CS 258: Quantum Cryptography

Mark Zhandry

Previously…

The Fundamental Formula of Modern Cryptography

Secure Cryptosystem =

Protocol

\+

Formal Security Model **M** — Usually conservative modeling of adversary's capabilities

\+

Computational Assumption **P** — Widely studied, concrete assumptions

\+

Proof that **P** implies **M** — Breaking **M** at least as hard as solving **P**

Formal Security Model **M**

Classically, typically of the form:
"For all PPT adversaries $\mathcal{A}$, there exists a negligible $\epsilon(\lambda)$ such that $\Pr[\mathcal{A} \ldots] \leq \epsilon(\lambda)$ "

The “obvious” way to adapt classical definitions to the quantum setting is to simply replace PPT with QPT

Computational Assumption **P**

Classically, typically of the form:
"For all PPT adversaries $\mathcal{A}$, there exists a negligible $\epsilon(\lambda)$ such that $\Pr[\mathcal{A}....] \leq \epsilon(\lambda)$ "

The "obvious" way to adapt classical assumptions to the quantum setting, again is to simply replace PPT with QPT

Sometimes these assumptions will be false (e.g. DLog); in this case replace with suitable post-quantum assumptions

Proof that **P** implies **M**

Classical proofs are a reduction, transforming PPT adversary $\mathcal{A}$ for **M** into PPT algorithm $\mathcal{B}$ for **P**

Classical reductions take classical inputs and produce classical outputs

If we feed a quantum $\mathcal{A}$ into the reduction, will the output $\mathcal{B}$ be anything meaningful?

All the proofs we’ve seen so far in this course work out quantumly:

CPA security from LWE

Collision resistance from Dlog on group action

CPA security from DDH on groups / group actions

Hardness of LWE from hardness of SIS

Let’s see an example where this fails!

Commitments from collision-resistance

Def (Commitment, Computational Sum-Binding): A commitment scheme is **classically/quantumly sum-binding** if, for all PPT/QPT adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[W_0] + \Pr[W_1] \leq 1 + \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that $\mathcal{A}$ succeeds in the following:

- $\mathcal{A}$ produces a commitment c and two msgs $m_0, m_1 \in \{0,1\}^*$ *of the same length*
- Give b to $\mathcal{A}$
- $\mathcal{A}$ tries to output $r \in \{0,1\}^\lambda$ s.t. $c = \mathsf{Com}(m_b, r)$

Lemma (informal): If H is classically collision-resistant, then Com is classically sum-binding

Intuition: if you could "open" c to two distinct messages, that would give a collision for H

Challenge: in security proof, commitment adversary only gives us one opening. How to we get two for a collision?

Solution: Keep program trace, get one input, "rewind" adversary, and run again to get second

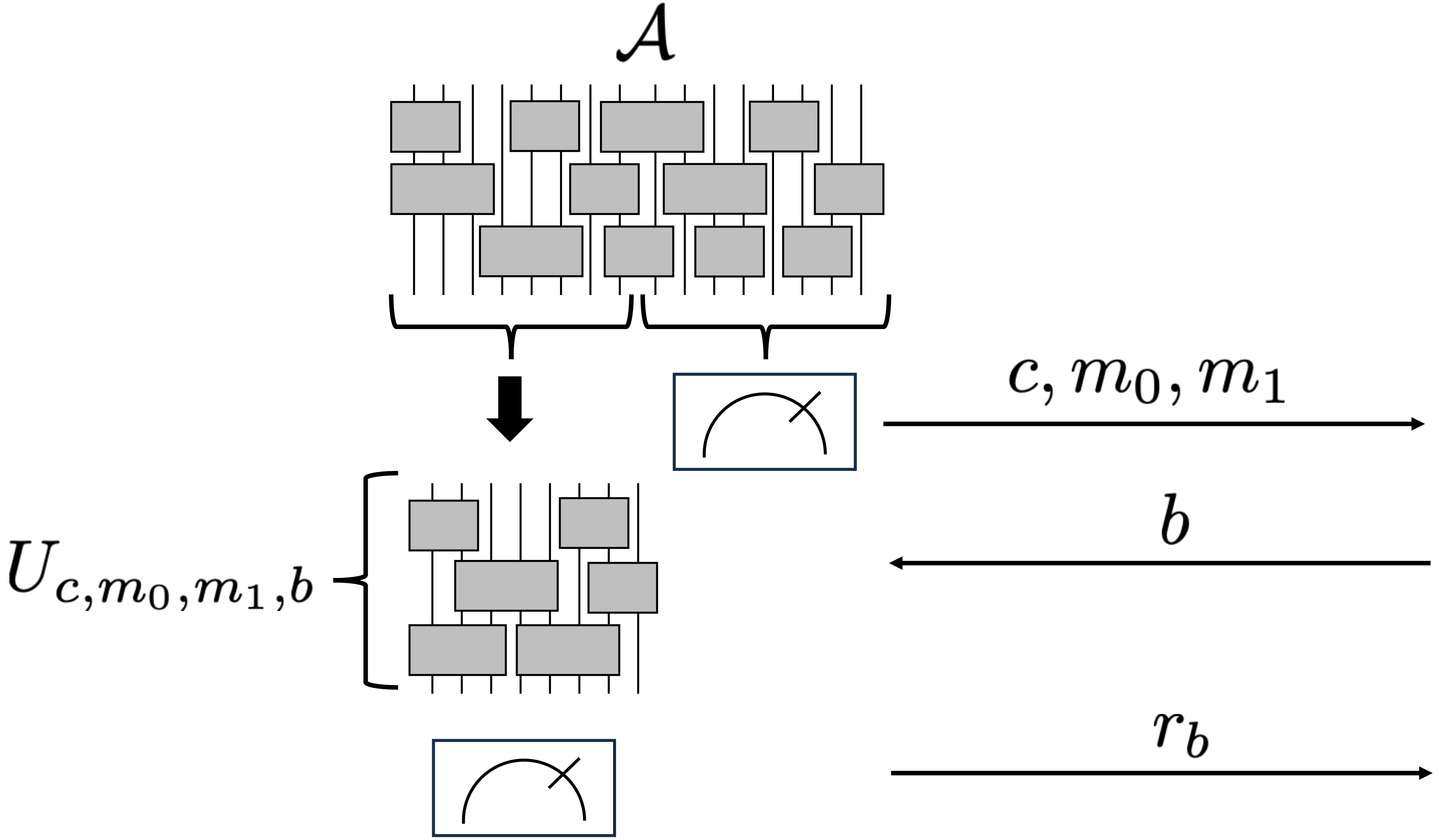
Ok, so what happens when we move to quantum?

Recall that $\mathcal{B}$ runs $\mathcal{A}$, but keeps a program trace so that it can return to a previous state

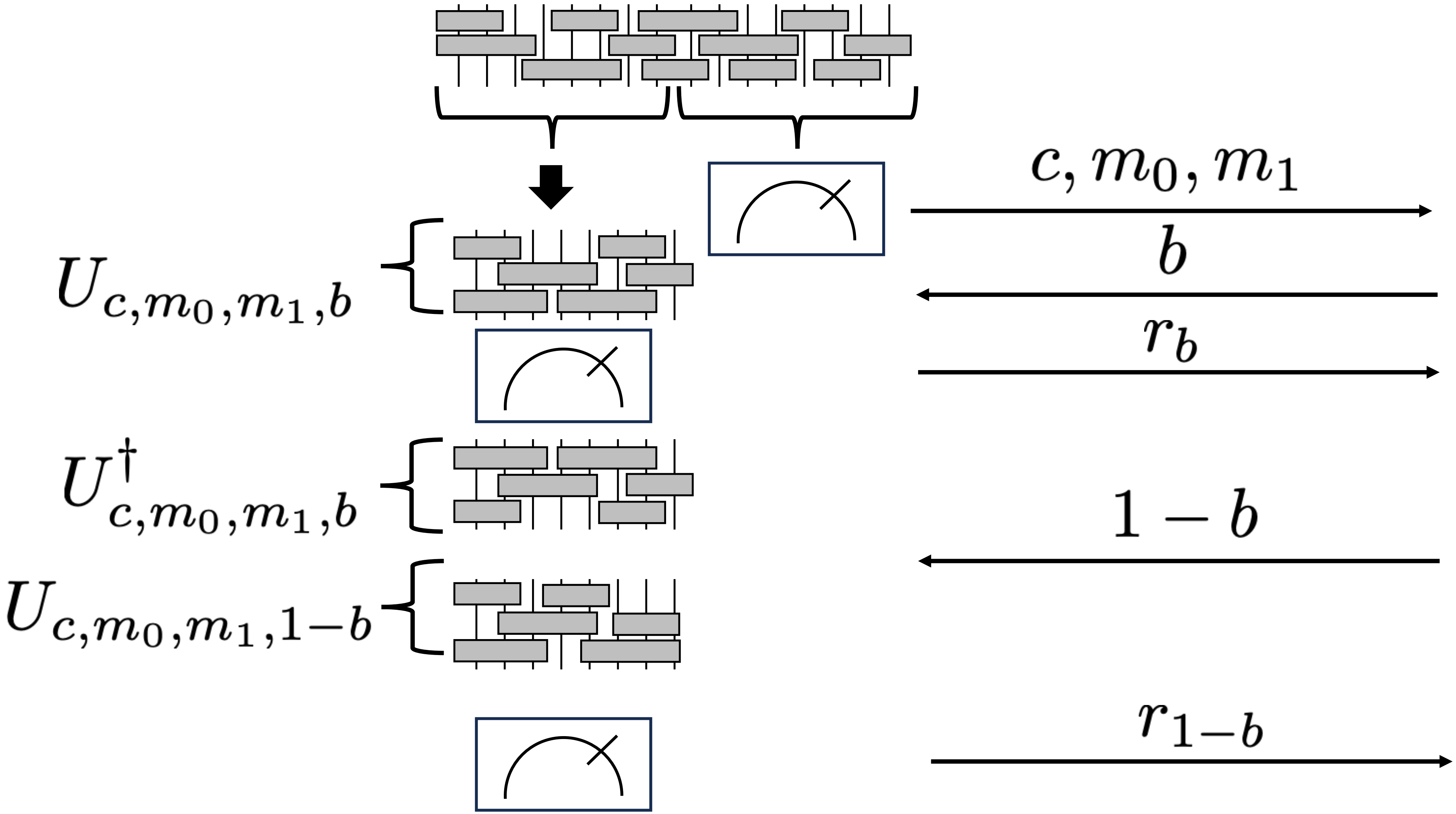
This simply does not make sense quantumly. By observer effect, extracting r_0 may have irreversibly altered the state of $\mathcal{A}$, so there's no returning to it

Today: what to do about rewinding

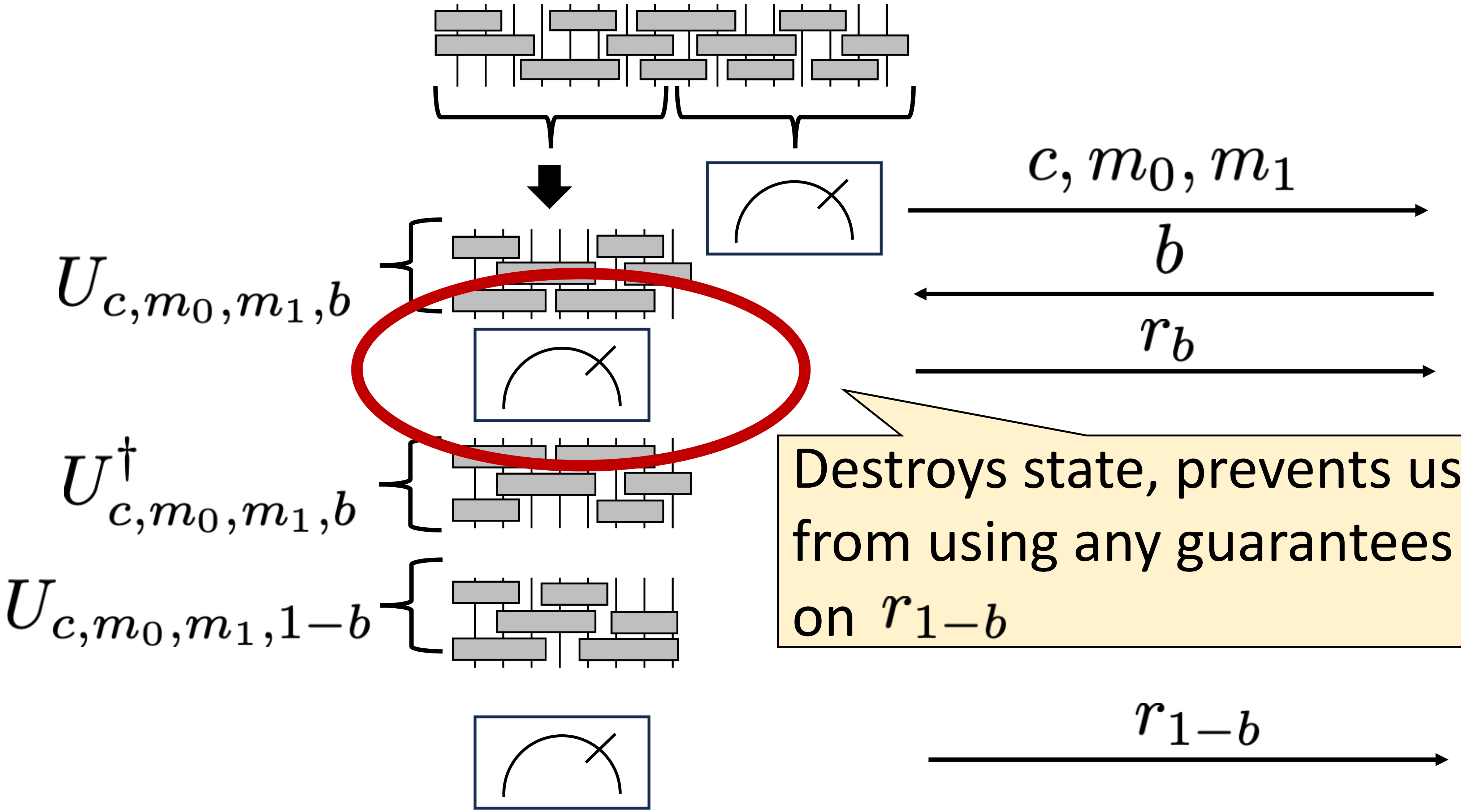
Modeling the adversary



Natural idea: rewind anyway

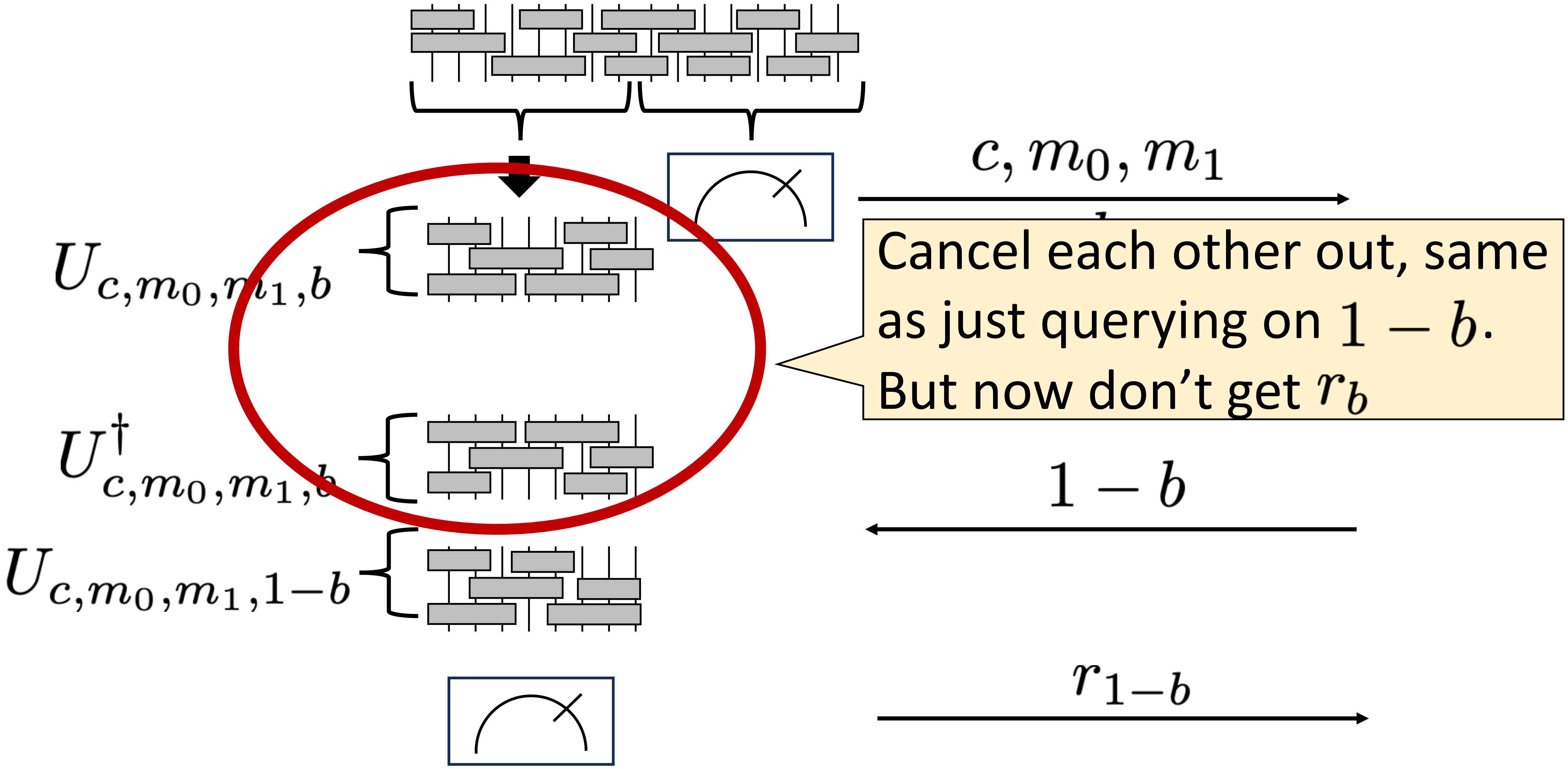


Doesn't work

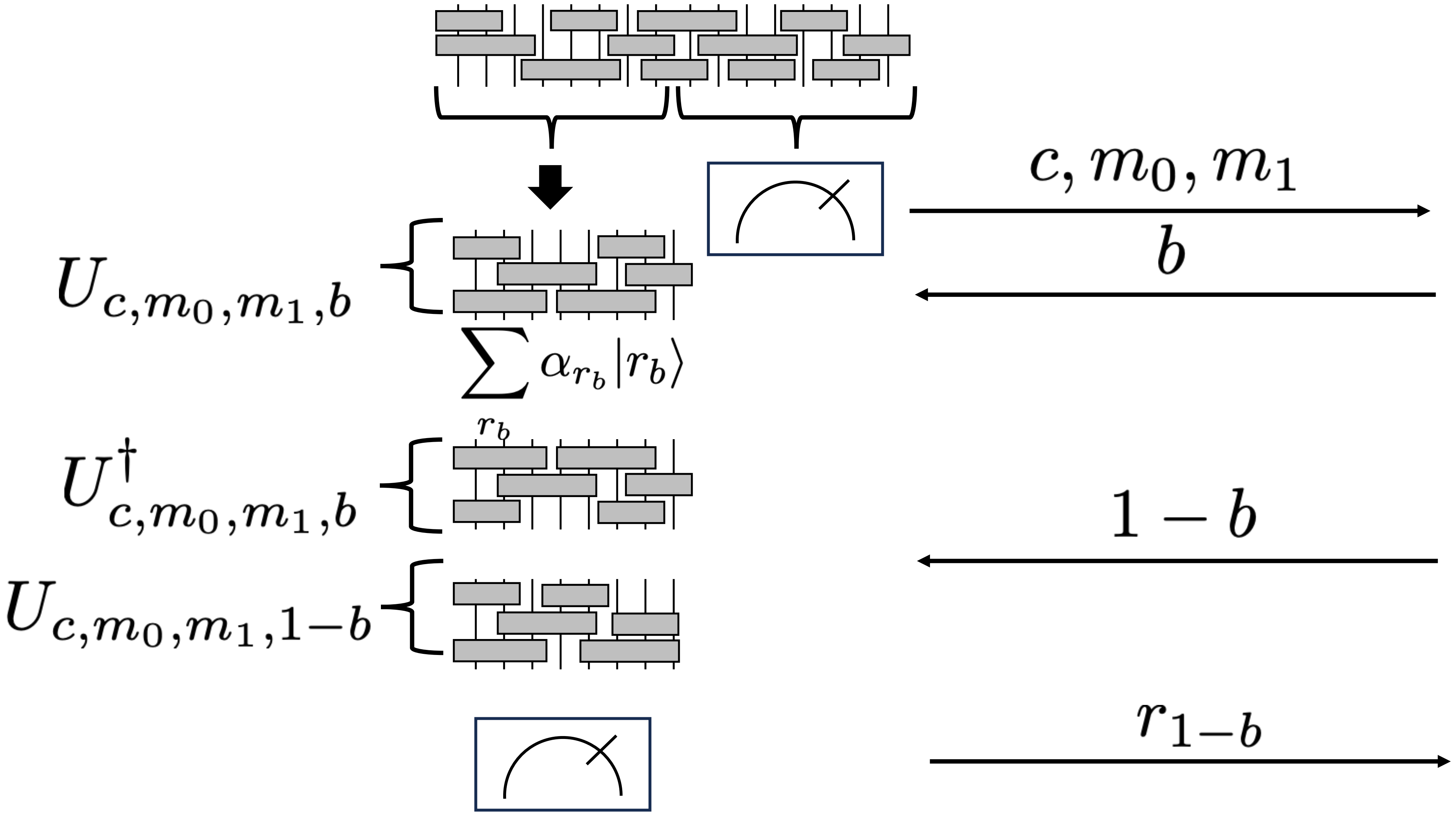


Destroys state, prevents us from using any guarantees on r_{1-b}

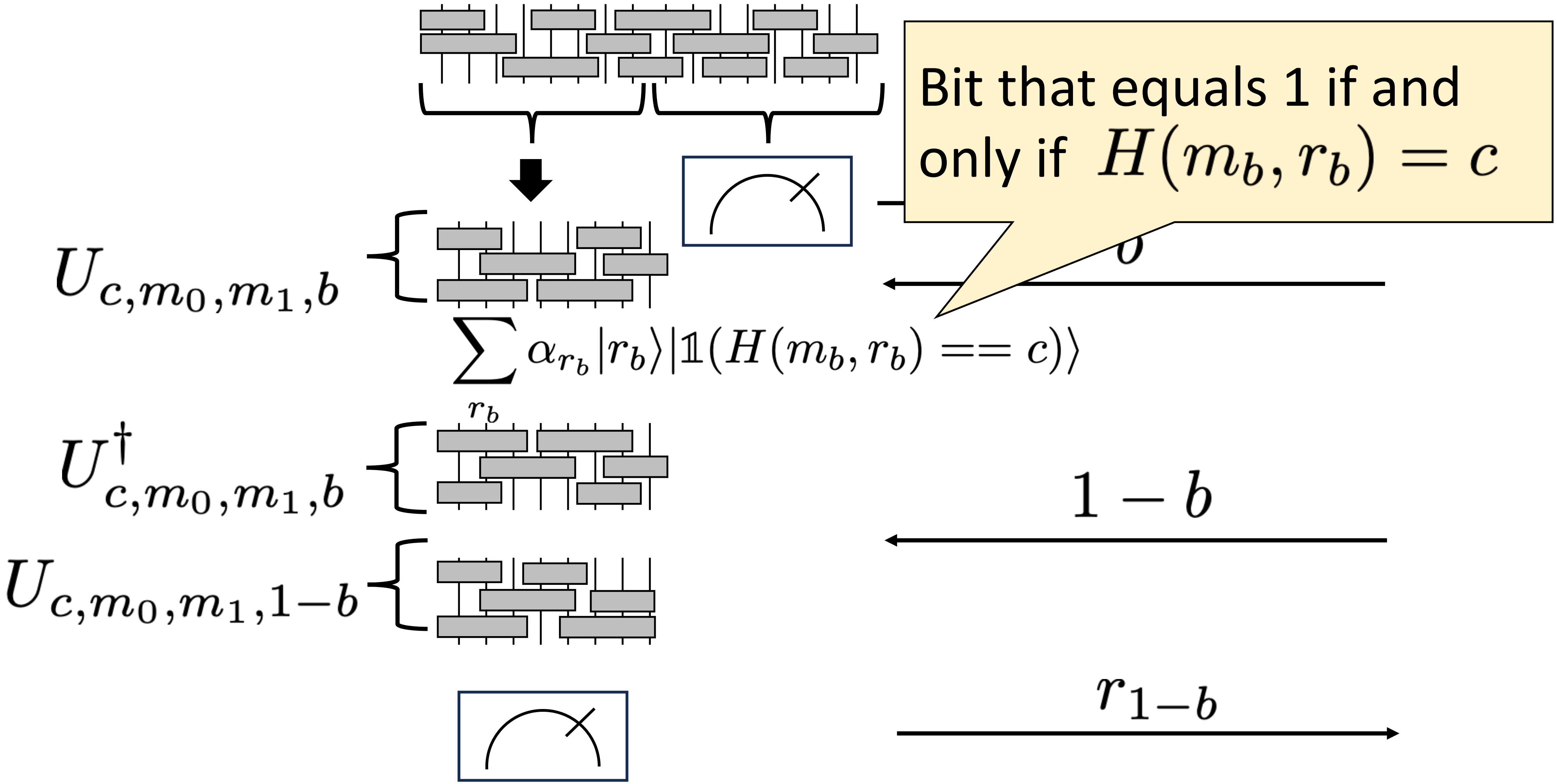
Let’s remove the problematic measurement



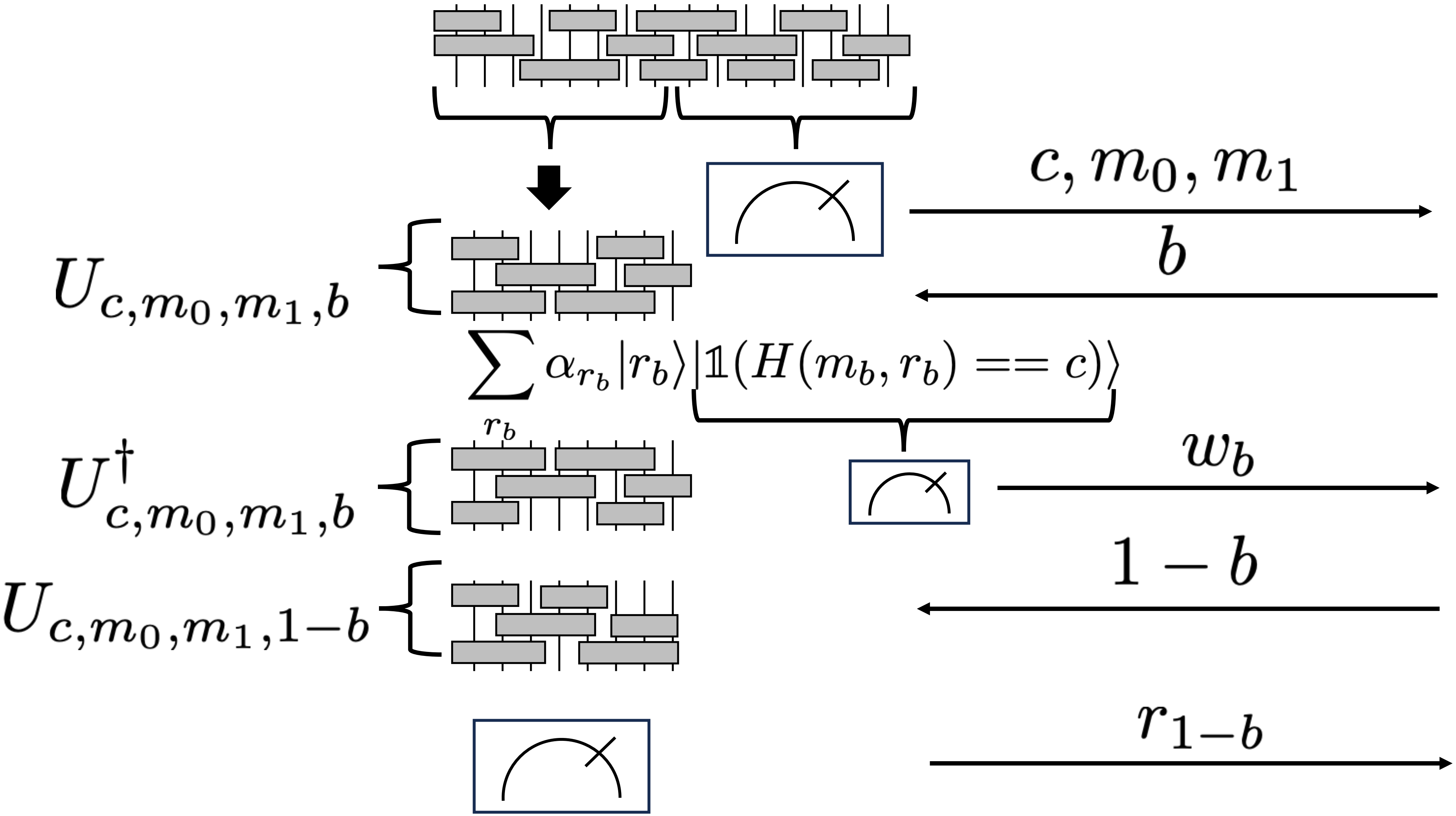
Something between



Something between



Something between



We still changed the state by measuring w_b

But w_b is just a bit - maybe change is small?

Gentle Measurement Lemma

Lemma: Consider two computations

(1) $|\psi\rangle \to T \to V \to M_1$ and (2)$|\psi\rangle \to T \to U \to M_0 \to U^\dagger \to V \to M_1$

Where T, U, V are unitaries and M_0, M_1 measure a single qubit.

Let p_1 be probability M_1 outputs 1 in (1)

Let p_0 be probability M_0 outputs 1 in (2)

Let p_1' be probability M_1 outputs 1 in (2), conditioned on M_0 outputting 1

Then $|p_1 - p_1'| \leq \sqrt{8(1-p_0)}$

Part 1: For any state $|\phi\rangle$, let $|\phi'\rangle$ be the result of measuring some qubit, conditioned on the outcome being 1. Let q be the probability of outputting 1. Then $|\,|\phi\rangle - |\phi'\rangle\,| \leq \sqrt{2(1-q)}$

Part 2: Fix any states $|\tau\rangle, |\tau'\rangle$ such that $|\,|\tau\rangle - |\tau'\rangle\,| \leq \epsilon$. Let r, r' be the probabilities that measuring some qubit of $|\tau\rangle, |\tau'\rangle$ gives 1. Then $|r - r'| \leq 2\epsilon$

Proof of Lemma: Recall two computations

(1) $|\psi\rangle \to T \to V \to M_1$ and (2) $|\psi\rangle \to T \to U \to M_0 \to U^\dagger \to V \to M_1$

Let p_1 be probability M_1 outputs 1 in (1)
Let p_0 be probability M_0 outputs 1 in (2)
Let p_1' be probability M_1 outputs 1 in (2), conditioned on M_0 outputting 1

Proof of Lemma: Recall two computations

(1) $|\psi\rangle \to T \to V \to M_1$ and (2) $|\psi\rangle \to T \to U \to M_0 \to U^\dagger \to V \to M_1$

Let p_1 be probability M_1 outputs 1 in (1)

Let p_0 be probability M_0 outputs 1 in (2)

Let p_1' be probability M_1 outputs 1 in (2), conditioned on M_0 outputting 1

Invoke Part 1 on $|\phi\rangle = UT|\psi\rangle$, let $|\phi'\rangle$ be conditioned on M_0 giving 1 $\Longrightarrow$ $|\ |\phi\rangle - |\phi'\rangle\ | \leq \sqrt{2(1-p_0)}$

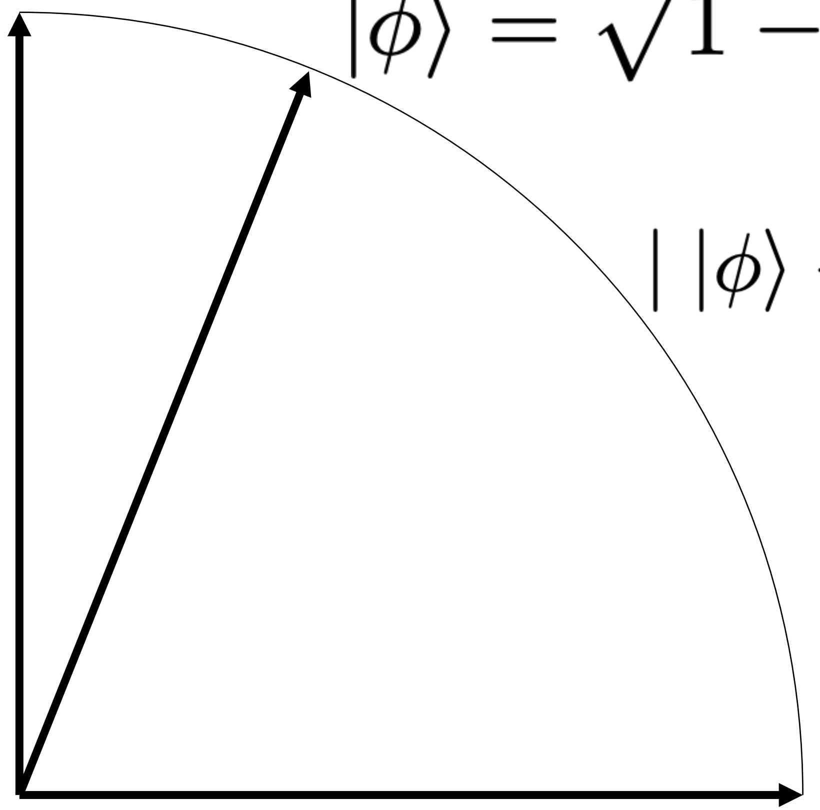
$\Longrightarrow$ $|\ VU^\dagger|\phi\rangle - VU^\dagger|\phi'\rangle\ | \leq \sqrt{2(1-p_0)}$

Invoke Part 2 $\Longrightarrow$ $|p_1 - p_1'| \leq \sqrt{8(1-p_0)}$

Part 1: For any state $|\phi\rangle$, let $|\phi'\rangle$ be the result of measuring some qubit, conditioned on the outcome being 1. Let q be the probability of outputting 1. Then $|\, |\phi\rangle - |\phi'\rangle \,| \leq \sqrt{2(1-q)}$

$|1\rangle = |\phi'\rangle$

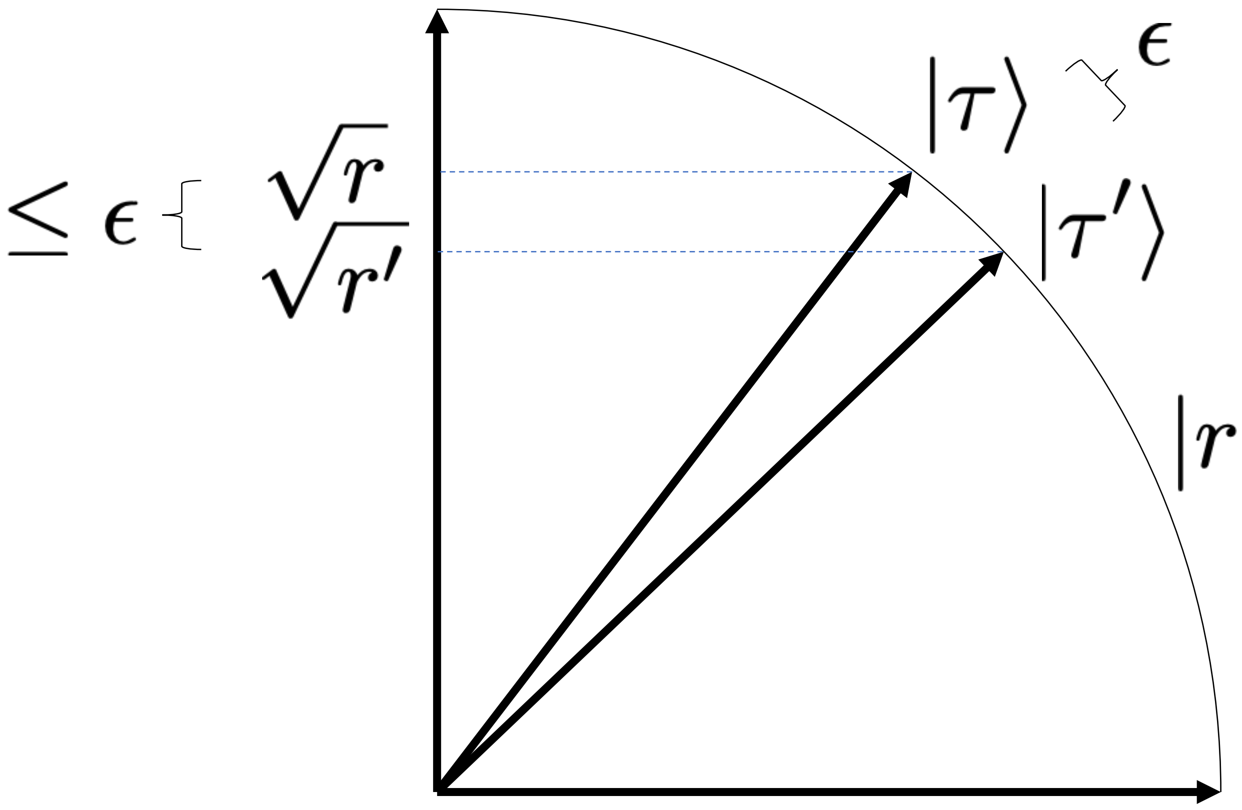
$$|\phi\rangle = \sqrt{1-q}e^{i\theta}|0\rangle + \sqrt{q}e^{i\zeta}|1\rangle$$



$$\begin{aligned} |\, |\phi\rangle - |\phi'\rangle \,|^2 &= (1-q) + (1-\sqrt{q})^2 \\ &= (1-q) + 1 + q - 2\sqrt{q} \\ &= 2 - 2\sqrt{q} \\ &\leq 2 - 2q \end{aligned}$$

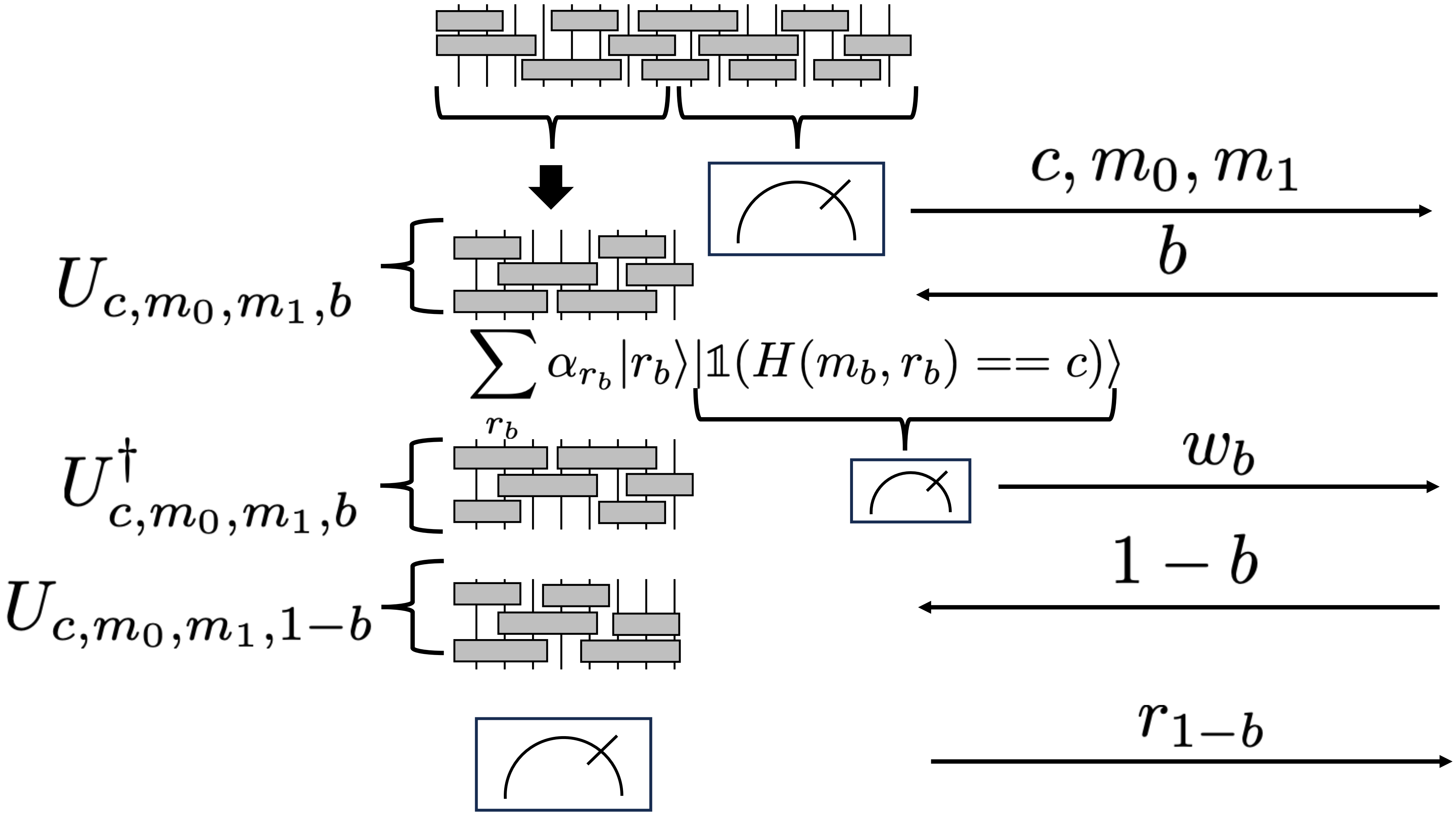
$|0\rangle$

Part 2: Fix any states $|\tau\rangle, |\tau'\rangle$ such that $|\,|\tau\rangle - |\tau'\rangle\,| \leq \epsilon$. Let r, r' be the probabilities that measuring some qubit of $|\tau\rangle, |\tau'\rangle$ gives 1. Then $|r - r'| \leq 2\epsilon$



$$
\begin{aligned}
|r - r'| &= |\sqrt{r}^2 - \sqrt{r'}^2| \\
&= (\sqrt{r} + \sqrt{r'})|\sqrt{r} - \sqrt{r'}| \\
&\leq (1+1)\epsilon = 2\epsilon
\end{aligned}
$$

Going back to our setup



Recall: Let $\Pr[W_b|c]$ be the probability conditioned on $\mathcal{A}$ producing a particular commitment c

Then for particular c, $\Pr[w_b = 1] = \Pr[W_b|c]$

Suppose we are given that $\Pr[W_0|c], \Pr[W_1|c] \geq 9/10$

By Gentle Measurement,

$$\Pr[H(m_{1-b}, r_{1-b}) = c | w_b = 1] \geq 9/10 - \sqrt{8(1 - 9/10)} \geq 5/1000$$

Under our assumption of a really good adversary, we can at least guarantee that it produces a superposition over good r_b, and then later produces a good r_{1-b}

But by the time it gets r_{1-b}, the prior r_b may be gone

Def: A hash function H is **collapsing** if, for all QPT adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr$$

Internal state of adversary

where $W_b(\lambda)$ is the event that $\mathcal{A}$ output

- $\mathcal{A}$ produces a superposition $\sum_{x,z} \alpha_{x,z} |x, z\rangle$
- If $b = 1$, measure x; if $b = 0$ measure $H(x)$
- Return state of $\mathcal{A}$, which outputs a bit b'

$$\sum_{x,z} \alpha_{x,z} |x, z\rangle \mapsto \sum_{x,z} \alpha_{x,z} |x, z, H(x)\rangle$$

Then measure and discard last register

Def: A hash function H is **collapsing** if, for all QPT adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that $\mathcal{A}$ outputs 1 in the following:

- $\mathcal{A}$ produces a superposition $\sum_{x,z} \alpha_{x,z}|x,z\rangle$
- If $b=1$, measure x; if $b=0$ measure $H(x)$
- Return state of $\mathcal{A}$, which outputs a bit b'

Because hash functions take big inputs to small outputs, measuring $H(x)$ does not fully collapse x. Nevertheless, it "looks like" it does

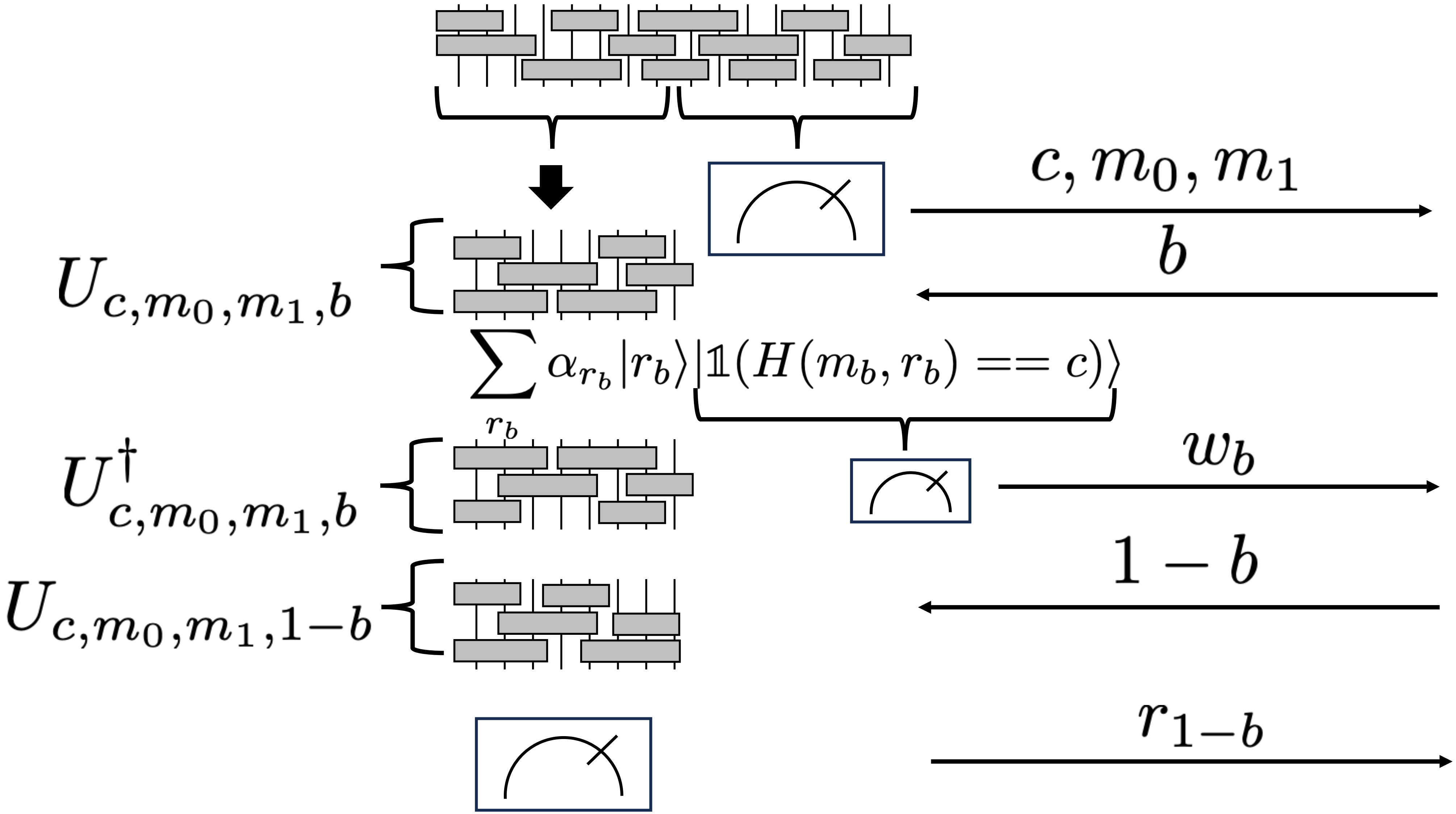
Intuition for collision resistance: even though hash function is many-to-1, it “behaves like” it is injective

One thing injective functions have is that it is impossible to find collisions

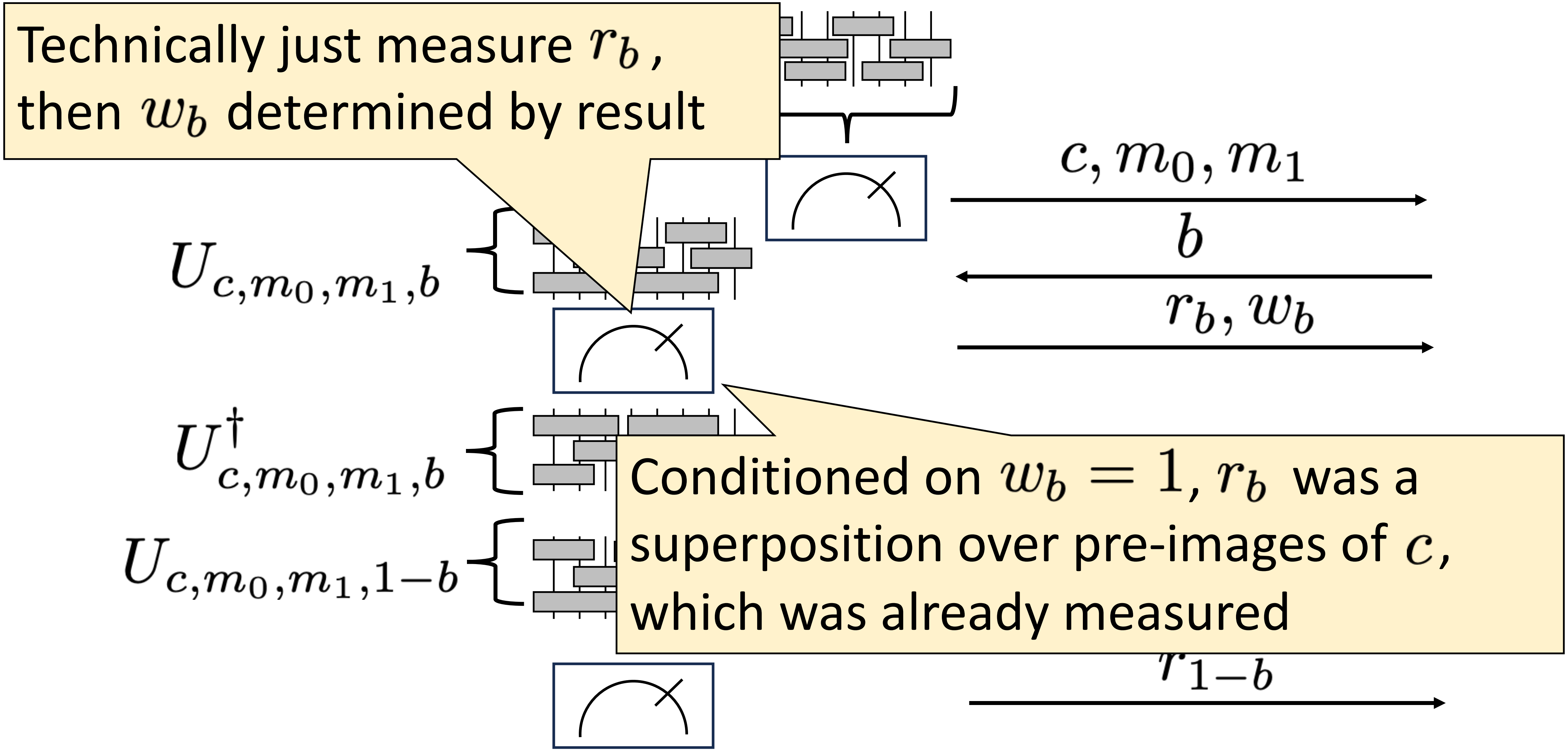
Same intuition for collapsing hash functions, but observe that in a quantum world, there are tasks that do not directly involve finding collisions

For an injective function, measuring output same as measuring input

Going back to our setup



Indistinguishable by collapsing



Just measure w_b :

$$\Pr[w_b = 1|c] \geq 9/10$$
$$\Pr[H(m_{1-b}, r_{1-b}) = c|w_b = 1] \geq 5/1000$$

Measure r_b :

$$\Pr[H(m_b, r_b) = c] = \Pr[w_b = 1|c] \geq 9/10$$
$$\Pr[H(m_{1-b}, r_{1-b}) = c|w_b = 1] \geq 5/1000 - \epsilon$$
$$\Pr[H(m_{1-b}, r_{1-b}) = c = H(m_b, r_b)] \geq (5/1000 - \epsilon) \times 9/10$$

Our proof only worked when

$$\Pr[W_0|c], \Pr[W_1|c] \geq 9/10$$

With a more cleaver proof, possible to show that collapsing implies sum-binding in full generality

Collapsing Hashes from LWE

SIS hash function:

$$f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$$
$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \bmod q$$

Thm: Assuming (quantum) LWE, SIS is collapsing

Thm: Assuming (quantum) LWE, SIS is collapsing

Proof idea: choose many random vectors

$$\mathbf{u}_i \leftarrow \mathbb{Z}_q^m$$

Define event V_i: measure $\mathbf{A} \cdot \mathbf{x} \bmod q$ as well as $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ for $j = 1, \cdots, i$

Notice $V_0 = W_0$, $V_{O(m)} = W_1$ since no collisions in measurement

Thm: Assuming (quantum) LWE, SIS is collapsing

Proof idea: Must show that $|\Pr[V_i] - \Pr[V_{i-1}]|$ is negligible

To do so, show that if already measuring $\mathbf{A} \cdot \mathbf{x} \bmod q$, can measure $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ without detection

Idea: first consider case $\mathbf{u}_i = \mathbf{A}^T \mathbf{s} + \mathbf{e} \bmod q$

$$\lfloor (\mathbf{s}^T \mathbf{A} + \mathbf{e}^T) \cdot \mathbf{x} \bmod q \rceil_{q/4}$$

$$= \lfloor \mathbf{s}^T \mathbf{A} \mathbf{x} + \mathbf{e}^T \mathbf{x} \bmod q \rceil_{q/4}$$

$$\approx \lfloor \mathbf{s}^T \mathbf{A} \mathbf{x} \bmod q \rceil_{q/4}$$

Solely a function of SIS hash output

Thm: Assuming (quantum) LWE, SIS is collapsing

Proof idea: Must show that $|\Pr[V_i] - \Pr[V_{i+1}]|$ is negligible

To do so, show that if already measuring $\mathbf{A} \cdot \mathbf{x} \bmod q$, can measure $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ without detection

Idea: first consider case $\mathbf{u}_i = \mathbf{A}^T\mathbf{s} + \mathbf{e} \bmod q$

⇒ Measuring $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ causes no change

Thm: Assuming (quantum) LWE, SIS is collapsing

Proof idea: Must show that $|\Pr[V_i] - \Pr[V_{i+1}]|$ is negligible

To do so, show that if already measuring $\mathbf{A} \cdot \mathbf{x} \bmod q$, can measure $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ without detection

Thus, if measuring $\lfloor \mathbf{u}_i^T \cdot \mathbf{x} \bmod q \rceil_{q/4}$ for uniform $\mathbf{u}_i$ was detectable, we would distinguish uniform from LWE sample (i.e. break decision LWE)

Annoying issue:

$$\begin{aligned} &\lfloor (\mathbf{s}^T\mathbf{A} + \mathbf{e}^T) \cdot \mathbf{x} \bmod q \rceil_{q/4} \\ &= \lfloor \mathbf{s}^T\mathbf{A}\mathbf{x} + \mathbf{e}^T\mathbf{x} \bmod q \rceil_{q/4} \\ &\approx \lfloor \mathbf{s}^T\mathbf{A}\mathbf{x} \bmod q \rceil_{q/4} \end{aligned}$$

Does not actually perfectly erase error. Need a more sophisticated proof to get full reduction to work

Next time: Another place where classical proofs break:
The Quantum Random Oracle Model