Compressed oracle technique

- Random oracle

  → Replace hash fun ⇝ random func

  Heuristic: If proven in ROM

  ⇒ assumed secure with real-life hash func

Why easier?

Example: 0-preimage finding

$$\begin{bmatrix} H \xleftarrow{\$} (X \to Y) \\ x \leftarrow A^H \quad // q\text{-queries} \\ win := [H(x) = 0] \end{bmatrix}$$

$$\Pr[win] \le \frac{q+1}{|Y|}$$

Proof:

(1) Replace H by lazy H

(2) When lazy sampling each H query made by A gives a rand output.
$\to \Pr[=0] = \frac{1}{|Y|}$

Lazy sampling

Instead of using $H \xleftarrow{\$} (X \to Y)$

we use a stateful oracle H:

- When queried on "fresh" x: return $\$$
- When queried on same x again: return previous value.

Thm: $H \xleftarrow{\$} (X \to Y)$ is perfectly indist. from lazy-samp. H

Quantum random oracle

- In Q setting: can eval. a hash func H in superpos.

$$\sum_{xy} \alpha_{xy} |x\rangle |0\rangle \longrightarrow \sum \alpha_{xy} |x\rangle |H(x)\rangle$$

E.g: Using superpos. queries, can do 0-preimage finding in $O(\sqrt{|Y|})$ queries (Grover)

Need to update the ROM: QROM:

- Difference: A gets superpos. access to H

$H \xleftarrow{\$} (X \to Y)$

$x \leftarrow A^{|H\rangle}$ // q-queries

win := $[H(x) = 0]$

$\Pr[\text{win}] \leq$?

$|x\rangle|y\rangle \to |x\rangle|y+H(x)\rangle$

Why difficult to prove?

Lazy sampling does not work*

- Classical: When $H(x)$ is first queried: pick $H(x)$

Consider: $\sum |x\rangle|0\rangle \longrightarrow \sum |x\rangle|H(x)\rangle$

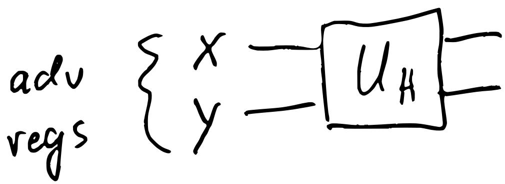
* in the normal way

Compressed oracles

Step 1 "Normal" QROM

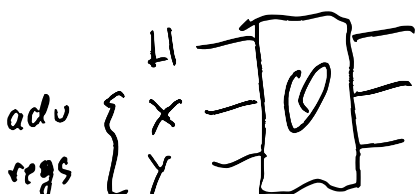
$$H \xleftarrow{\$} (X \to Y)$$

$$U_H : |x, y\rangle \mapsto |x, y + H(x)\rangle$$



Step 2: Superpos. between oracles

New register $H \leftarrow \sum_{h \in X \to Y} |h\rangle$



$$\mathcal{O} : |h, x, y\rangle \mapsto |h, x, y + h(x)\rangle$$

Thm: Normal QROM perf. indist from $\mathcal{O}$

Representing H (the state reg.)

$h : X \to Y$ can be written as

$(h_1, h_2, h_3, \ldots)$ $\quad h_i := h(i)$

H can be repr. as $H_1, H_2, H_3, \ldots$,

one for every input.

Extend H_x a bit.

Normally: Space of H_x is $\mathbb{C}^Y$,

in other words: $|y\rangle$ $(y \in Y)$

Now: Space of H_x is $\mathbb{C}^{Y \cup \{\perp\}}$

in other words: $|y\rangle$ $(y \in Y)$ or $|\perp\rangle$

$$|*\rangle := \sum_{y \in Y} |y\rangle$$

Initial state: $H \leftarrow \sum_h |h\rangle$

becomes: $H_x \leftarrow |*\rangle$ for all x

<u>Step 3</u>: Identifying undef. outputs

$H_x = |*\rangle$ means that $h(x)$ is undef.

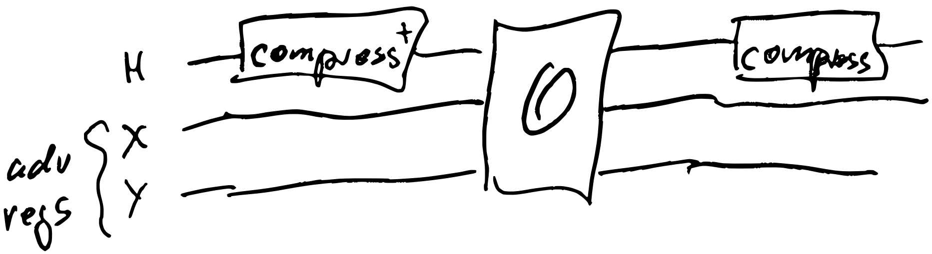
Want a unitary: that transforms $|*\rangle$ into $|\perp\rangle$

$$\text{Compress}_1 : |y\rangle \to |y\rangle \quad \text{(def'd stays def'd)}$$
$$|*\rangle \to |\perp\rangle \quad \text{($*$ means undef)}$$

Initial state: $H \leftarrow \text{compress} \cdot \underbrace{\sum |h\rangle}$

$\hookrightarrow |*\rangle|*\rangle|*\rangle \dots$

$\hookrightarrow \text{compress}_1$ on each H_x



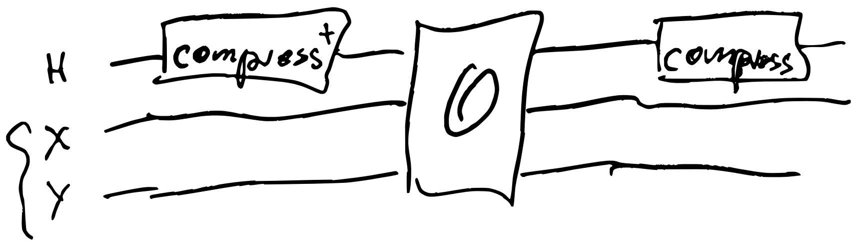
Thm: This "compressed oracle" is perfectly indist from O

(1) Initial state is $\text{compress}_1 |*\rangle \otimes \text{compress}_1 |*\rangle \otimes \dots$

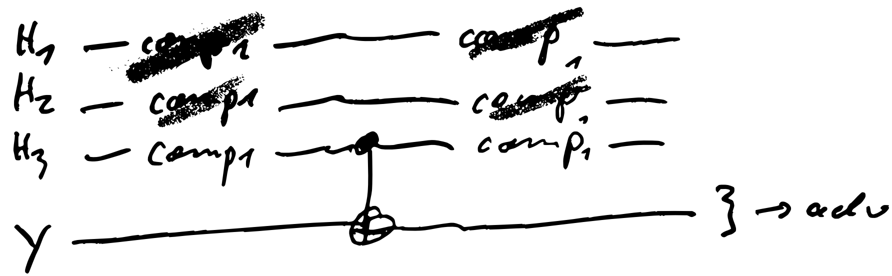
$= |\perp\rangle \otimes |\perp\rangle \otimes \dots$

What does a query do?

Say: $X = |3\rangle$



$\equiv$



$\Rightarrow$ at most one H_x can become non-$|1\rangle$ in each query

$\Rightarrow$ After q queries: H is superpos of $|h\rangle$ with $|h| \le q$

Big problem: $\mathrm{compress}_1$ does not exist!

$$\mathrm{compress}_1 |*\rangle = |\bot\rangle$$

$$\mathrm{compress}_1 |*\rangle = \mathrm{compress}_1 \left(\sum |y\rangle\right)$$

$$= \sum \mathrm{compress}_1 |y\rangle = \sum |y\rangle \neq |\bot\rangle$$

$$\lightning$$

<u>But:</u> $\exists$ unitary $\mathrm{compress}_1$:

$$\mathrm{compress}_1 |*\rangle \approx |\bot\rangle$$

$$\mathrm{compress}_1 |y\rangle = |y\rangle + \mathrm{small}_y$$

Example: 0-preimage finding

$$\left[\begin{array}{l} H \xleftarrow{\$} (X \to Y) \\ x \leftarrow A^{|H\rangle} \\ \text{win} := [H(x) = 0] \end{array}\right.$$

Step 1: Replace $|H\rangle$ by CO.

$H \leftarrow |\bot\rangle \dots |\bot\rangle$

$x \leftarrow A^{CO}$

win $= [H(x) = 0]$

Invariant: $I := \mathrm{span}\{|h\rangle : 0 \notin \mathrm{im}(h)\}$

Initial state $\in I$

By some computing: If state $\psi \in I$ before query then $CO \cdot \psi \overset{1/\sqrt{|Y|}}{\approx} I$.

In the end:

$O(q/\sqrt{Y})$-far

$\Rightarrow$ if $q \ll \sqrt{Y}$ then you don't find 0

$\psi_x + \varepsilon$ $\quad\quad$ $\|\varepsilon\| = \frac{1}{\sqrt{Y}}$

$\sum_x \alpha_x (\psi_x + \varepsilon)$

Error: $\sum_x \alpha_x \varepsilon$ can be $\sqrt{|Y|} \cdot \varepsilon$