Compressed oracles

Classical Random Oracle

- Say $h: \{0,1\}^n \to \{0,1\}^n$ is hash function
  $D \to D$
- Model h as uniformly random func
- Example: 0-search

$$\Pr[h(x)=0 : x \leftarrow A^h()] \leq \frac{q}{2^n}$$ (← #queries)

Proof sketch (lazy sampling)

- Let h be empty partial function (initially)
- When A queries $h(x)$: $h(x) \xleftarrow{\$} \{0,1\}^n$

Each time: $\Pr[h(x)=0] = 2^{-n}$

$\Rightarrow \Pr[\exists x: h(x)=0] \leq q \cdot 2^{-n}$ ∎

Quantum setting

Quantum query: X, Y → U_{query} → X, Y: $|x,y\rangle \to |x, y \oplus h(x)\rangle$

→ A can perform queries in superpos

⇒ Breaks lazy sampling

Zhandry's compressed oracles

- Can do kind of lazy sampling
  ⇒ Gives a lot of post-q security proofs.
- But: Cannot handle invertible permutations
- Why are inv. perms important?
  - ↳ Sponge / SHA3
  - ↳ Ideal ciphers
  - ↳ Proofs involving strong qPRP

Our approach

Step 1: "Standard oracle"

Instead of: $h \xleftarrow{\$} (D \to R)$ — X, Y → U_{qu} → X, Y, $U_{qu}|x,y\rangle \to |x, y \oplus h(x)\rangle$

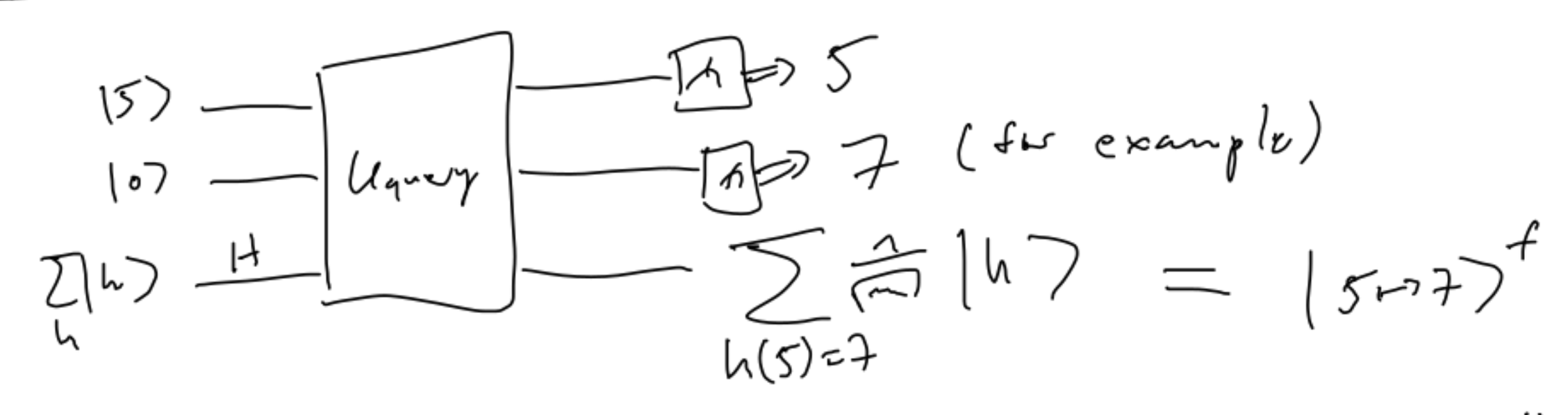
We do:

$$H \leftarrow \sum_{h: D \to R} \frac{1}{\sqrt{|D \to R|}} |h\rangle$$

$|x,y,h\rangle \to |x, y \oplus h(x), h\rangle$

Standard tools ⇒ std. oracle perf. indist. from orig. RO

Why useful? Example:



$$\sum_{h(5)=7} \frac{1}{\sqrt{\cdots}} |h\rangle = |5 \mapsto 7\rangle^f$$

Idea: Describe oracle state in terms of "restr. h-superpositions"

$$|f\rangle^f := \sum_{h \text{ compat. with } f} \frac{1}{\sqrt{\cdots}} |h\rangle$$

(f ← partial function)

(compatible: if $f(x) \neq \bot \Rightarrow f(x) = h(x)$)

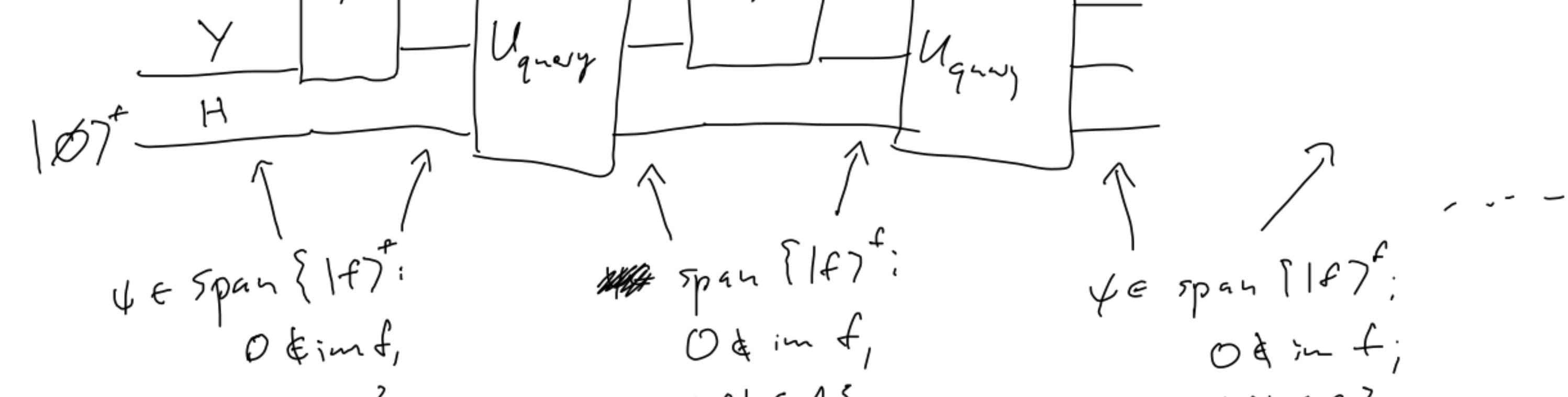
Example:

$\mathcal{H}_{EXY} \otimes \text{span}\{|f\rangle^f : 0 \notin \text{im } f\}$

says: no 0-output was found

Proof sketch (that 0-search is hard)

$$\Pr[H(x)=0 : x \leftarrow A^h()] \in O\left(\frac{q^2}{2^n}\right)$$



$\psi \in \text{span}\{|f\rangle^f : 0 \notin \text{im} f, |f| \leq 0\}$

$\text{span}\{|f\rangle^f : 0 \notin \text{im } f, |f| \leq 1\}$ — $\psi \overset{4\sqrt{2^{-n}}}{\approx}$

$\psi \in \text{span}\{|f\rangle^f : 0 \notin \text{im } f; |f| \leq 2\}$ — $\psi \overset{2 \cdot 4\sqrt{2^{-n}}}{\approx}$

. . . .

⇒ final $4q\sqrt{2^{-n}}$ far from "0-free state"

$$\Rightarrow \Pr[H(x)=0] \leq (\cdot)^2 = \frac{16 q^2}{2^{-n}}$$

Main thm (sketch)

If $\psi \overset{\varepsilon}{\approx} \text{span}\{|f\rangle^f : f \in A, |f| \leq \ell\}$

Then $U_{query}\psi \overset{\varepsilon + 4\sqrt{c}}{\approx} \text{span}\{|f\rangle^f : f \in A, |f| \leq \ell + 1\}$

Assuming: $\forall f \in A$ with $|f| \leq \ell : \forall x$

$$\frac{|\{z : f(x := z) \notin A\}|}{2^n} \leq c$$

Zhandry:

$$|5 \mapsto 7\rangle \not\rightsquigarrow \sum_{h(5)=7} \frac{1}{\sqrt{\cdot}} |h\rangle$$

$$\rightsquigarrow \sum_{h(5)=7} + \frac{1}{\sqrt{2^{-n}}} \sum_{h(5)=1} \frac{1}{\sqrt{\cdot}} |h\rangle - \frac{1}{\sqrt{2^{-n}}} \sum_{h} \frac{1}{\sqrt{\cdot}} |h\rangle$$

(correction)

Permutations

Invertible std oracle

Init state of H: $\sum_{h: D \hookrightarrow D} \frac{1}{\sqrt{\cdots}} |h\rangle$

Query: U_{query} $|x,y,h\rangle \to |x, y \oplus h(x), h\rangle$

Invert: $|h\rangle \mapsto |h^{-1}\rangle$

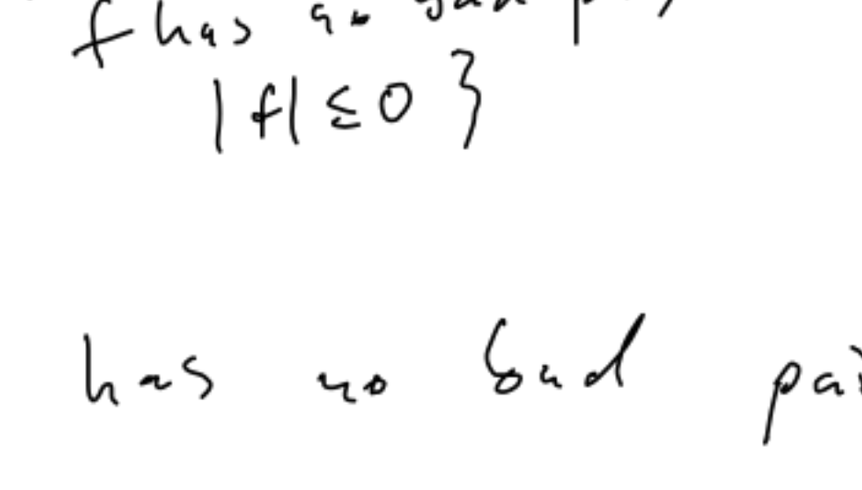
Def: $|f\rangle^P := \sum_{\substack{h: D \hookrightarrow D \\ h, f \text{ compatible}}} \frac{1}{\sqrt{\cdots}} |h\rangle$ E.g.: $|\emptyset\rangle^P = \sum_{h: D \hookrightarrow D} \frac{1}{\sqrt{\cdots}} |h\rangle$

$$\Rightarrow \Pr[h(x)=0 : x \leftarrow A^h()] \in O\left(\frac{q^2}{2^n}\right)$$ for h perm.

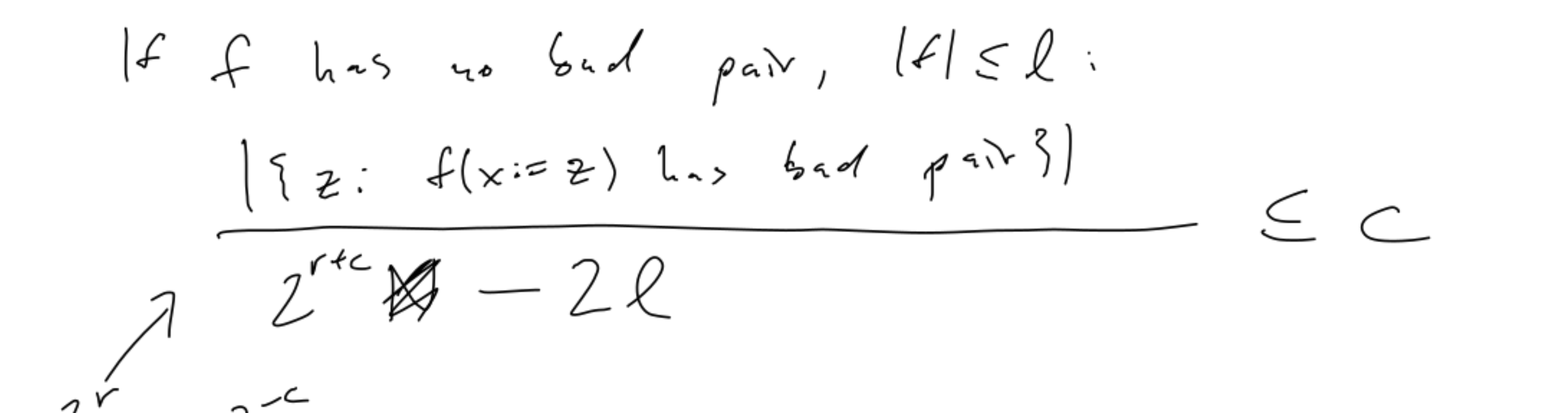
Invert $|f\rangle^P = |f^{-1}\rangle^P$

⇒ Invariants are simply inverted

Example: 2 sided 0-search



(x,y) "bad pair"



$\text{span}\{|f\rangle^P : f$ has no bad pair $|f| \leq 0\}$

$\text{span}\{|f\rangle^P : f$ has no bad pair, $|f| \leq 1\}$ (error $\sim 4\sqrt{2^{-r}}$)

If f has no bad pair, $|f| \leq \ell$:

$$\frac{|\{z : f(x := z) \text{ has bad pair}\}|}{2^{r+c} - 2\ell} \leq c$$

$\sim \frac{2^r}{2^{r+c}} = 2^{-c}$

⇒ final state $\sim 4q\sqrt{2^{-r}}$ - close to invariant

$$\Rightarrow \Pr[\text{find bad pair}] \leq O\left(\frac{q^2}{2^r}\right)$$

Sponge: $\Pr[\text{coll}] \in O\left(\frac{q^3}{2^{\min\{c,d\}}}\right)$

SHA3-512: $\frac{q^3}{2^{512}} \rightsquigarrow \sim 2^{170}$ queries