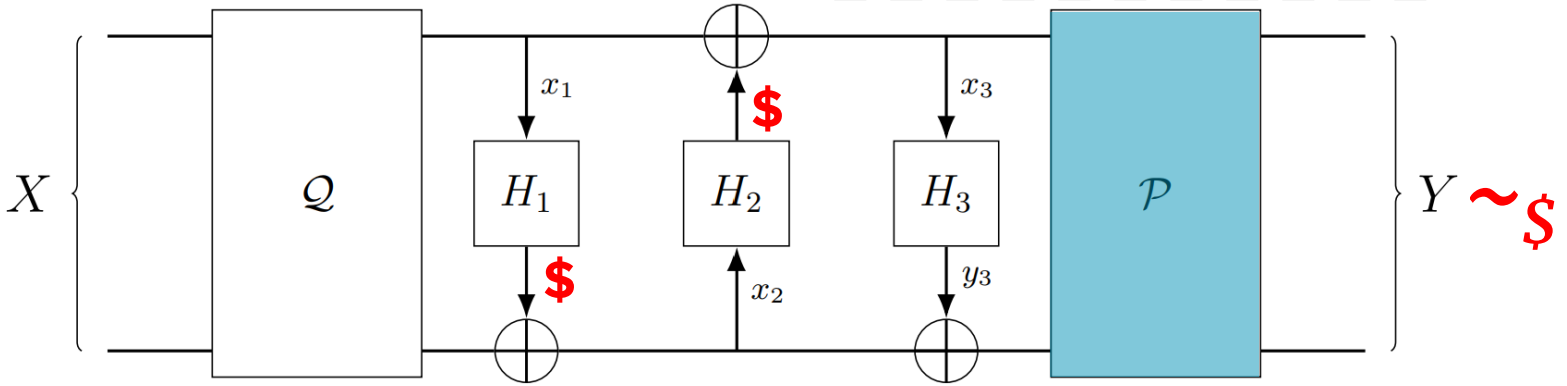
Lifting Adaptive Reprogramming



D

X

$Prog(D)$
1. $X \leftarrow D$
2. "$P3FQ(X) := \$$"

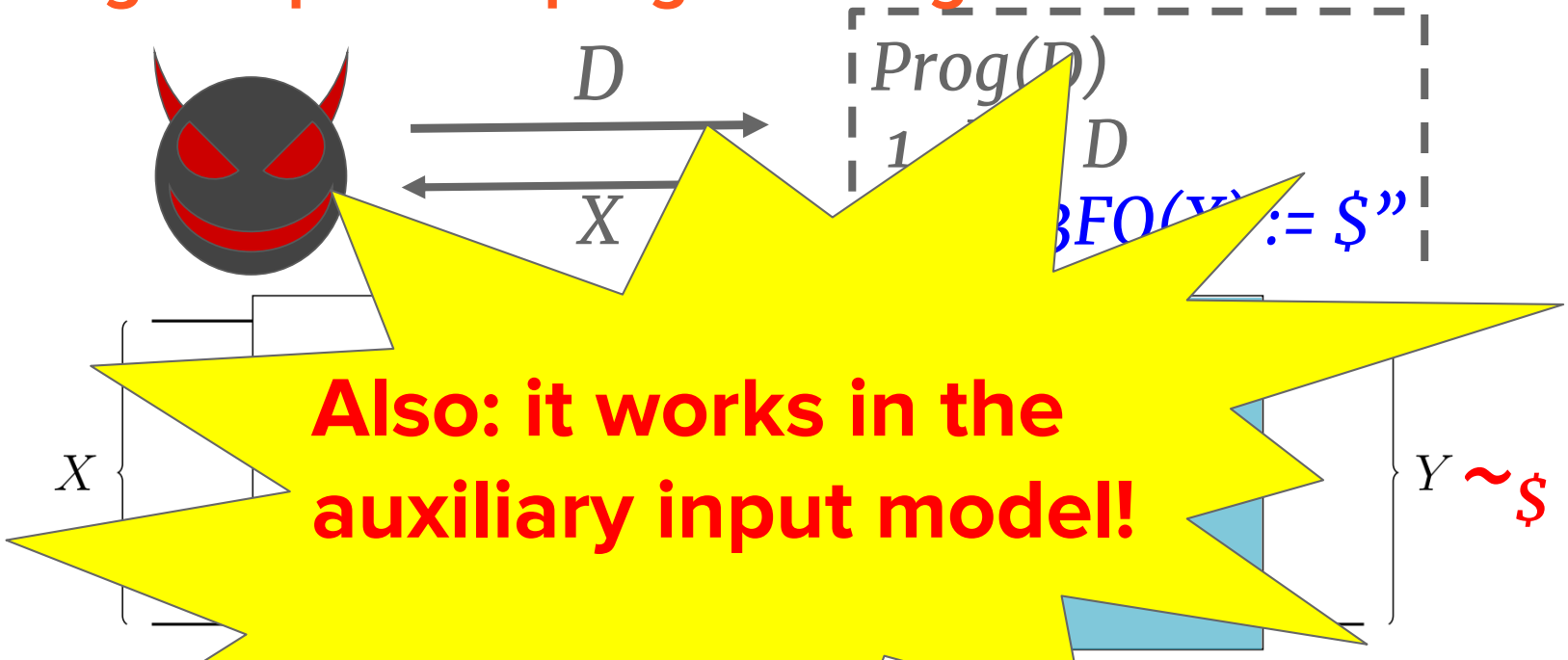


P is masking Q ⇒ X is indep. of Q

⇒ $H_\infty(\ x_1 :=$ left wire of $Q(X) \mid Q\ ) \approx H_\infty(X)$

⇒ apply [GHHM21] for "$H_1(x_1) := \$$" and for H_2

Lifting Adaptive Reprogramming



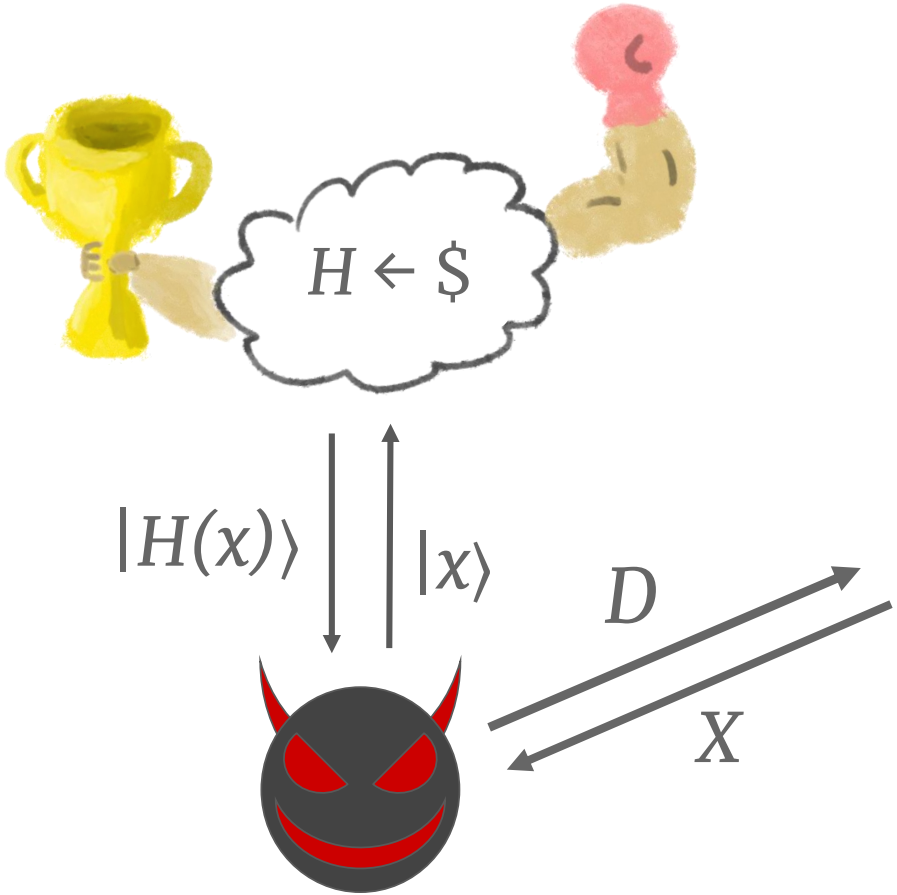
Also: it works in the auxiliary input model!

P is [illegible] of Q

$\Rightarrow H_\infty(\, x_1 :=$ le[illegible]ire of $Q(X) \mid Q\,) \approx H_\infty(X)$

$\Rightarrow$ apply [GHHM21] for “$H_1(x_1) := \$$” and for H_2

Reprogramming With Advice



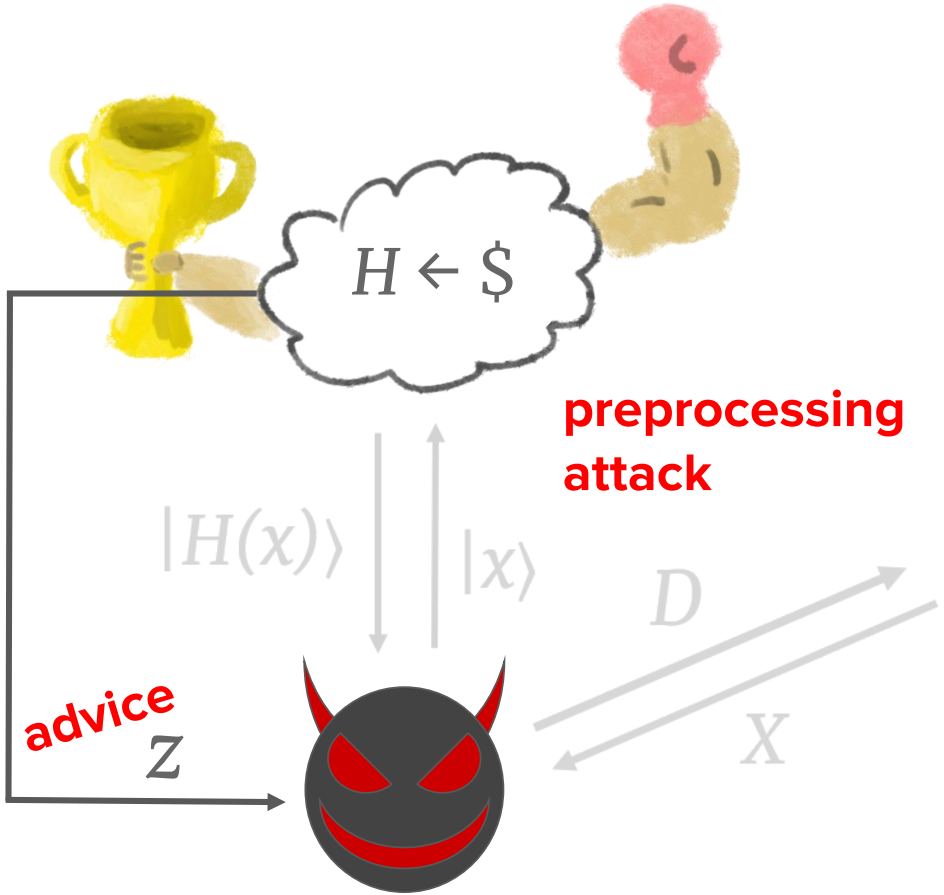
[GHHM21] theorem: Indistinguishable for D with high min-entropy.

$NoProg(D)$
1. $X \leftarrow D$

or ≈

$Prog(D)$
1. $X \leftarrow D$
2. $H(X) := \$$

Reprogramming With Advice



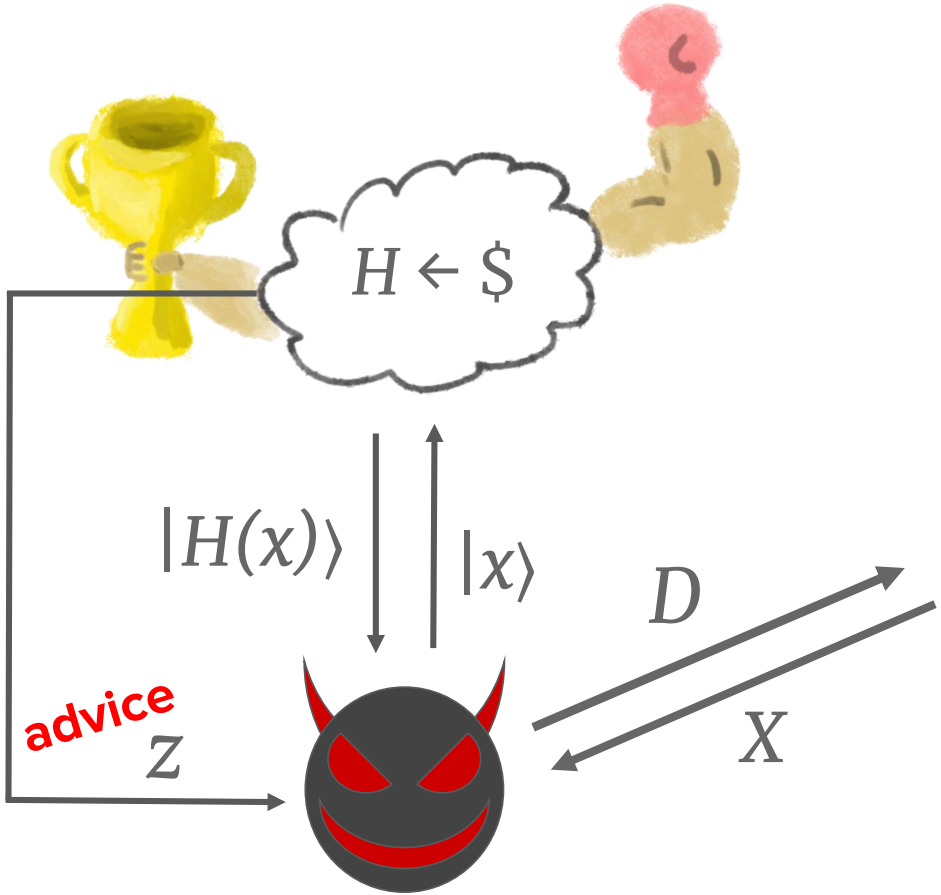
[GHHM21] theorem: Indistinguishable for D with high min-entropy. But with advice?

$No\ Prog(D)$
1. $X \leftarrow D$

or ≈?

$Prog(D)$
1. $X \leftarrow D$
2. $H(X) := \$$

Reprogramming With Advice



Our new theorem:
Indistinguishable for D with high min-entropy –
even with (finite) advice!

$No\ Prog(D)$
1. $X \leftarrow D$

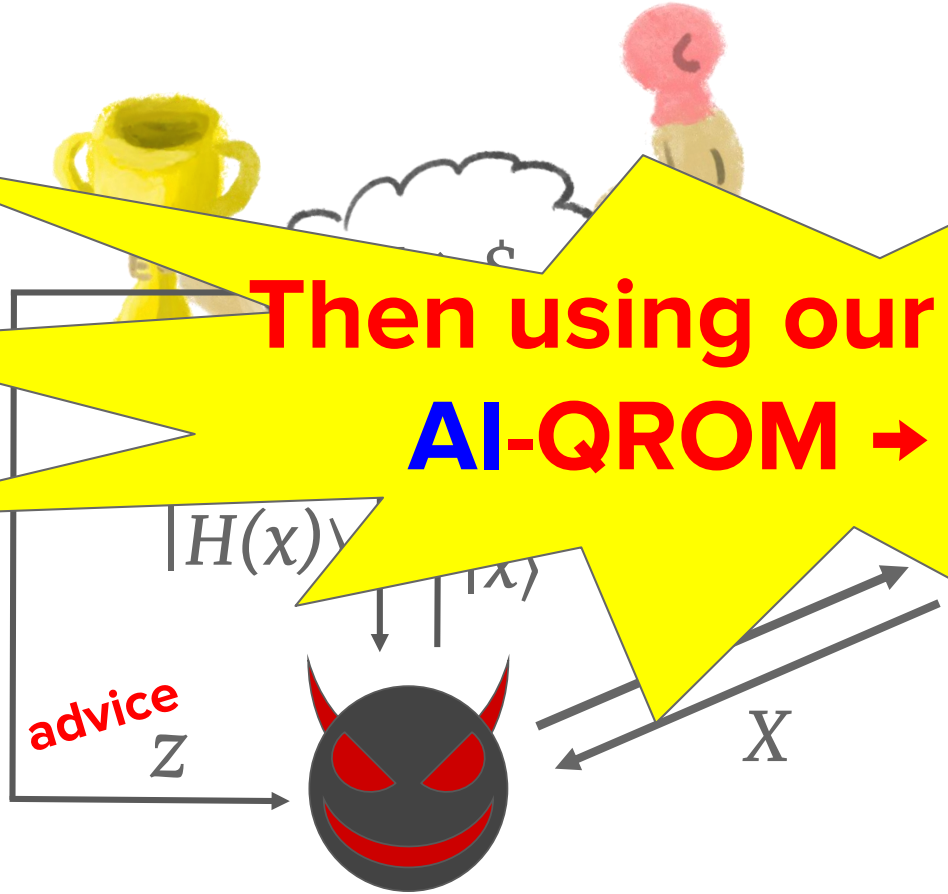
or ≈

$Prog(D)$
1. $X \leftarrow D$
2. $H(X) := \$$

Reprogramming With Advice

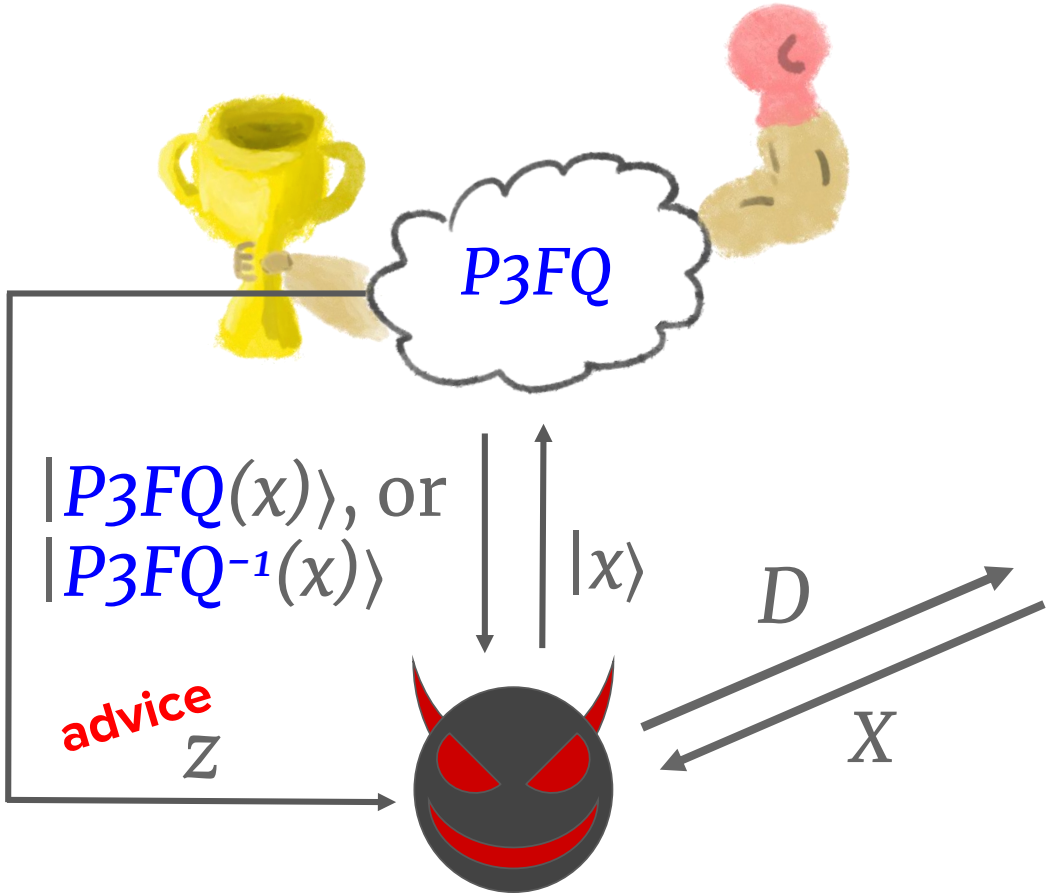
Our new theorem:
Indistinguishable for D with high min-entropy – [illegible] with (finite) advice!

Then using our P3FQ lifting,
AI-QROM → AI-QRPM!



$Prog(D)$
1. $X \leftarrow D$
2. $H(X) := \$$

Reprogramming With Advice



Our new theorem:
Indistinguishable for D with high min-entropy –
even with (finite) advice!

No Prog(D)
1. $X \leftarrow D$

or ≈ ✓

Prog(D)
1. $X \leftarrow D$
2. *"P3FQ(X) := $"*

Table of Contents

Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal

A Fiat–Shamir Transformation From Duplex Sponges

Alessandro Chiesa
alessandro.chiesa@epfl.ch
EPFL

Michele Orrù
m@orru.net
CNRS

July 9, 2025

Abstract

We analyze a variant of the Fiat–Shamir transformation based on an ideal permutation. The transformation relies on the popular duplex sponge paradigm, and minimizes the number of calls to the permutation (given the information to absorb/squeeze). This closely models deployed variants of the Fiat–Shamir transformation, and our analysis provides concrete security bounds to guide security parameters in practice. Our results contribute to the ongoing community-wide effort to achieve rigorous, and ultimately formally verified, security proofs for deployed cryptographic proofs. Along the way, we find that indifferentiability (a property proven for many modes of operation, including the duplex sponge) is ill-suited for establishing the knowledge soundness and zero knowledge of a non-interactive argument.

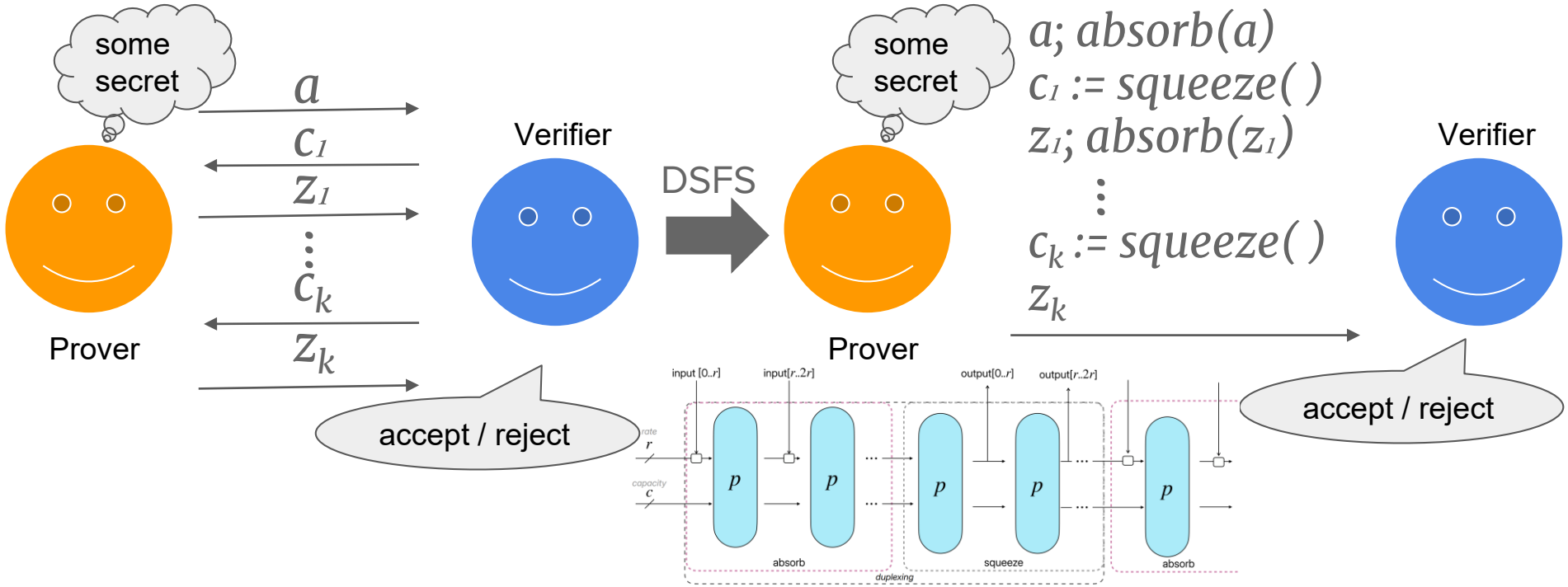
We additionally contribute `spongefish`, an open-source Rust library implementing our Fiat–Shamir transformation. The library is interoperable across multiple cryptographic frameworks, and works with any choice of permutation. The library comes equipped with Keccak and Poseidon permutations, as well as several "codecs" for re-mapping prover and verifier messages to the permutation's domain.

Keywords: Fiat–Shamir transformation; duplex sponge

Signal

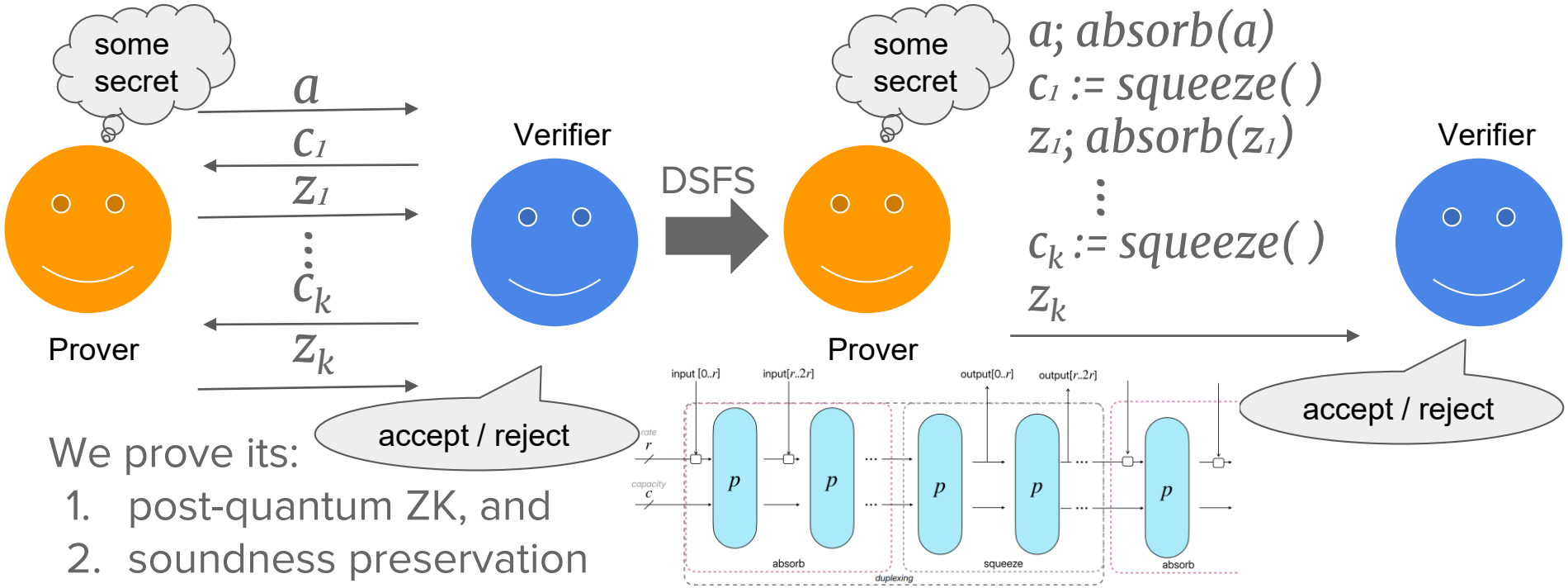
Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal



Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal



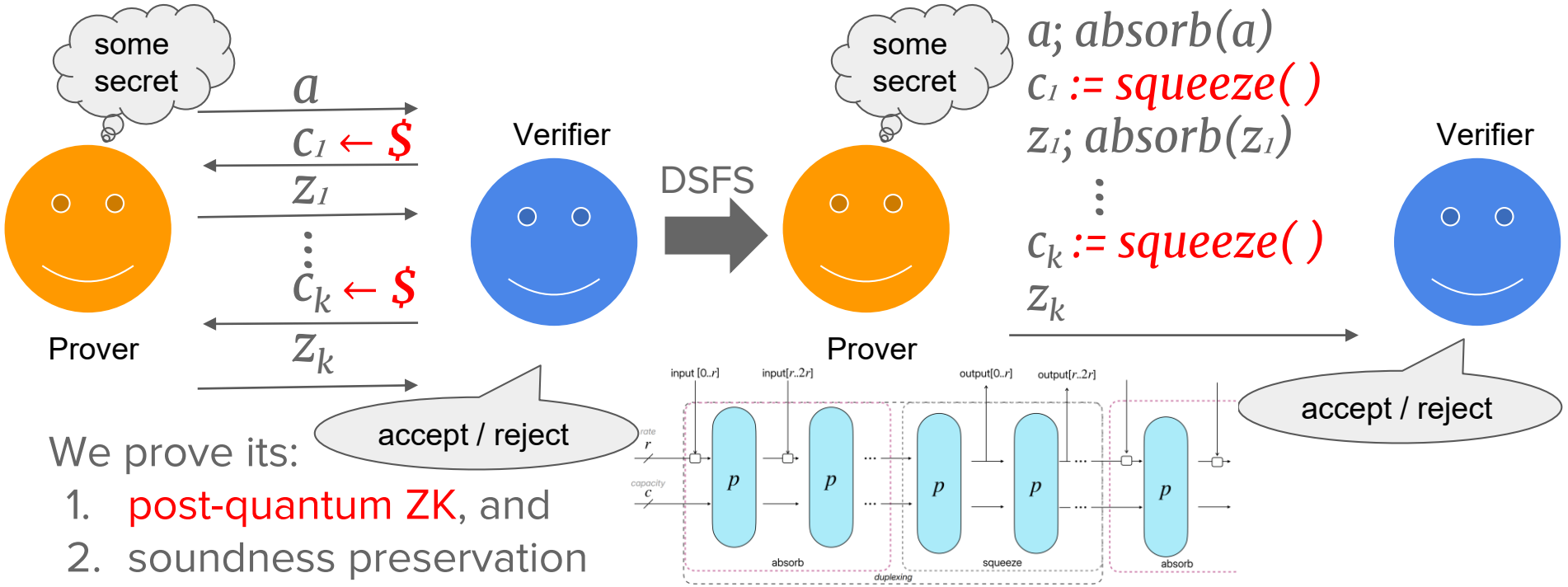
We prove its:

1. post-quantum ZK, and
2. soundness preservation

via lifting 2 different QROM reprogramming techniques to QRPM.

Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal



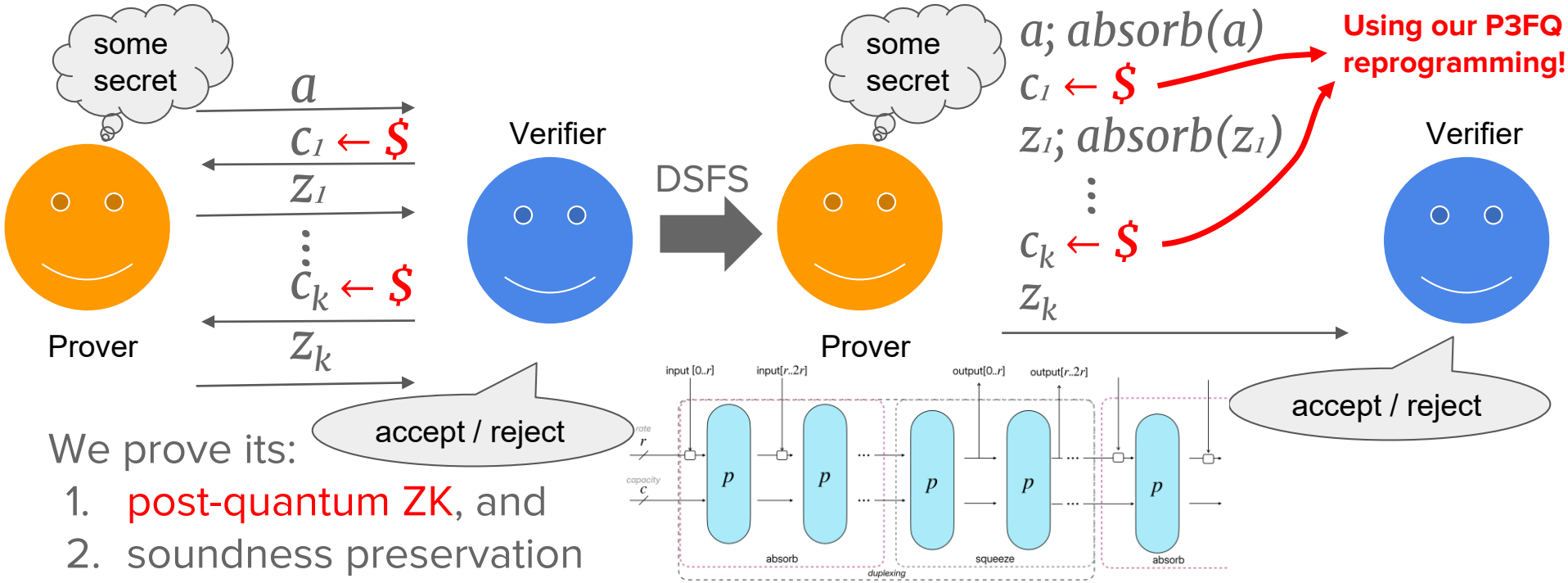
We prove its:

1. post-quantum ZK, and
2. soundness preservation

via lifting 2 different QROM reprogramming techniques to QRPM.

Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal



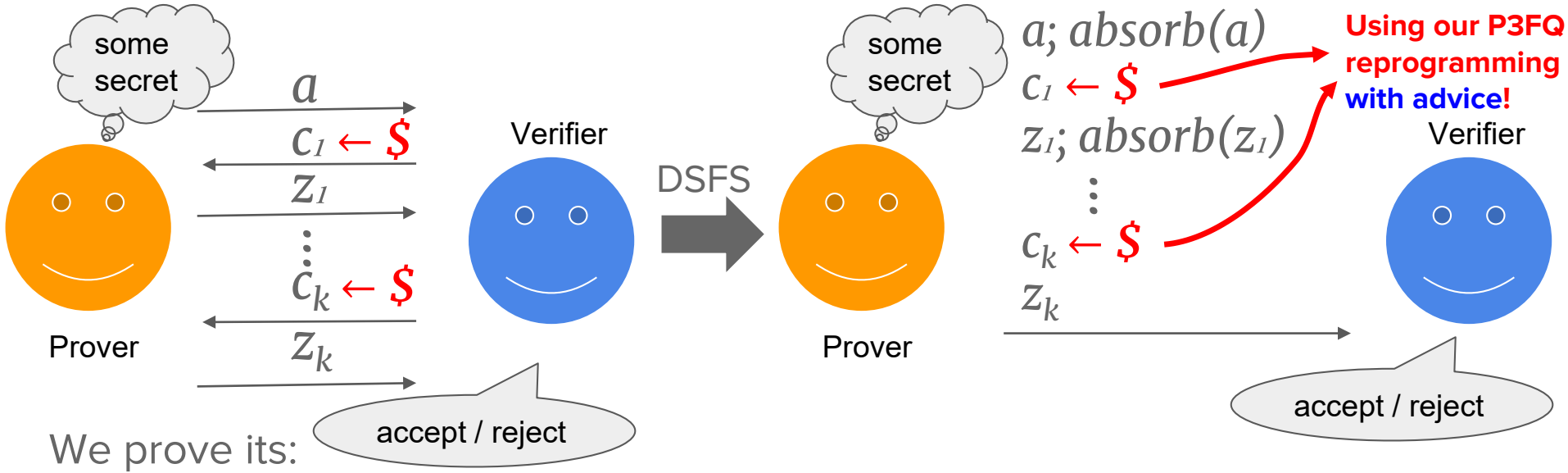
We prove its:

1. post-quantum ZK, and
2. soundness preservation

via lifting 2 different QROM reprogramming techniques to QRPM.

Applications: Duplex-Sponge Fiat-Shamir (DSFS)

a permutation-based variant of Fiat-Shamir, considered by Signal



We prove its:

1. post-quantum ZK (also w.r.t. preprocessing distinguishers), and
2. soundness preservation

via lifting 2 different QROM reprogramming techniques to QRPM.

More Applications (WIP)...

Post-Quantum Security of the Even-Mansour Cipher

Gorjan Alagic[1], Chen Bai[2], Jonathan Katz[3][0000−0001−6084−9303], and Christian Majenz[4][0000−0002−1877−8385]

[1] QuICS, University of Maryland, and NIST
[2] Dept. of Electrical and Computer Engineering, University of Maryland
[3] Dept. of Computer Science, University of Maryland
[4] Dept. of Applied Mathematics and Computer Science, Technical University of Denmark

Abstract. The Even-Mansour cipher is a simple method for constructing a (keyed) pseudorandom permutation E from a public random permutation $P : \{0,1\}^n \to \{0,1\}^n$. It is secure against classical attacks, with optimal attacks requiring q_E queries to E and q_P queries to P such that $q_E \cdot q_P \approx 2^n$. If the attacker is given *quantum* access to both E and P, however, the cipher is completely insecure, with attacks using
$q_E, q_P = O(n)$ queries known.

More Applications (WIP)...

Post-Quantum Security of the Even-Mansour Ci

Gorjan Alagic[1], Chen Bai[2], Jo
Maje

[1] QuICS, Un
[2] Dept. of Electrical and C
[3] Dept. of Comput
[4] Dept. of Applied Mathematics

Abstract. The Even-Mansou
ing a (keyed) pseudorandom p
mutation $P : \{0,1\}^n \to \{0,1\}$
with optimal attacks requiring
that $q_E \cdot q_P \approx 2^n$. If the attac
and P, however, the cipher is
queries known

Tight Quantum Time-Space Tradeoffs for Permutation Inversion

Akshima[1], Tyler Besselman[1], Kai-Min Chung[2], Siyao Guo[1], and Tzu-Yi Yang[2]

[1]NYU Shanghai
[1]{akshima, tyler.william.b, siyao.guo}@nyu.edu
[2]Academia Sinica
[2]{kmchung, dhss6645}@as.edu.tw

October 15, 2025

Abstract

In permutation inversion, we are given a permutation $\pi : [N] \to [N]$, and want to prepare some advice of size S, such that we can efficiently invert any image in time T. This is a fundamental cryptographic problem with profound connections to communication complexity and circuit lower bounds.
classical setting, a tight $ST = \tilde{\Theta}(N)$ bound has been established since the seminal

Thank you for listening.

ia.cr/2026/146

References

[CHLYY25] A. Cojocaru, M. Hhan, Q. Liu, T. Yamakawa, A. Yun. *Quantum Lifting for Invertible Permutations and Ideal Ciphers.* In CRYPTO 2025

[Carolan25] J. Carolan. Compressed Permutation Oracles. In STOC 2026

[MMW24] C. Majenz, G. Malavolta, M. Walter. *Permutation Superposition Oracles for Quantum Query Lower Bounds*. In STOC 2025

[ABKM21] G. Alagic, C. Bai, J. Katz, and C. Majenz. *Post-Quantum Security of the Even-Mansour Cipher.* In EUROCRYPT 2022