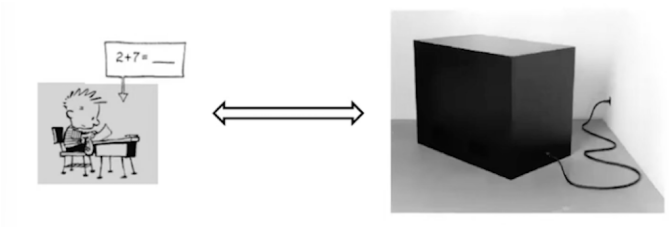
Using Post-Quantum Crypto to Level the Playing Field for Quantumness Test

Essential Steps (Brakerski–Christiano–Mahadev–Vazirani–Vidick)

Quantum computers aren't all-powerful

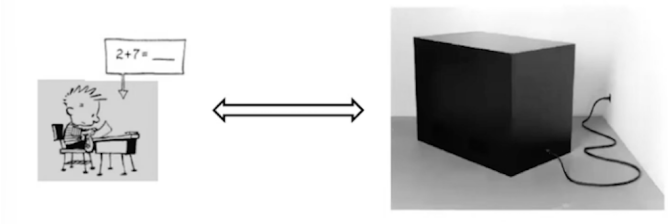


Post-quantum cryptography: there are classical cryptosystems that even quantum computers (believed) cannot break.

Example driver: NIST PQC standardization.

Implication (informal): armed with the *secret key*, the verifier can efficiently compute facts that the quantum device cannot compute from public information alone.

Use post-quantum crypto to level the playing field



Wrong way: cripple the quantum computer by forcing it to play only on the classical verifier's turf (tasks where quantum brings no leverage).

Right way: make the quantum computer play on turf where

- the verifier has a *cryptographic advantage* (trapdoor knowledge),
- but the quantum computer can still exercise its *unique capability* (superposition / interference),
- yielding an experimentally checkable separation.

One function f with two branches (trapdoor claw-free)

We use a **single public function** with a hidden branch bit:

$$f : \{0,1\} \times \mathcal{X} \to \mathcal{Y}, \qquad y = f(b, x).$$

For a typical output $y \in \mathcal{Y}$ there are **two preimages**

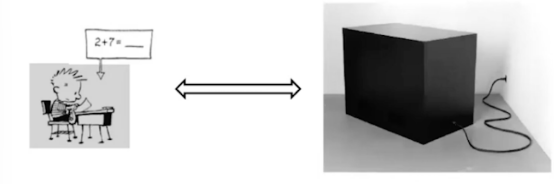
$$y = f(0, x_0) = f(1, x_1) \quad (\text{a } \textit{claw}).$$

Trapdoor claw-free property:

- Easy to evaluate $f(b, x)$.
- Hard (for any PPT adversary) to find a claw (x_0, x_1) with $f(0, x_0) = f(1, x_1)$.
- With secret trapdoor td, verifier can invert: given y, recover (x_0, x_1).

Instantiation: lattice-based (LWE) constructions (informal: $y = As + e$ is hard to invert without trapdoor).

What the verifier knows vs what the device knows



Verifier (classical):

- holds trapdoor *td*
- given y, can compute (x_0, x_1)
- can therefore check consistency of answers

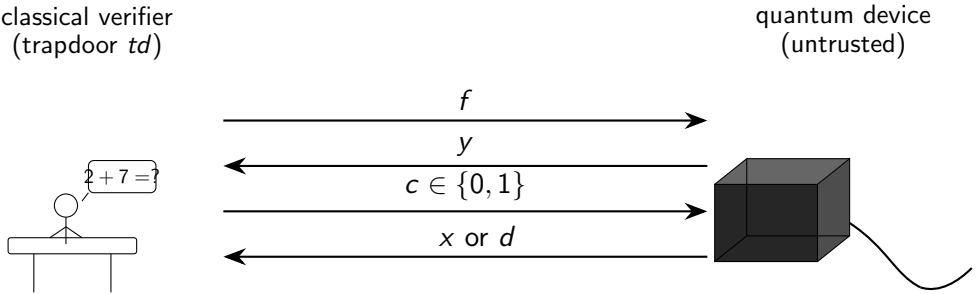
Quantum device (untrusted):

- knows only public description of f
- can create superpositions over preimages
- but cannot classically "solve" for both x_0, x_1

Quantum capability (key move): prepare (implicitly) a state correlated with a claw:

$$|\psi_y\rangle = \frac{1}{\sqrt{2}}\big(|0, x_0\rangle + |1, x_1\rangle\big) \quad \text{where } f(0, x_0) = f(1, x_1) = y.$$

Outline of the challenge–response protocol



Challenge bit c:

- $c = 0$ (preimage challenge): return x such that $f(b, x) = y$ for some b.
- $c = 1$ ("Hadamard / phase" challenge): return a string d satisfying

$$d \cdot (x_0 \oplus x_1) = 0 \pmod 2,$$

where (x_0, x_1) are the two preimages of y.

Quantum advantage: answer either challenge

From the correlated (implicit) state

$$|\psi_y\rangle = \frac{1}{\sqrt{2}}\big(|0, x_0\rangle + |1, x_1\rangle\big),$$

the device can respond as follows.

If $c = 0$ (preimage): measure in computational basis $\Rightarrow$ output (b, x_b), hence a valid preimage $x = x_b$.

If $c = 1$ (Hadamard / phase): apply Hadamard on the branch register (and appropriate transforms) and measure to obtain d that is (approximately) orthogonal to $x_0 \oplus x_1$ (see Simon's algorithm):

$$d \cdot (x_0 \oplus x_1) = 0 \pmod 2.$$

Message: quantum interference lets the device extract a global relation involving *both* preimages.

Why a classical device cannot pass (rewinding intuition)

Soundness intuition: no PPT classical prover can answer both challenges for the same y.

Suppose a classical prover could:

- answer $c = 0$ giving a valid preimage x_b, and
- answer $c = 1$ giving a valid d correlated with $x_0 \oplus x_1$.

Then a **rewinding** extractor can run the prover twice (same randomness, two challenges) and combine transcripts to recover a claw (x_0, x_1), contradicting claw-freeness.

Technical backbone: adaptive hardcore bit. Given one preimage and any side-information d, predicting

$$d \cdot (x_0 \oplus x_1)$$

with non-negligible bias would yield an efficient claw-finding algorithm.

Therefore, passing the test is evidence of *quantumness* (under LWE/PQC assumptions).

Takeaway: cryptographic quantumness test

- Post-quantum crypto gives the verifier leverage (trapdoor inversion).
- The quantum device's leverage is superposition/interference over two preimages.
- A single challenge–response protocol distinguishes quantum from classical, assuming LWE-based trapdoor claw-free security.
- Extensions yield **certifiable randomness** from a single device.

(This slide deck intentionally mirrors the "kid vs black box" narrative: the verifier is simple, the device is opaque, crypto forces honest structure.)