Quantum Security for the Fiat-Shamir Transform

Based on

J. Don, S. Fehr, C. Majenz, C. Schaffner, "Security of the Fiat-Shamir Transformation in the Quantum Random Oracle Model." CRYPTO 2019, pp 356-383, and the "Picnic" submission.

February 11, 2020, NIST Postquantum Crypto Seminar

Carl A. Miller

(Not for public distribution.)

The Basics

- The Fiat-Shamir transform can be used to turn interactive proofs-of-knowledge into digital signature schemes.

- This paper shows that Fiat-Shamir is secure in the quantum random oracle model (QROM).

- They offer some tentative applications to NIST PQC candidates.

Fiat-Shamir in the Classical Context

The Random Oracle Model

A hash function is an (efficiently computable) function

$$h: \{0,1\}^n \to \{0,1\}^m$$

which behaves a lot like a random function.

In a security proof "in the random oracle model," each use of the hash function is replaced by a black box,

which chooses a random output for each new input.

Σ-Protocols

Three rounds:

1. Commit.
2. Challenge.
3. Verify.

Bob then checks that a predicate P (x, e, w) holds.

$\xrightarrow{x}$

e (uniformly random) $\longleftarrow$

$\xrightarrow[w]{}$

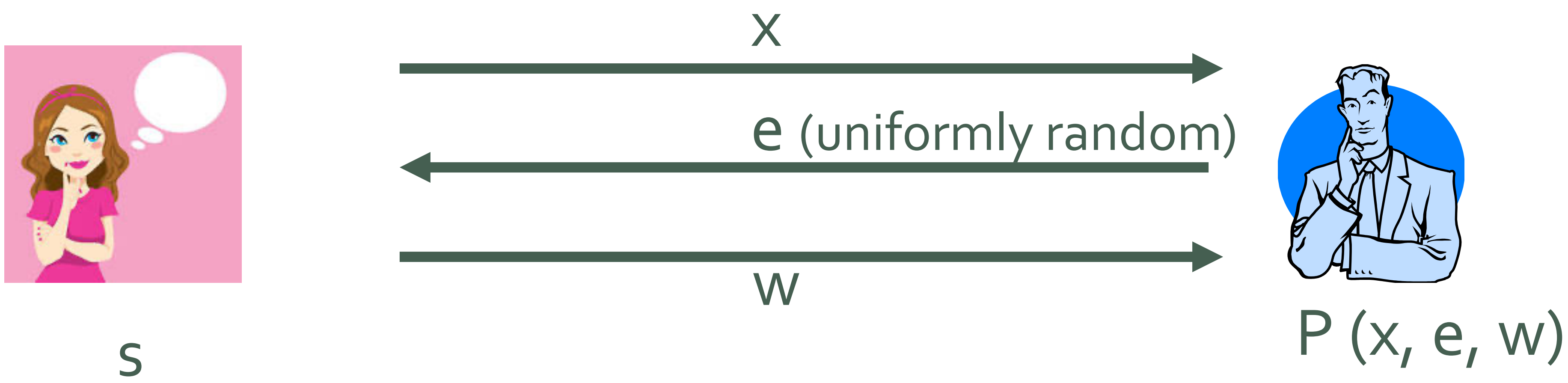
P (x, e, w)

Σ-Protocols

These are useful when there is a bit string s such that:

- Alice can efficiently satisfy P if she knows s;
- With no information, Alice can't efficiently satisfy P.

(Proof of knowledge.)



Fiat-Shamir Transform

Alice uses a hash function H to compute e.

s

$\xrightarrow{x}$

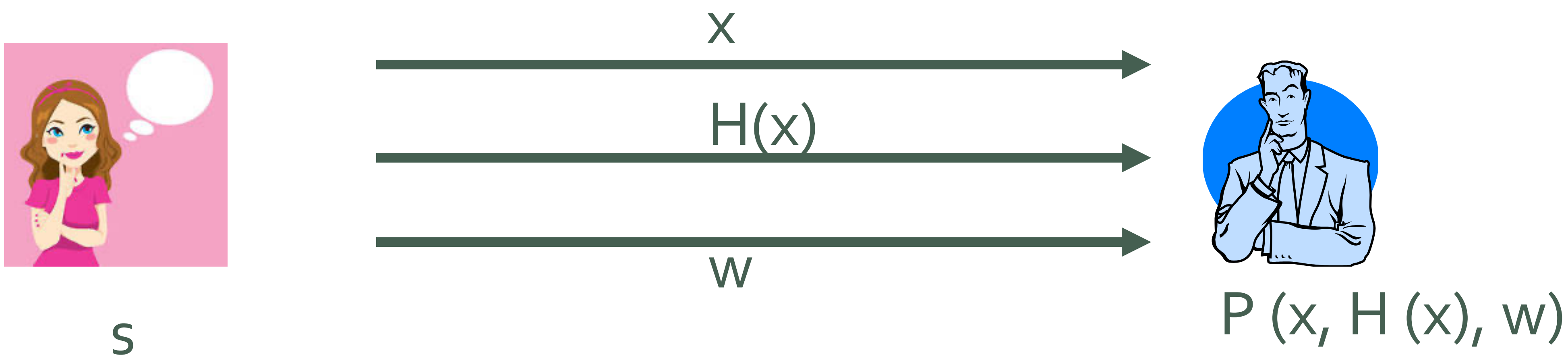
$\xrightarrow{e}$

$\xrightarrow[w]{}$

Fiat-Shamir Transform

Alice uses a hash function H to compute e.
Bob simply checks P on the hash.

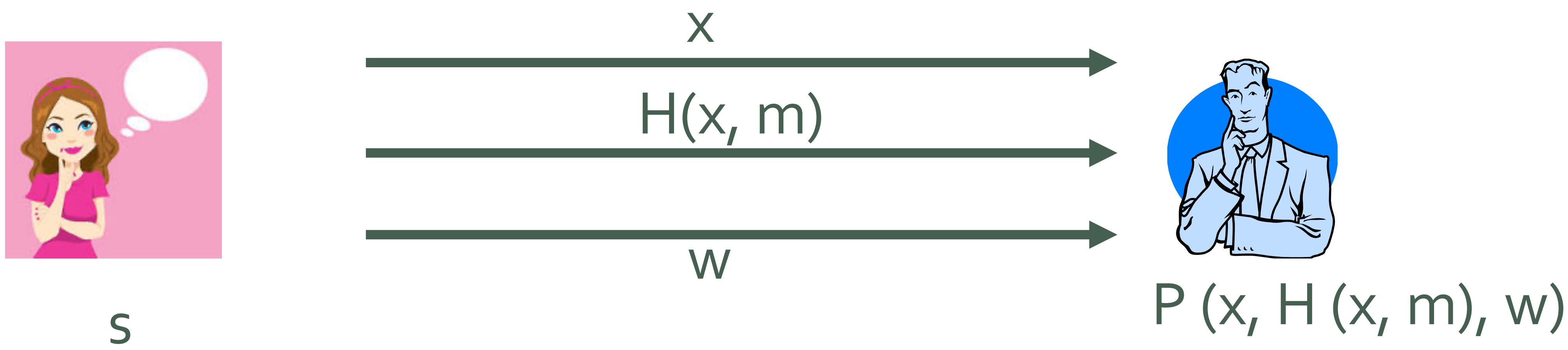
(To make this a signature scheme, hash the message m as well.)



Fiat-Shamir Transform

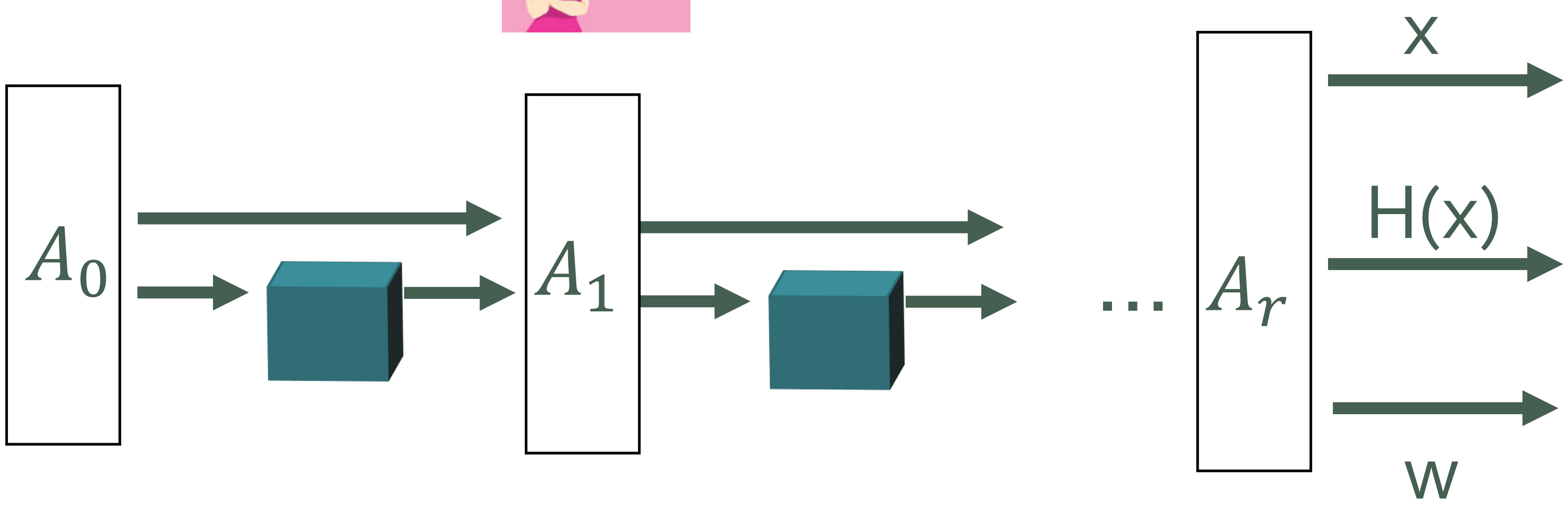
Alice uses a hash function H to compute e.
Bob simply checks P on the hash.

(To make this a signature scheme, hash the message m as well.)



Fiat-Shamir is Secure in the ROM

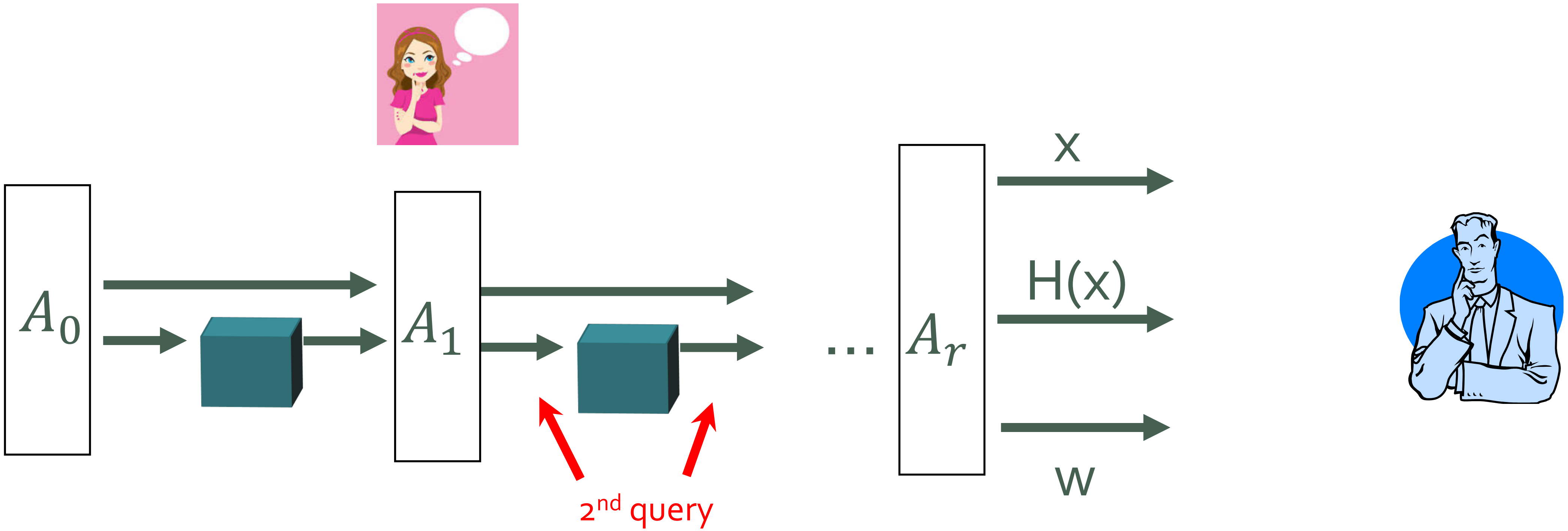
Suppose that Z is a Σ-protocol, and Alice has an algorithm that works for Fiat (Z) with non-negligible prob.
She wants an algorithm that works for Z.



Fiat-Shamir is Secure in the ROM

For i = 1, …, r, let p_i be the probability that the protocol succeeds **and** that the final pair (x, H(x)) was generated on the ith query.

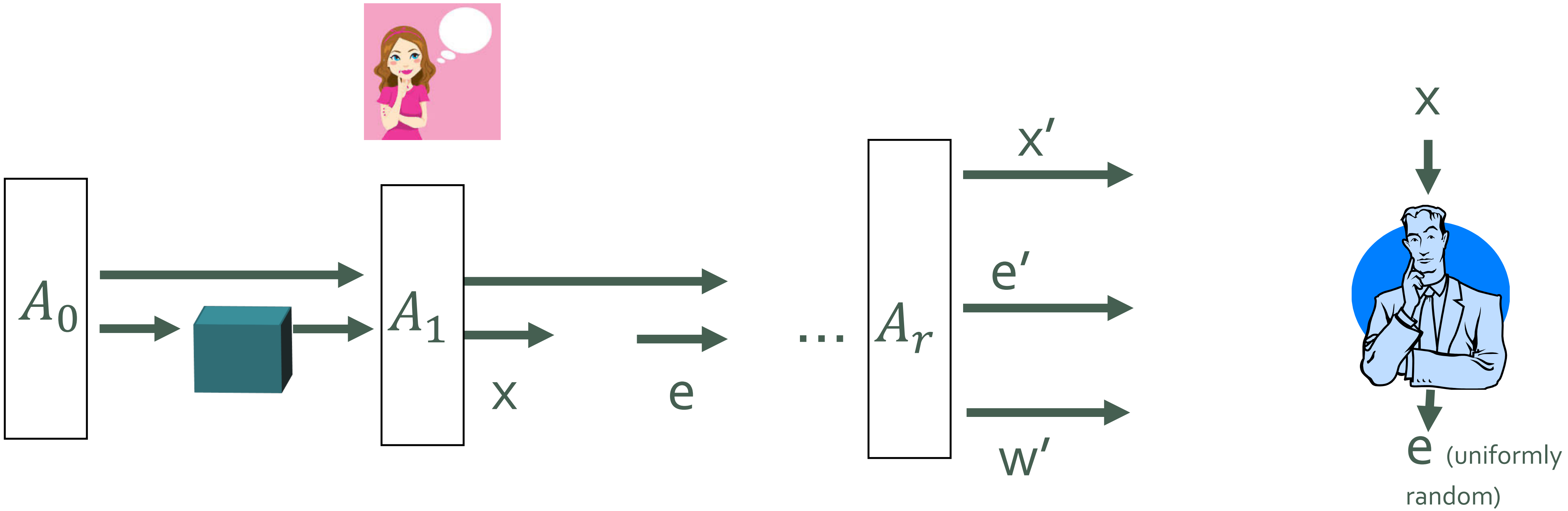
Let p = overall probability of success.



Fiat-Shamir is Secure in the ROM

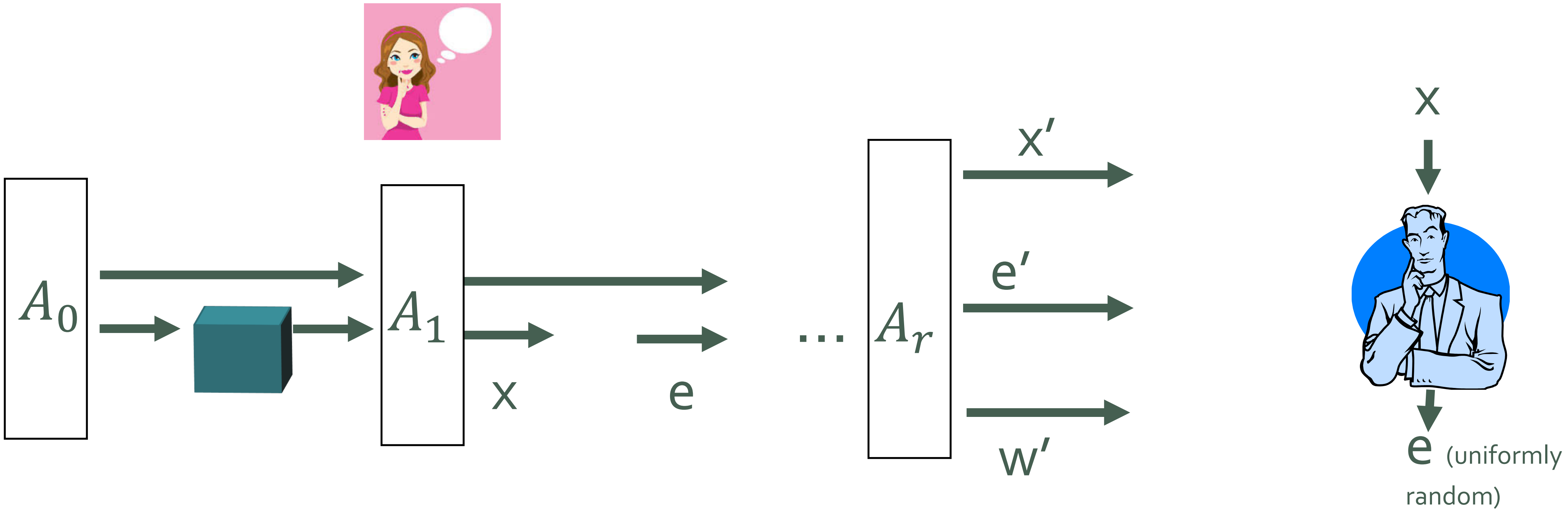
Alice chooses a random round i. On the ith round (only) she uses Bob in place of the random oracle.

She then finishes as usual.



Fiat-Shamir is Secure in the ROM

W/ prob. p_i, the output will include x and e as desired.

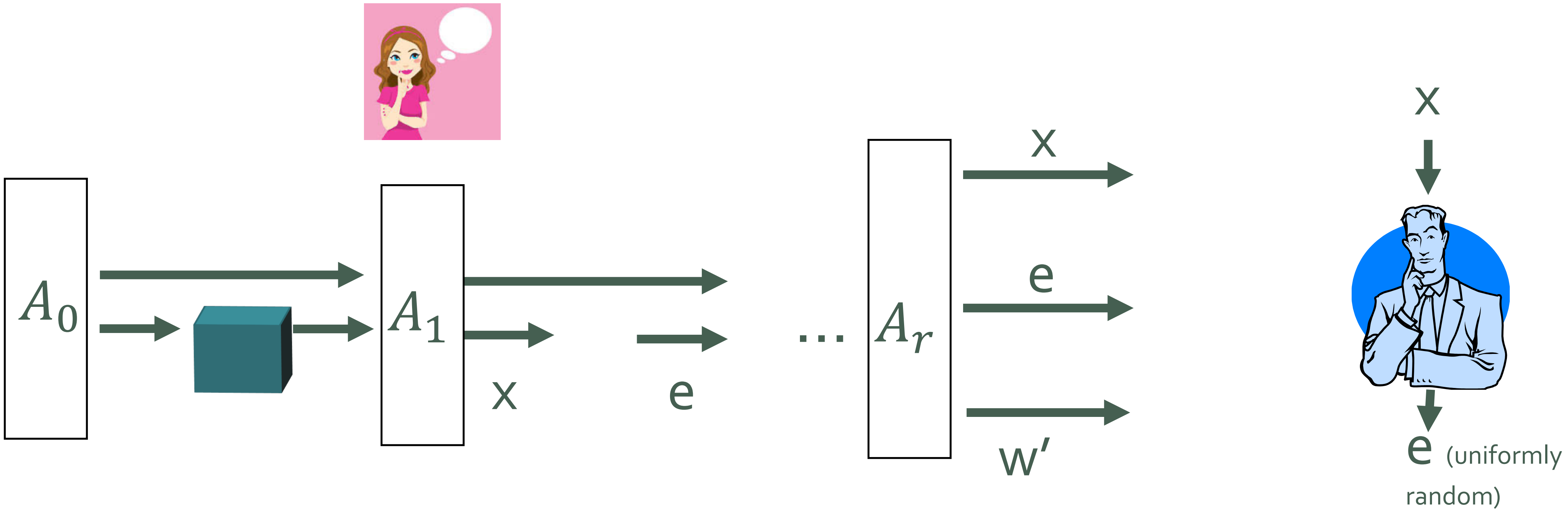


Fiat-Shamir is Secure in the ROM

W/ prob. p_i, the output will include x and e as desired.

So, the overall probability of success is

$$\frac{p_1+p_2+\cdots+p_r}{r} \approx \frac{p}{r}. \qquad \text{(non-negl.)}$$



The Quantum Random Oracle Model

The QROM

A quantum random oracle is initiated by choosing a random function

$$f: \{0,1\}^n \rightarrow \{0,1\}^m$$

The oracle accepts bit strings in superposition and returns outputs in superposition.

$$\frac{|a_1 > +|a_2 > +|a_3 >}{\sqrt{3}} \longrightarrow$$

$$\longrightarrow \frac{|a_1, f(a_1) > +|a_2, f(a_2) > +|a_3, f(a_3) >}{\sqrt{3}}$$

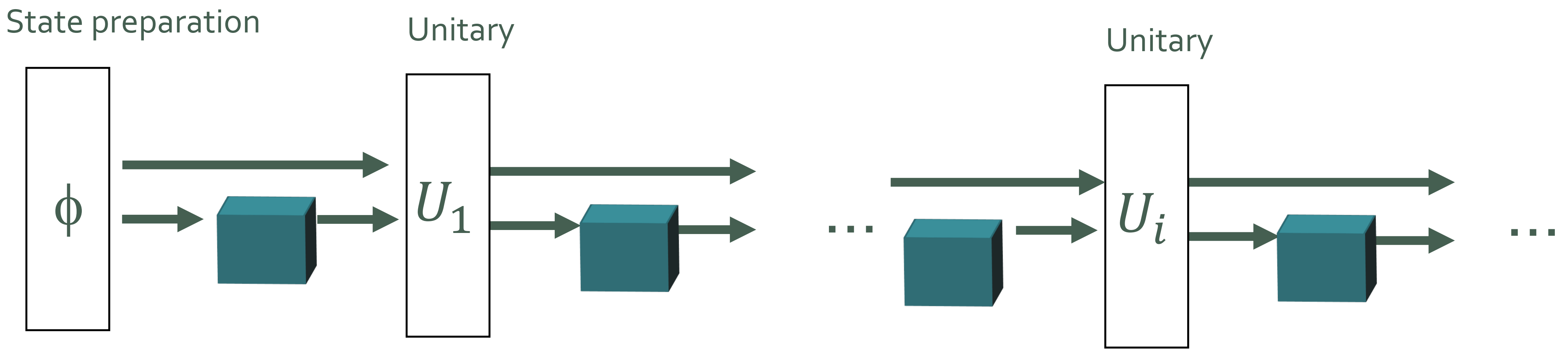
The QROM

Trying to adapt the previous Fiat-Shamir argument here raises multiple issues. (One is that measuring the input to a QROM disturbs it.)

We could use the **Unruh transform.**
That’s known to work, although it’s more complicated.

Fiat-Shamir is Secure in the QROM

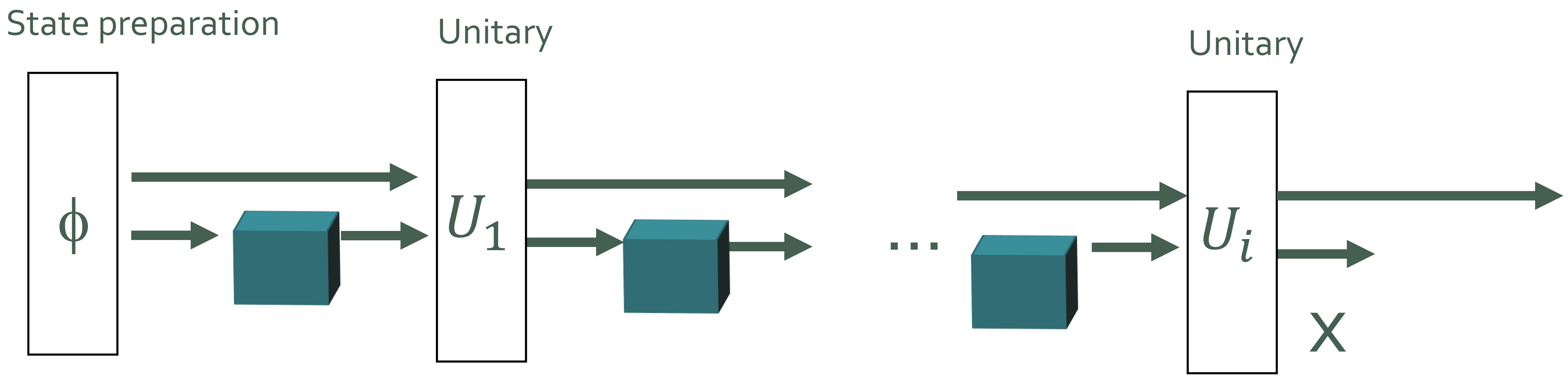
Suppose that Z is a Σ-protocol, and Alice has a **quantum algorithm** that works for Fiat (Z) with non-negligible prob.
She wants an algorithm that works for Z.



Fiat-Shamir is Secure in the QROM

Alice runs the protocol until a randomly chosen round i.

She measures x, sends it to Bob, receives e.

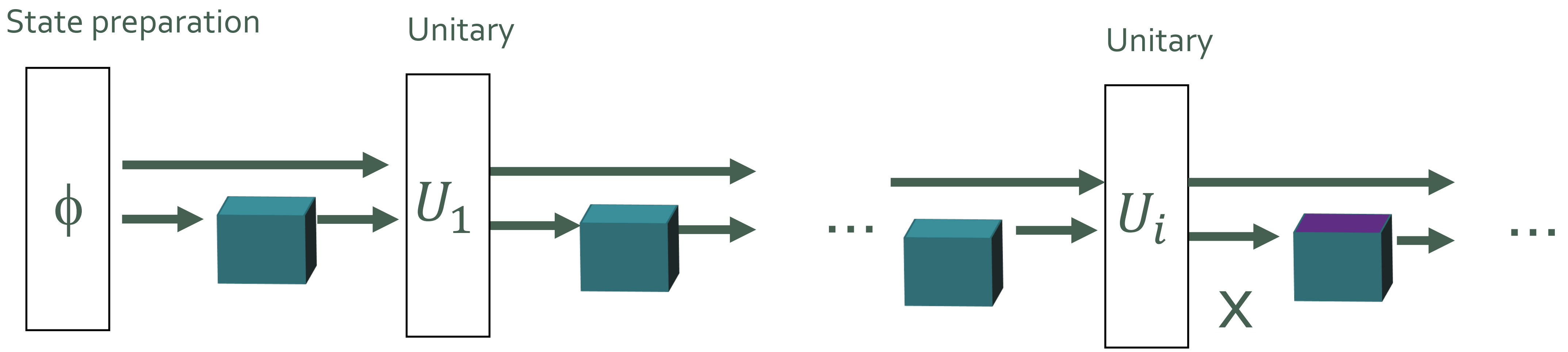


Fiat-Shamir is Secure in the QROM

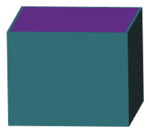
She prepares an altered quantum oracle, forcing $x \to e$. 

She replaces the **<u>(i+2) thru rth</u>** uses of the oracle with the new one.

With probability ½, she replaces the **<u>(i+1)th</u>** use with the new one.

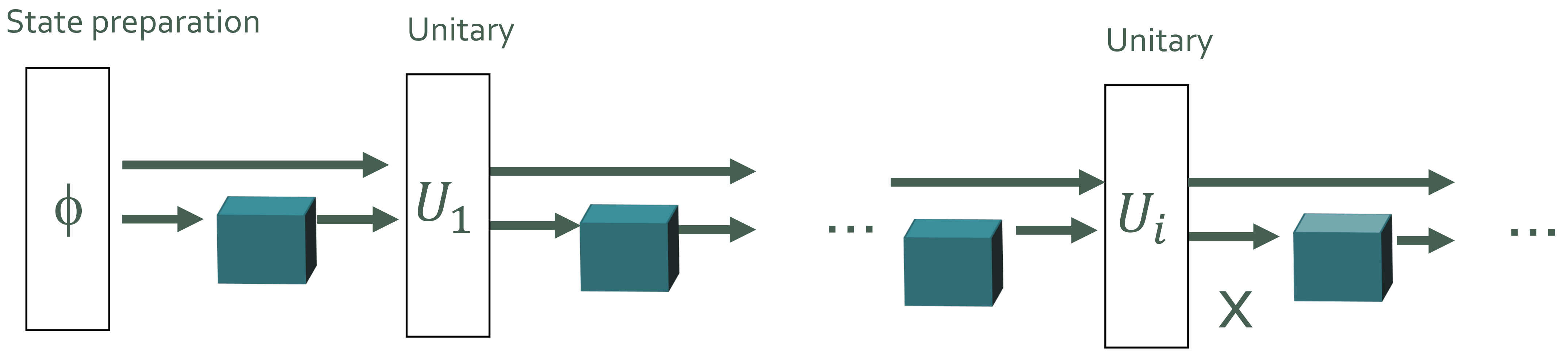


Fiat-Shamir is Secure in the QROM

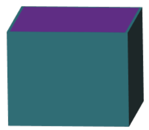
She prepares an altered quantum oracle, forcing $x \to e$. 

She replaces the **(i+2) thru rth** uses of the oracle with the new one.

With probability ½, she replaces the **(i+1)th** use with the new one.

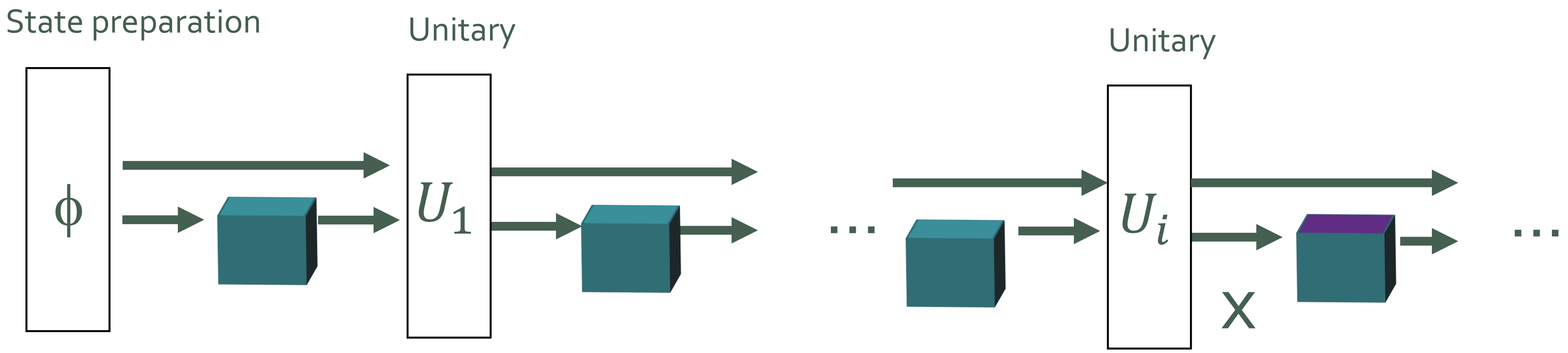


Fiat-Shamir is Secure in the QROM

She prepares an altered quantum oracle, forcing $x \to e$. 

She replaces the **(i+2) thru rth** uses of the oracle with the new one.

With probability ½, she replaces the **(i+1)th** use with the new one.

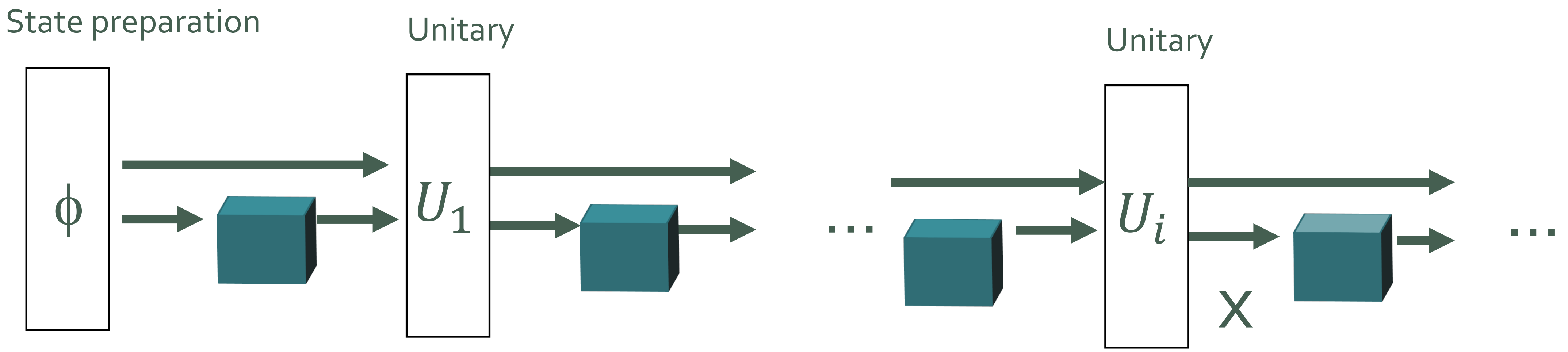


Fiat-Shamir is Secure in the QROM

Thm. With probability $\frac{p}{O(r^2)}$, the output will be of the form

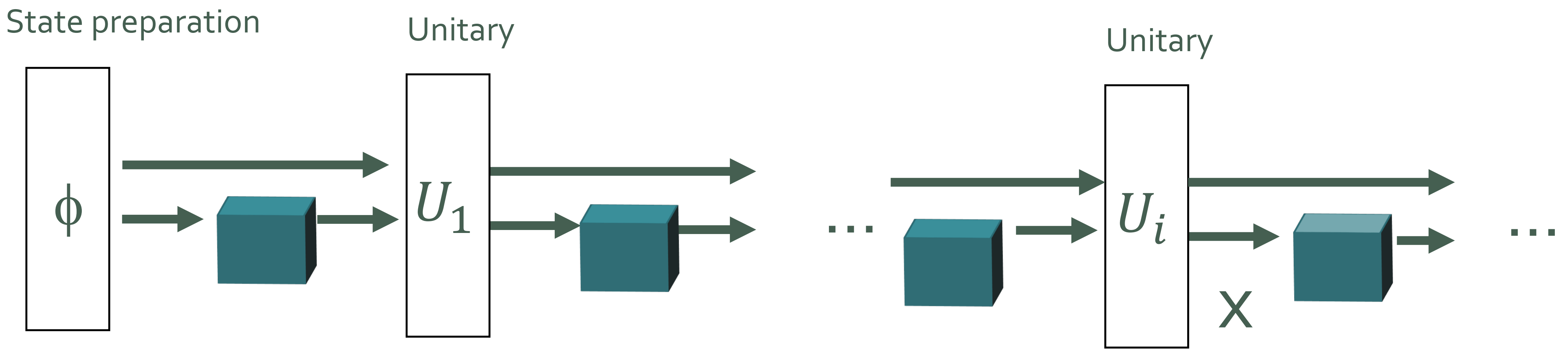
(x, e, w),

and the predicate P (x, e, w) will be satisfied.



Fiat-Shamir is Secure in the QROM

Conclusion: If Alice can win Fiat (Z) with non-negligible probability, then she can win Z with non-negligible probability.



Applications to PQC Candidates?

Picnic

In Picnic, the designers take two Σ-protocols (ZKB++ and KKW) and apply Fiat-Shamir and Unruh transforms to construct signatures schemes.

J. Don et al. explain a proof, via their main result, of a scheme similar to Picnic.

They also briefly address lattice-based schemes.

The Picnic Signature Scheme

Design Document

Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, Greg Zaverucha

March 30, 2019

Version 2.0