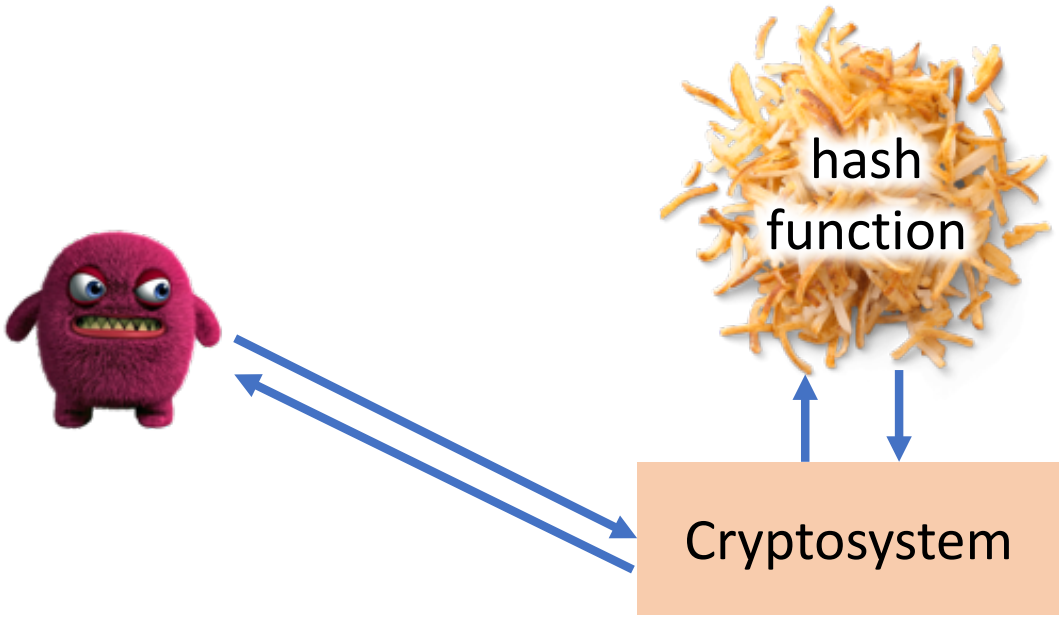
Quantum Random Oracle Model, Part 1

Mark Zhandry (Princeton & NTT Research)

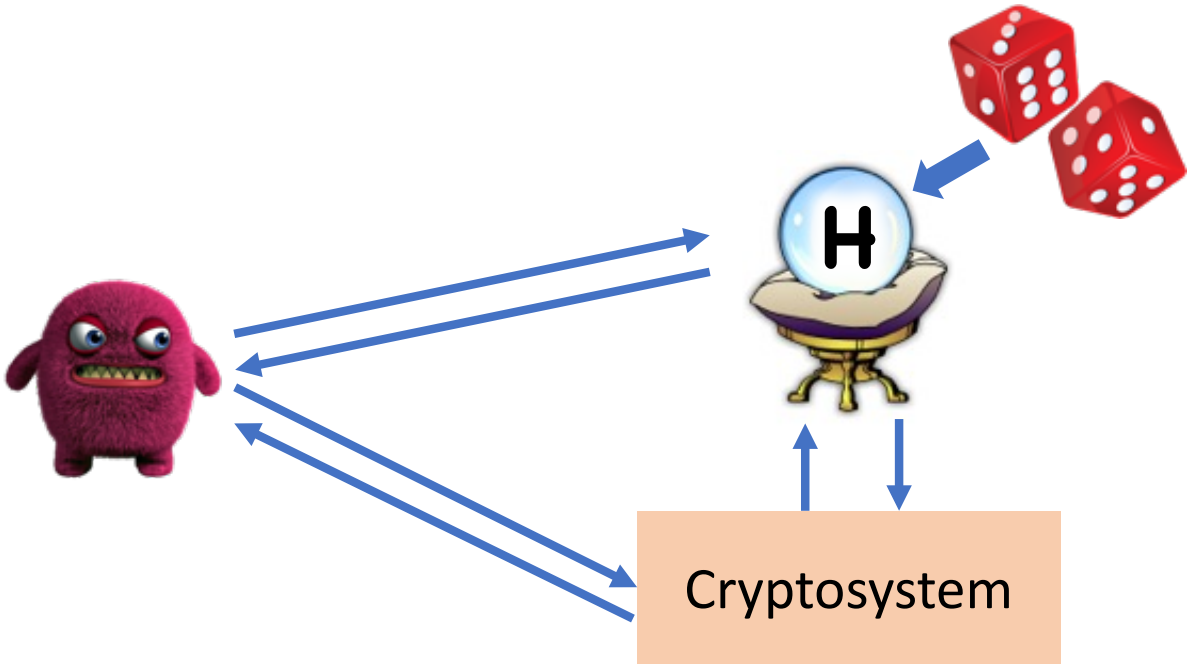
(Classical) Random Oracle Model (ROM)
[Bellare-Rogaway'93]



Examples: OAEP, Fujisaki-Okamoto, Full-Domain Hash, …

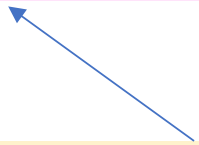
(Classical) Random Oracle Model (ROM)

[Bellare-Rogaway'93]



(Classical) Random Oracle Model (ROM)
[Bellare-Rogaway'93]

Idea: If $\exists$ ROM security proof, any attack must exploit structure of hash function

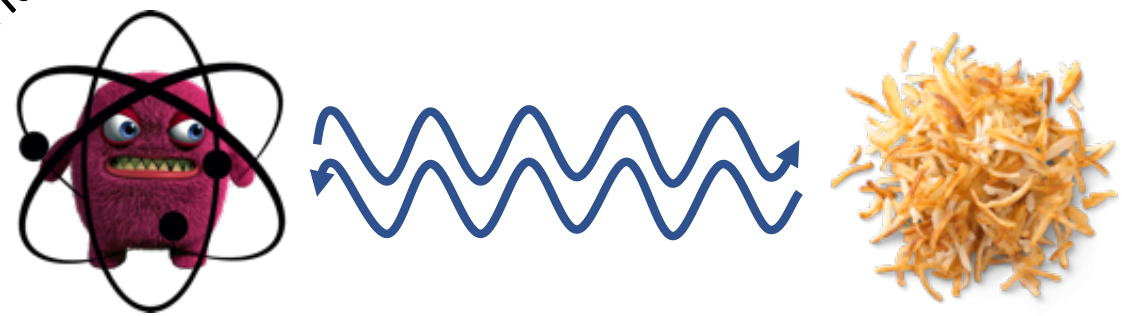


Hopefully not possible for well-designed hash

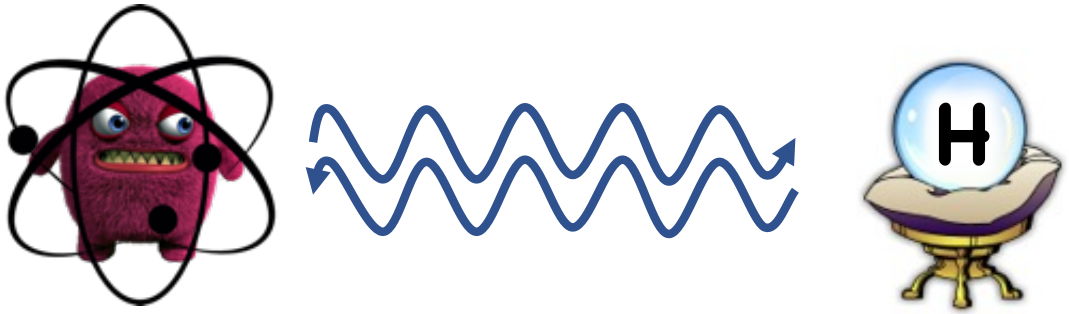
The Quantum Random Oracle Model (QROM)

[Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]

Real World



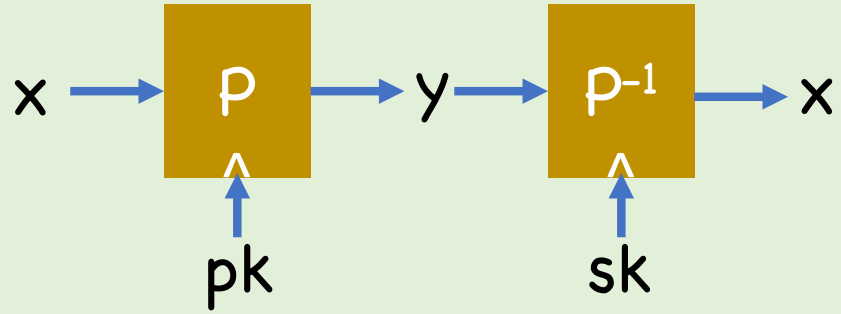
ROM



Now standard in post-quantum crypto

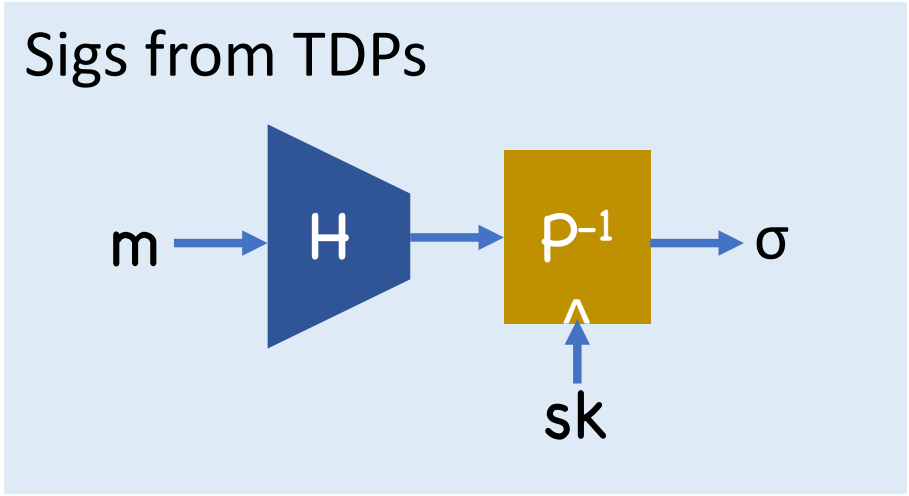
Example: Full Domain Hash

Building Block: Trapdoor Permutations



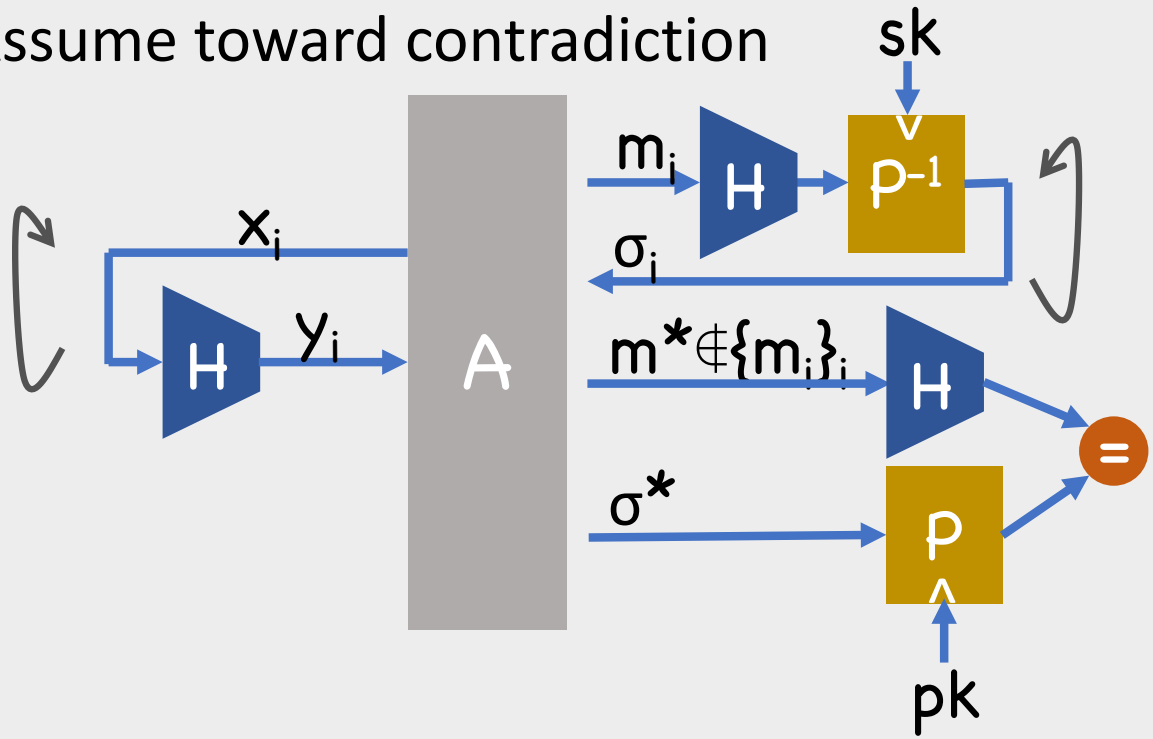
Security: $\forall$ PPT A, Pr[A(pk,y)=x] < negl

Example: Full Domain Hash



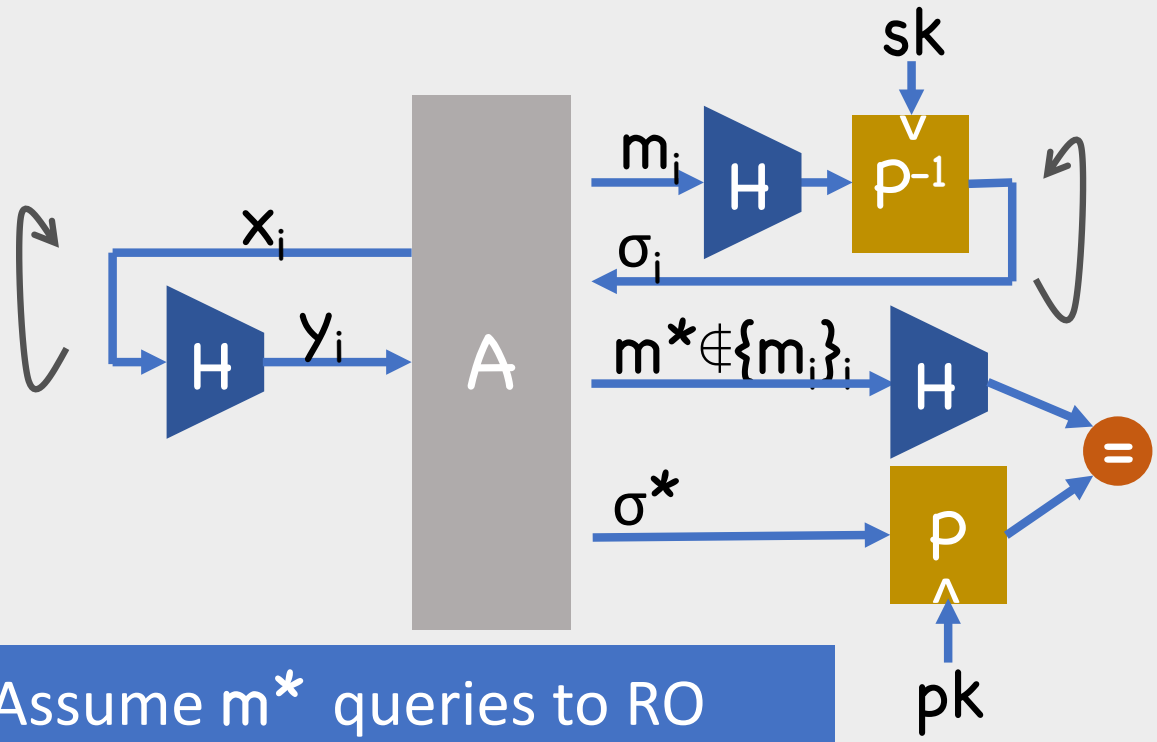
Example: Full Domain Hash

Proof: Assume toward contradiction



Example: Full Domain Hash

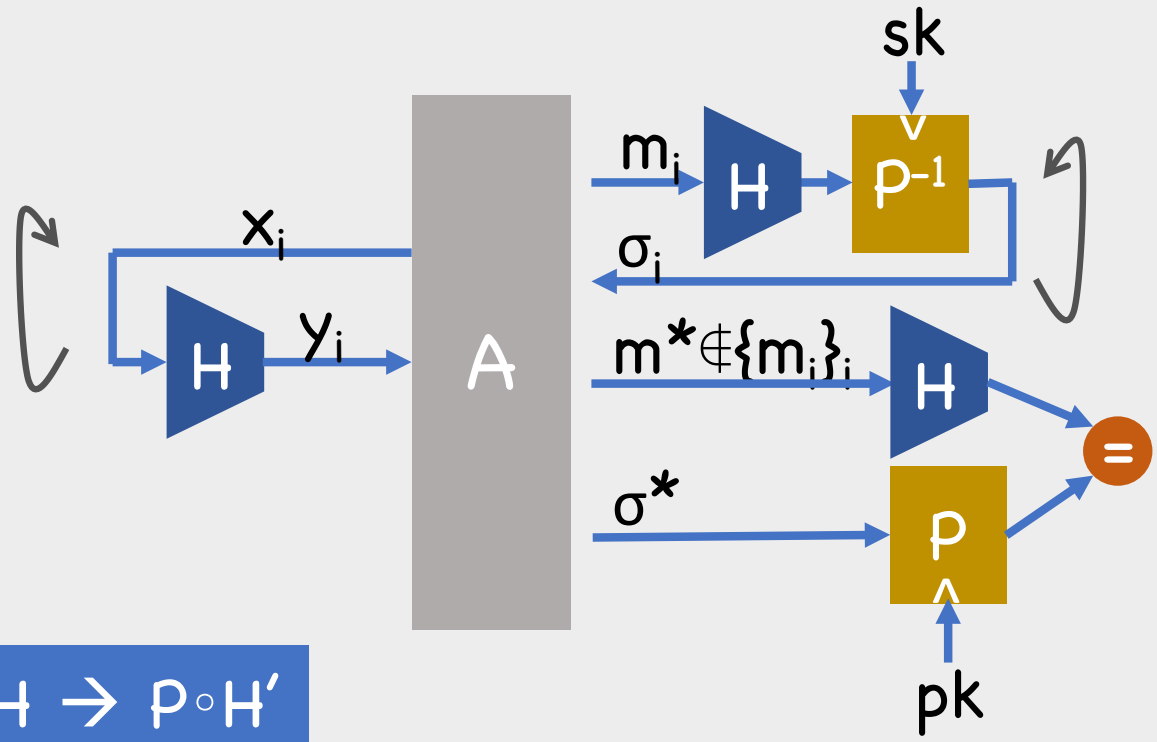
Proof:



Step 0: Assume m^* queries to RO

Example: Full Domain Hash

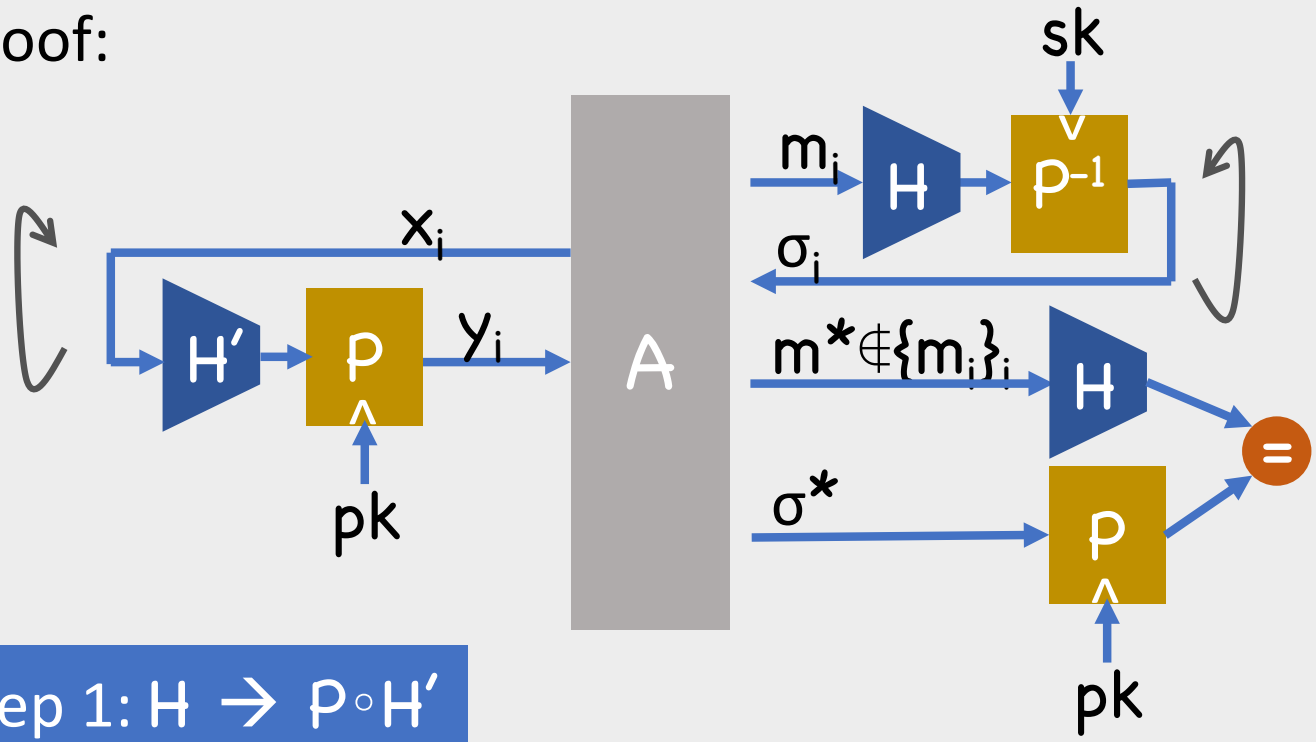
Proof:



Step 1: H → P∘H'

Example: Full Domain Hash

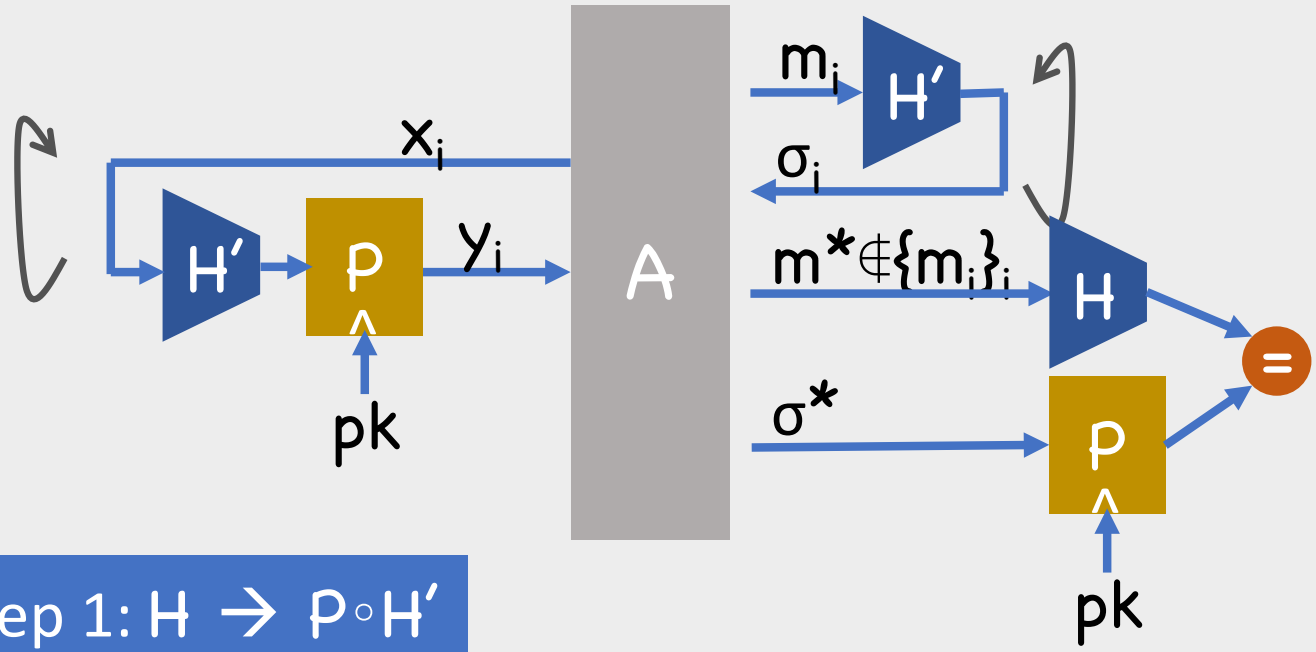
Proof:



Step 1: H → P∘H'

Example: Full Domain Hash

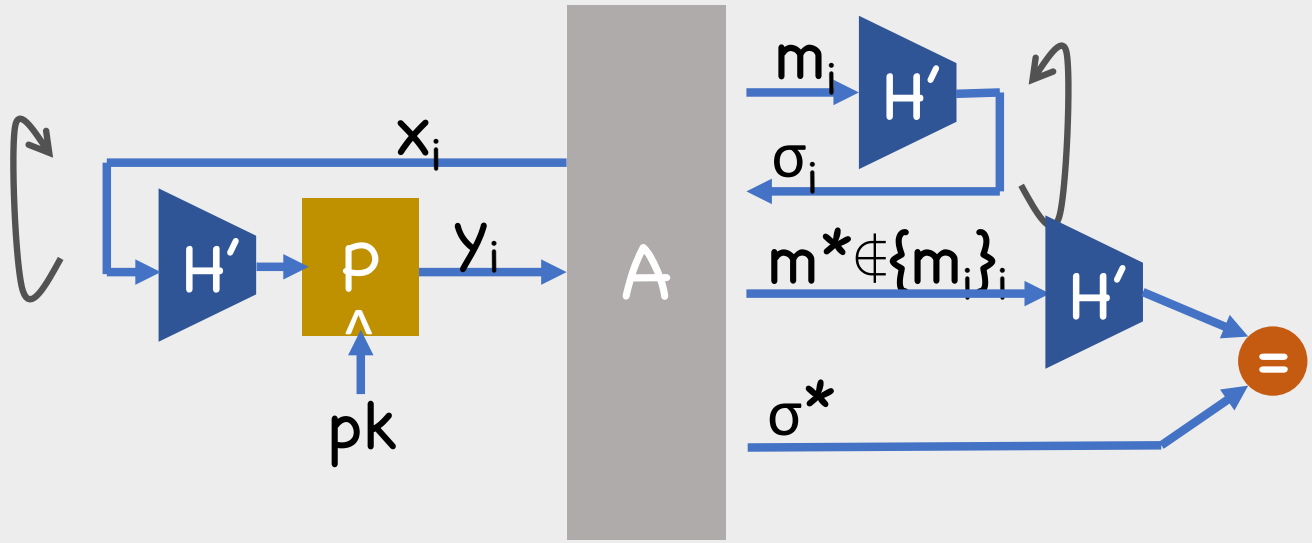
Proof:



Step 1: H → P∘H′

Example: Full Domain Hash

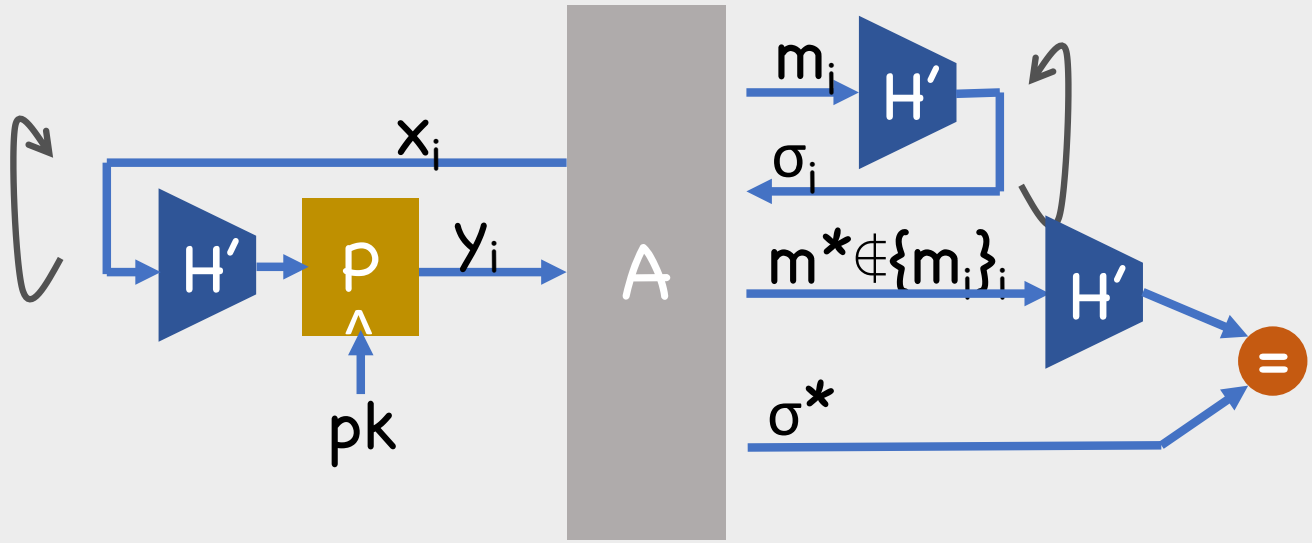
Proof:



Step 1: H → P∘H′

Example: Full Domain Hash

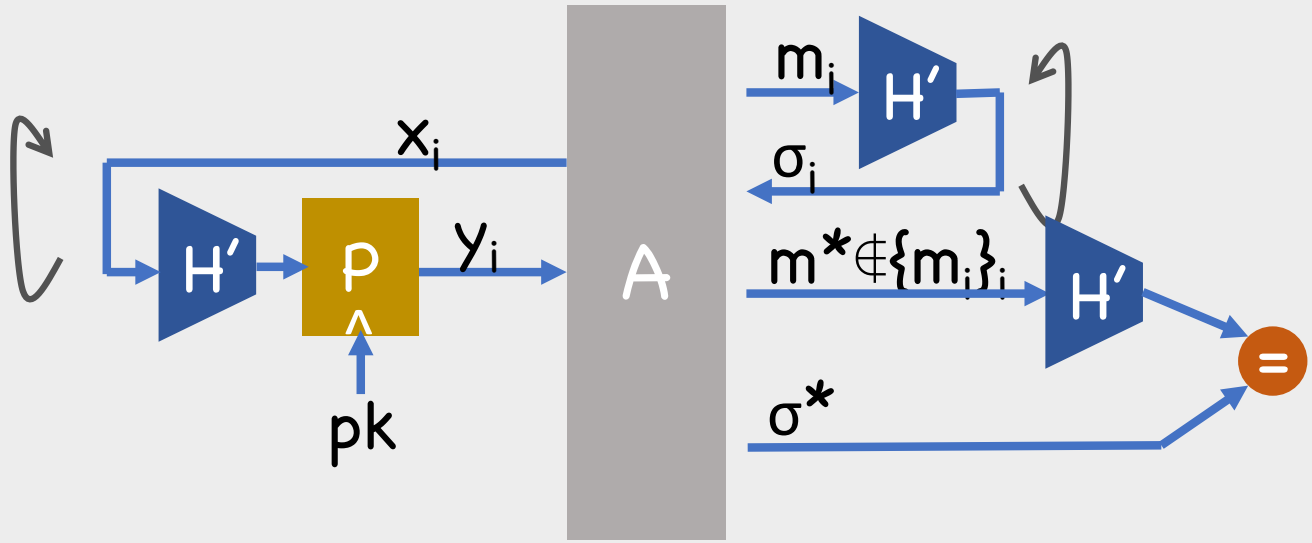
Proof:



Notice: A computes H′(m*), given only P(pk,H′(m*))

Example: Full Domain Hash

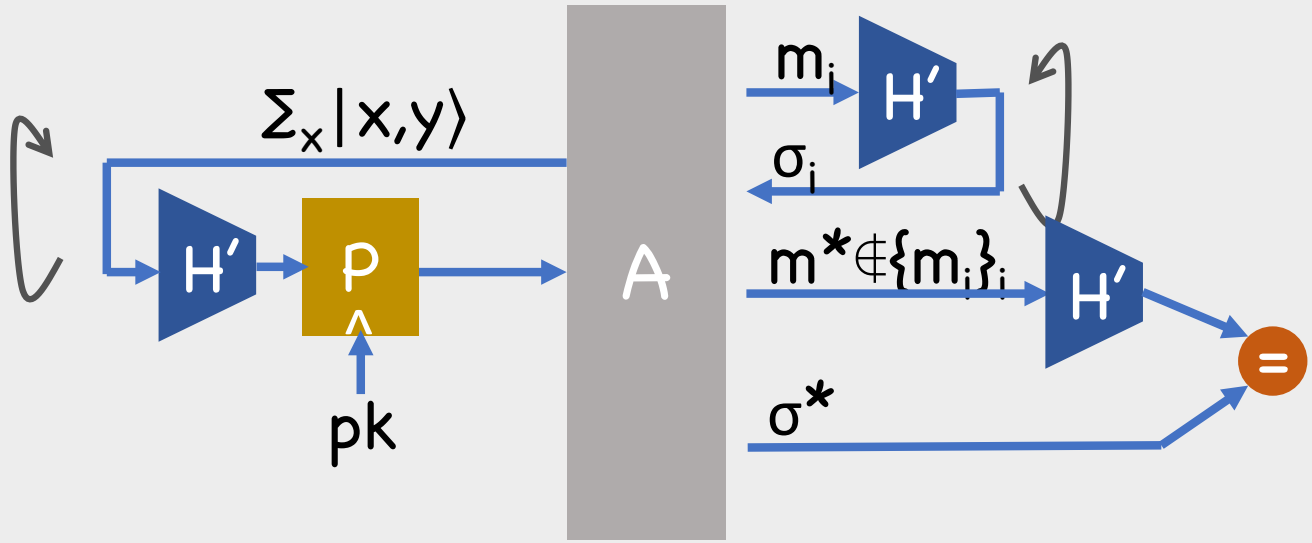
Proof:



B(y): set $H'(x_i)=y$ for random query → advantage ε/q

Example: Full Domain Hash

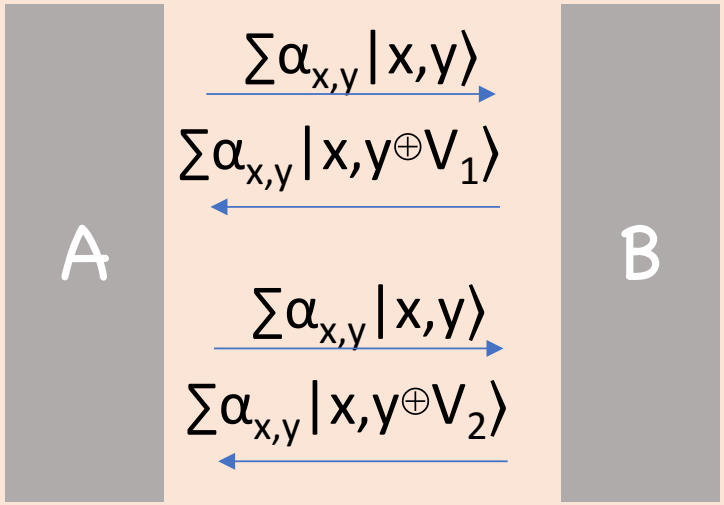
QROM Proof?



How does B insert challenge?

Challenges

Take 1: Per QUERY



Problem: repeated queries?

Problem: distinguishing attack

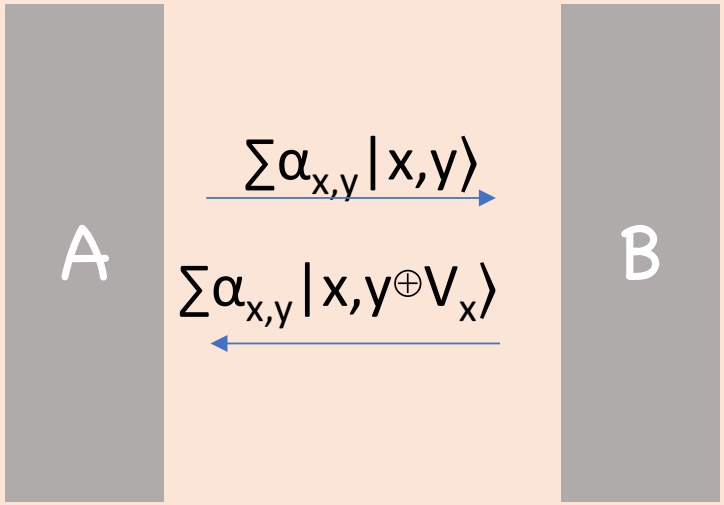
Security Proof Challenges

Typical QROM reductions commit to entire function H at beginning, remain consistent throughout

[Zhang-Yu-Feng-Fan-Zhang'19]: "Committed programming reductions"

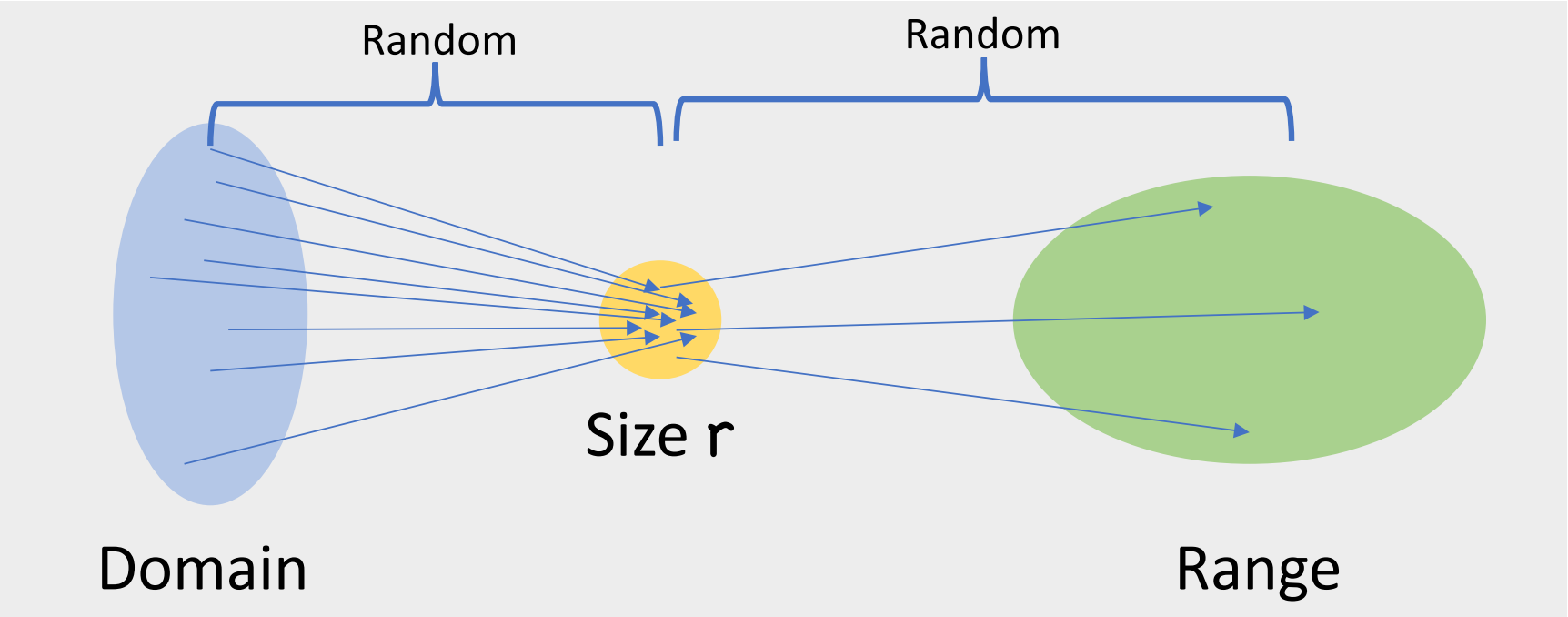
Security Proof Challenges

Take 2: Per VALUE



Problem: exp-many values
→ Pr[correctly guess m*] =negl

Small Range Distributions



Small Range Distributions

Thm [Z'12b]: No q quantum query alg can distinguish SR_r from random, except with probability $O(q^3/r)$.

Quantum collision finding ➡ bound tight

Finishing The Proof

$$\Pr[A \text{ wins} \mid H' \text{ random}] \geq \varepsilon$$

$$\Pr[A \text{ wins} \mid H' = SR_r] \geq \varepsilon - O(q^3/r)$$

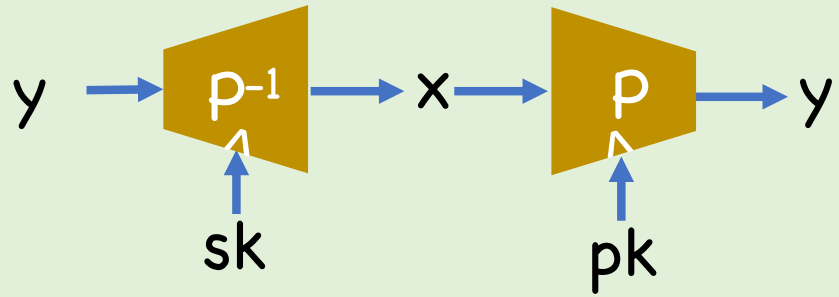
$B(y)$ inserts y into random output

$$\Rightarrow \Pr[B \text{ inverts } y] \geq \varepsilon/r - O(q^3/r^2) = O(\varepsilon^2/q^3)$$

$$r = O(q^3/\varepsilon)$$

Example: Full Domain Hash, Take 2

Building Block: Pre-image Sampleable Funcs

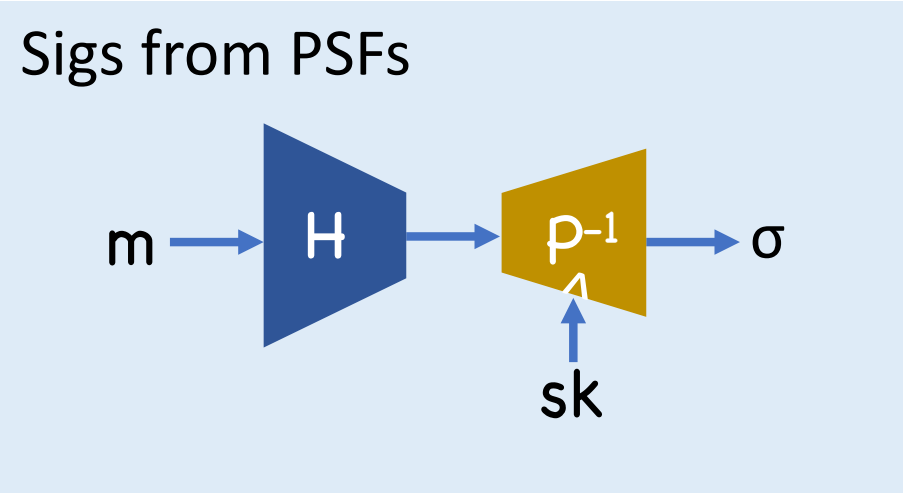


Security: (1) Collision resistant

(2) random y → ≈random x

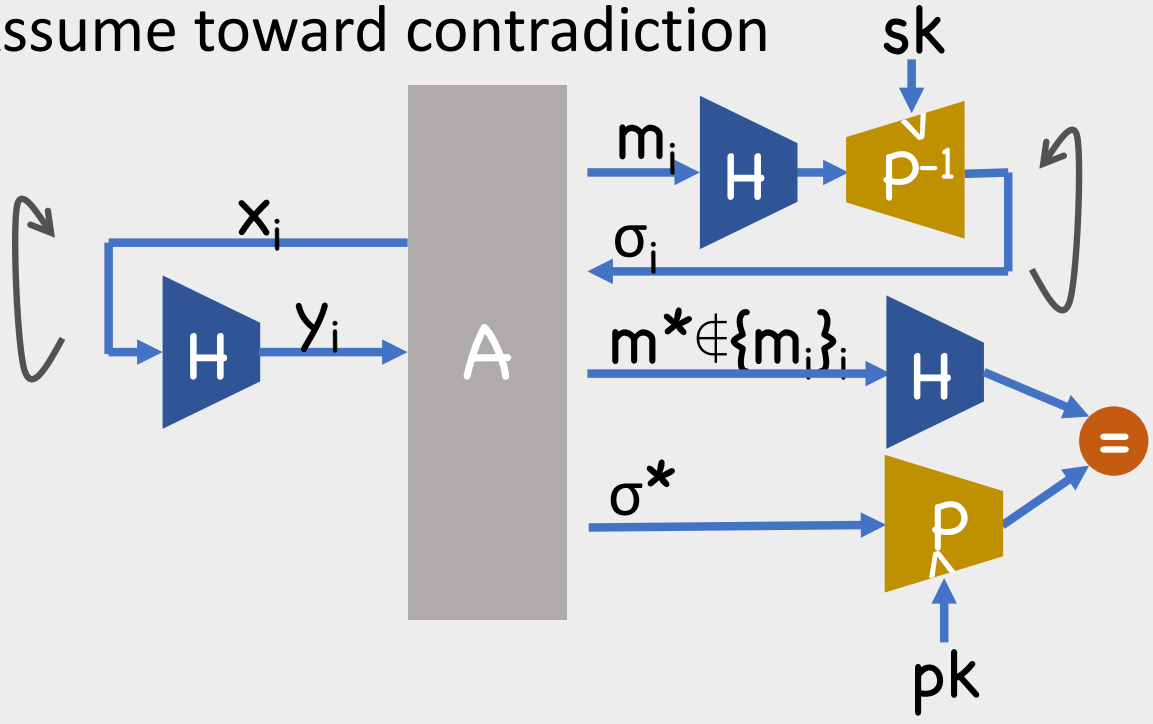
[Gentry-Peikert-Vaikuntanathan'08]: construction from LWE

Example: Full Domain Hash, Take 2



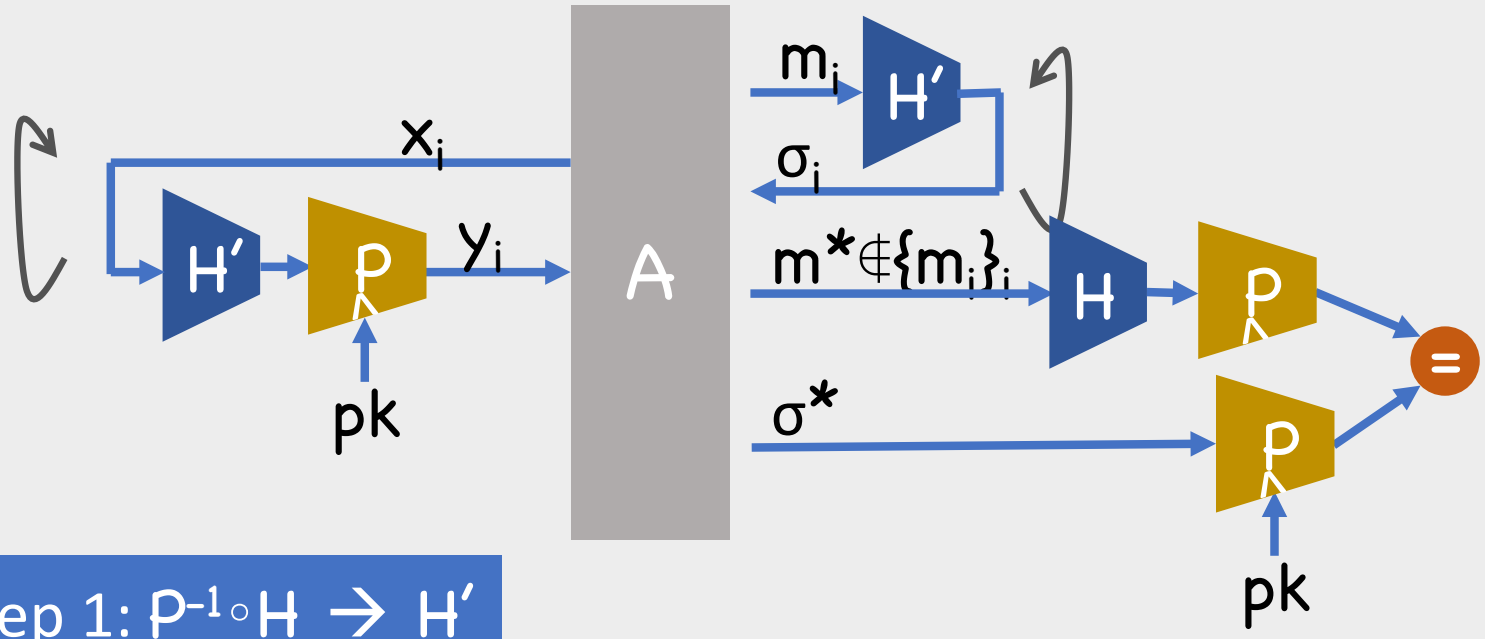
Example: Full Domain Hash, Take 2

Proof: Assume toward contradiction



Example: Full Domain Hash, Take 2

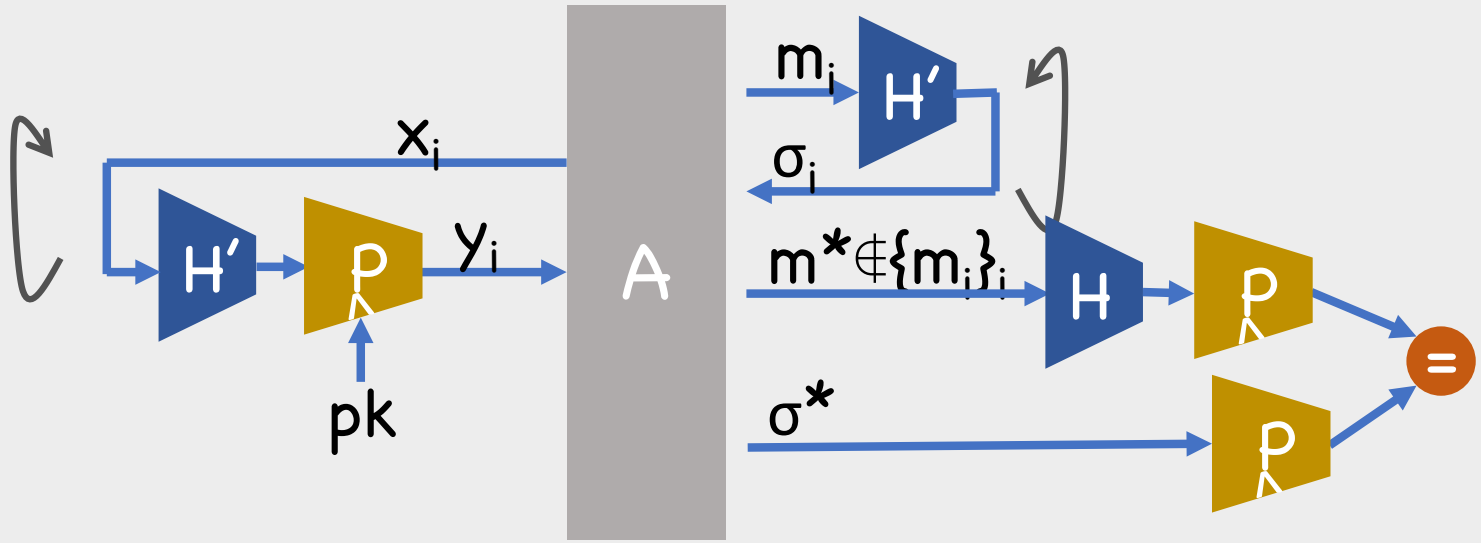
Proof:



Step 1: $P^{-1} \circ H \rightarrow H'$

Example: Full Domain Hash, Take 2

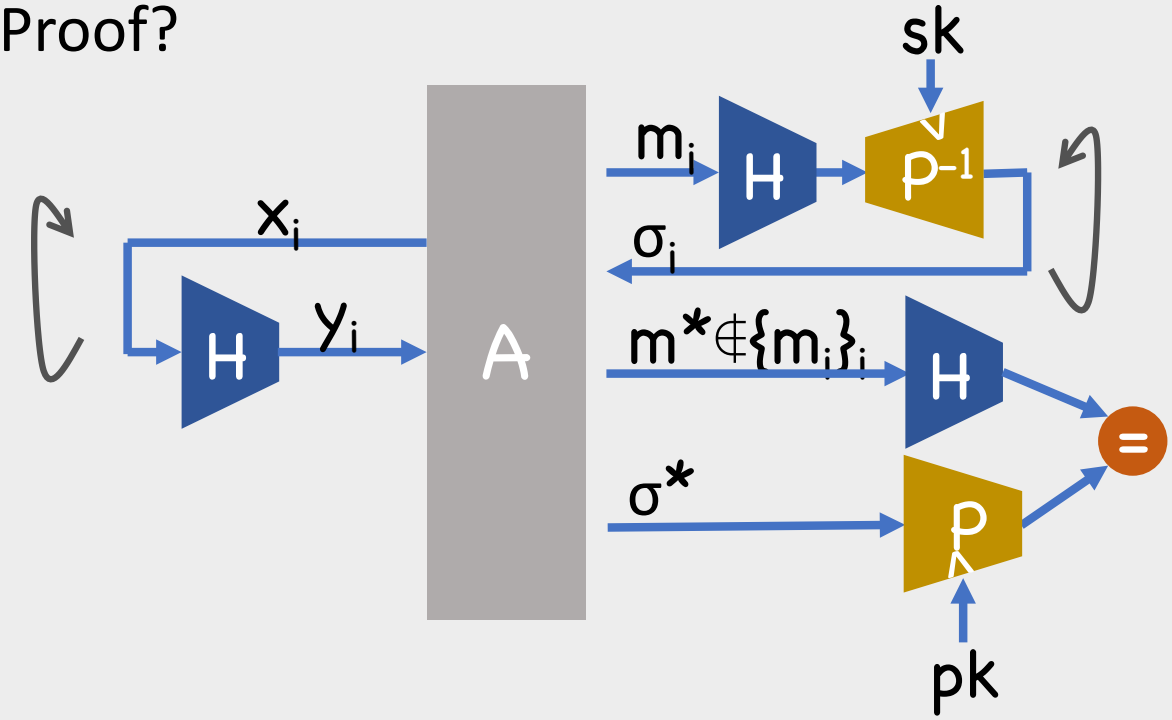
Proof:



Notice: H(m*), σ* form collision → advantage ε

Example: Full Domain Hash, Take 2

QROM Proof?



Example: Full Domain Hash, Take 2

Main* QROM issue: simulating H' efficiently

As before, can do using $2q$-wise independence

*some issues having to do with $P^{-1}(y)$ being only approximately uniform

Rule of Thumb

Rule of Thumb: If loss of classical reduction is independent of **q**, good chance we can upgrade to quantum security

No per query hybrid

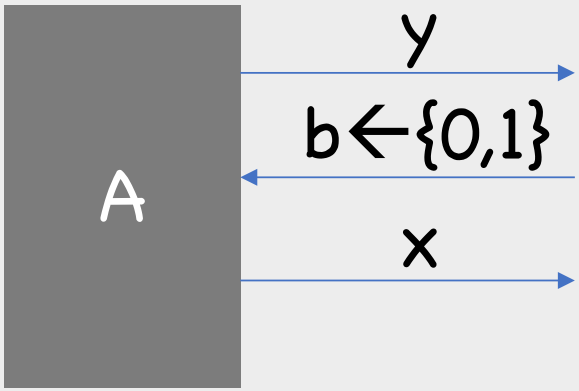
If loss in reduction depends on **q**, new reduction likely needed, maybe impossible

Can All ROM Proofs be Upgraded?

Thm [Yamakawa-Z'20]: No, assuming LWE or relative to an oracle

Recall: Impossibility of Quantum Rewinding
[Ambainis-Rosmanis-Unruh'14]

Coin flipping/commitment game

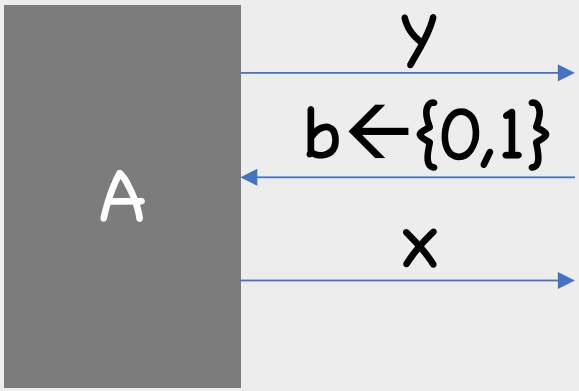


Win if
- Hash(x)=y
- $x_1 = b$

Devised *quantum* A and col. res. Hash where Pr[A wins] ≈ 1

New Game

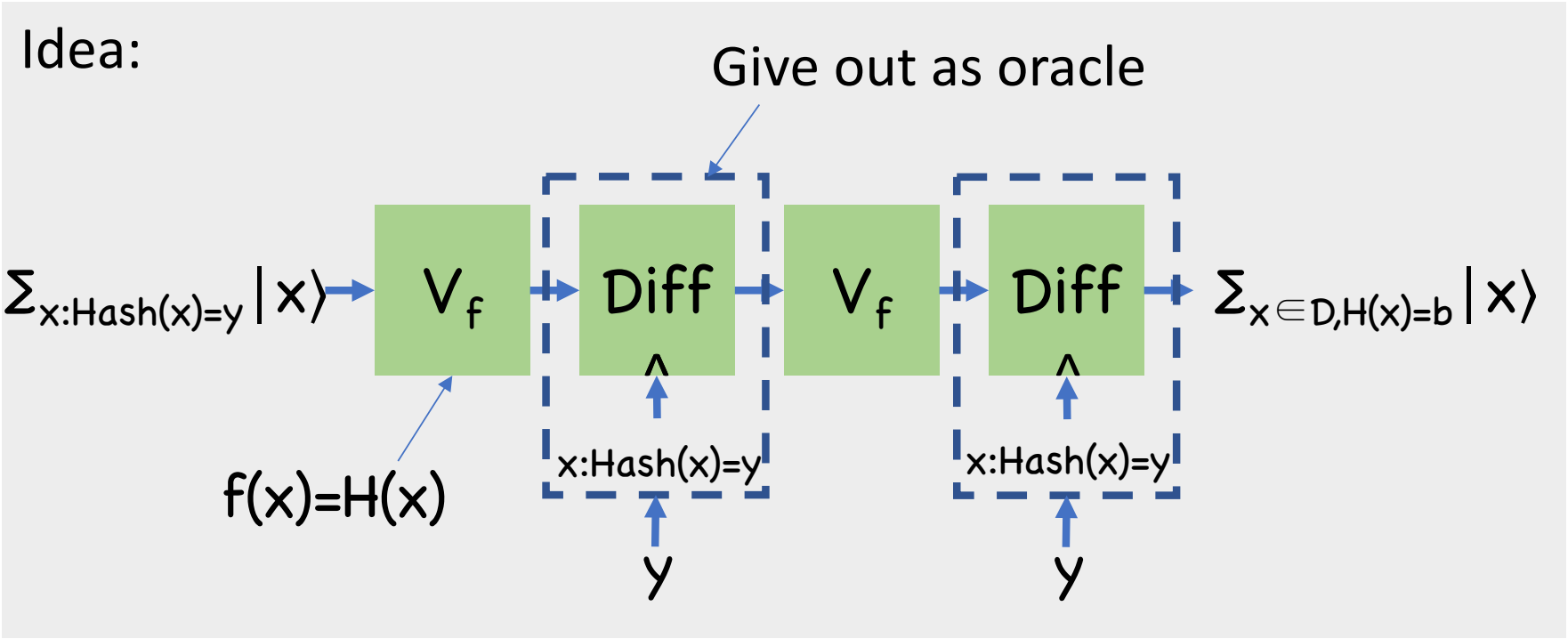
Coin flipping/commitment game



Win if
- Hash(x)=y
- H(x) = b (1-bit RO)

Essentially same A,Hash work here

Quantum Alg


Idea:
Give out as oracle
$\Sigma_{x:Hash(x)=y} |x\rangle$
V_f
Diff
V_f
Diff
$\Sigma_{x \in D, H(x)=b} |x\rangle$
f(x)=H(x)
x:Hash(x)=y
x:Hash(x)=y
y
y

No Classical-Query Alg

Suppose $\exists$ classical query quantum A s.t. $Pr[A \text{ wins}] \geq \frac{1}{2}+\varepsilon$

- Consider H queries on x s.t. $Hash(x)=y$
- First such query x_0 has prob $\frac{1}{2}$ of $H(x_0)=b$
- If A only ever outputs x_0, $Pr[A \text{ wins}] \leq \frac{1}{2}$
- Therefore, A must sometimes output $x_1 \neq x_0$
- But then x_0, x_1 form collision for $Hash$

QROM Impossibility

[Yamakawa-Z'20]: More generally, upgrade proofs of quantumness to proofs of quantum access to RO

Up Next

Tomorrow, will look at further examples

In particular, we will see barriers/impossibilities for committed programming reductions, and how to overcome them