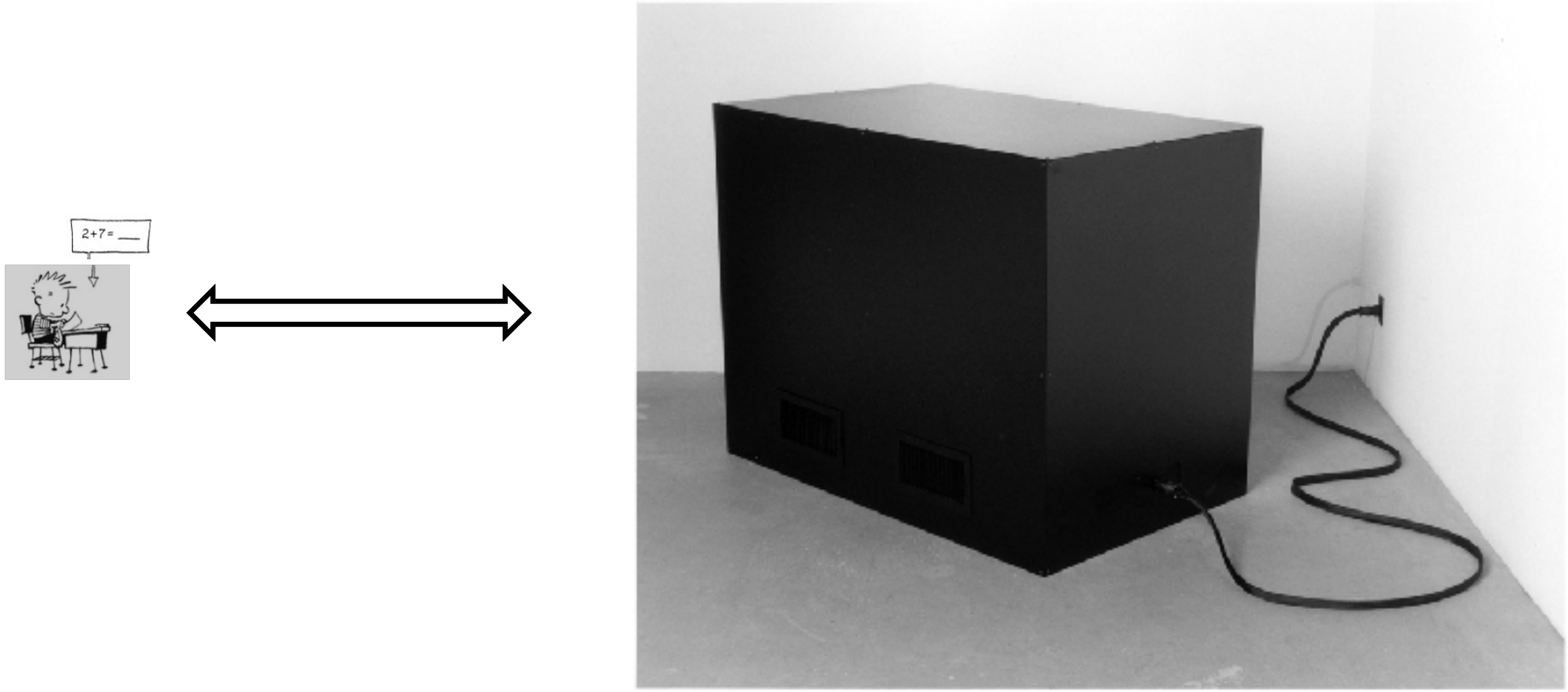
A cryptographic leash for quantum computers: classical proofs of quantumness

Umesh V. Vazirani

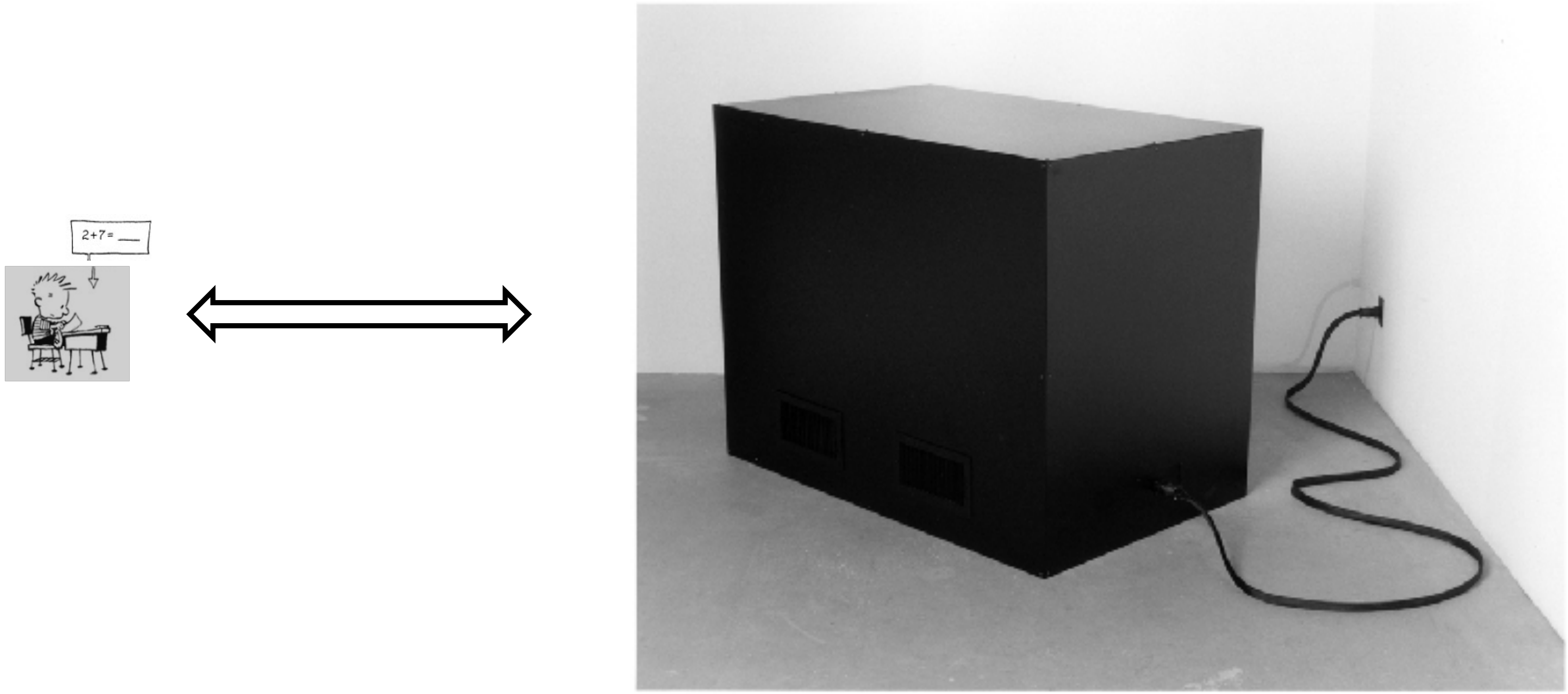
U. C. Berkeley

Verification and Validation of Quantum Computers



- Hilbert space is exponentially large
- Exponential power of quantum computer

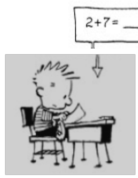
Verification and Validation of Quantum Computers

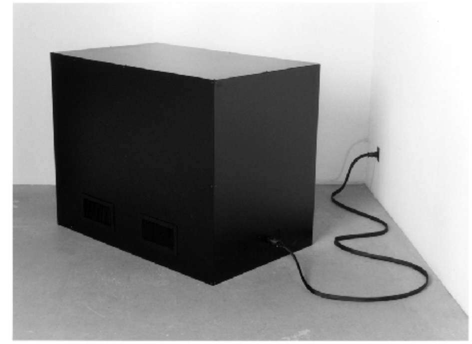


Enforce qubit structure on prover’s Hilbert space

Enforce initial state + X & Z operators on qubits

Cryptographic leash for Quantum Computers



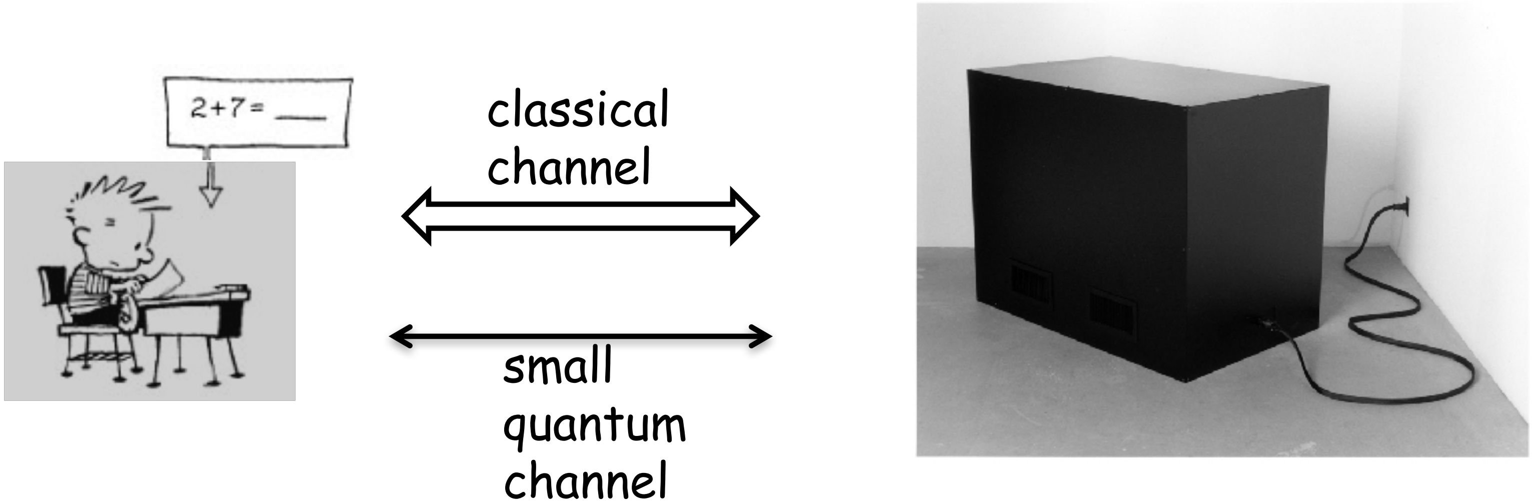


Post-quantum cryptography: there are classical cryptosystems that even quantum computers cannot break. NIST challenge

i.e. armed with the secret key, classical Verifier can decrypt messages that a quantum computer can't

- Proof of quantumness
- Certifiable randomness
- Verification of quantum computation
- Fully homomorphic quantum computation
- Device independent quantum key distribution from computational assumptions

Mildly Quantum Verifier



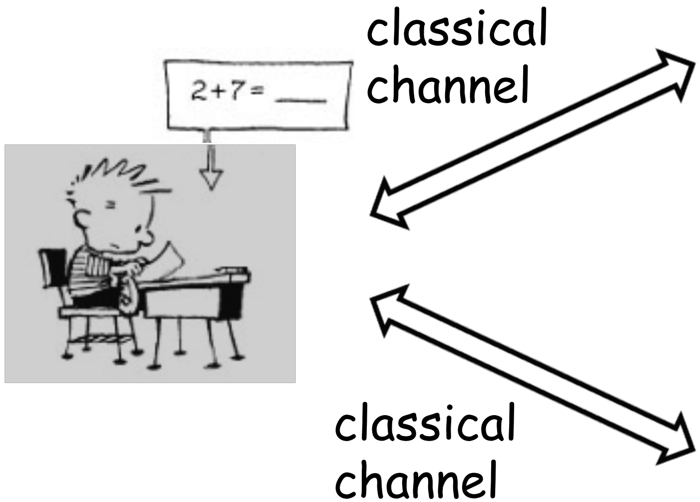
Verifier has constant # bits of quantum storage + quantum channel to Prover.

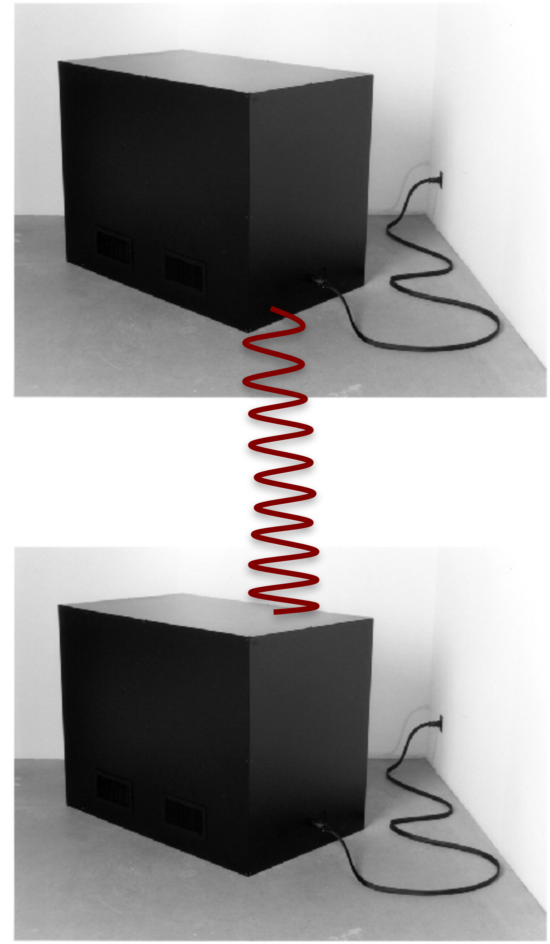
Idea: randomize qubits so quantum computer performs its computation “under the covers” & test: $X^r Z^s|\psi>$

[Aharonov, Ben-Or, Eban ‘09]

[Broadbent, Fitzsimons, Kashefi ’09]

Classical Verifier & entangled quantum provers: Classical Leash

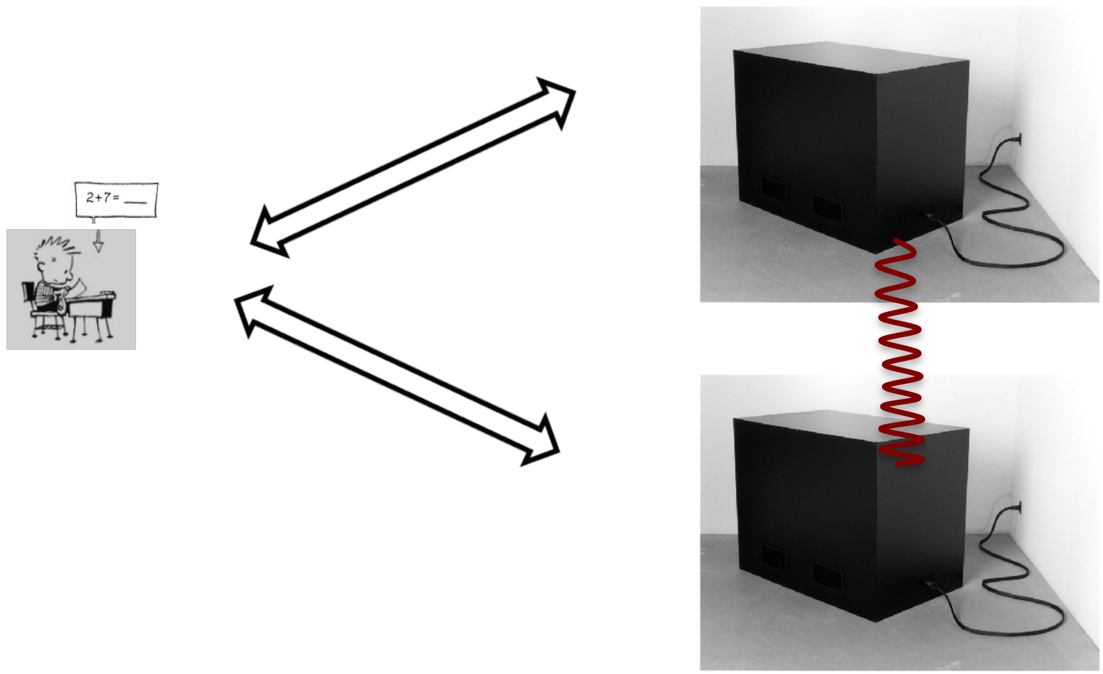




Use properties of entanglement to enforce qubit structure, initial state + X & Z operators

Reichardt, Unger, V. *Nature* **496**, 456–460 (25 April 2013)

Classical Verifier & entangled quantum provers: Classical Leash



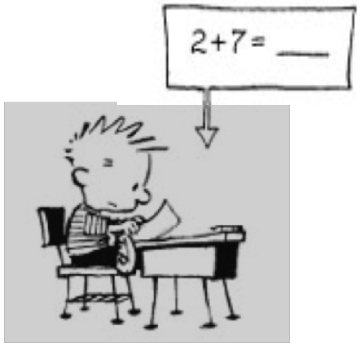
- Reichardt, Unger, V 2013: poly(n) CHSH tests to enforce n qubits
- Natarajan & Vidick 2018: quantum low degree tests – poly-log n CHSH (or magic square) tests, poly-log n communication
- Ji, Natarajan, Vidick, Wright, Yuen 2020: MIP*=RE

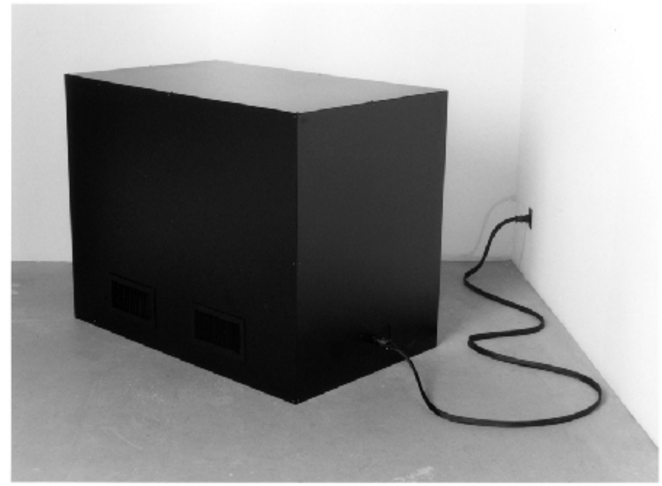
Outline

- Qubit certification protocol based on trapdoor claw-free functions (TCF)
- TCF with adaptive hardcore bit based on LWE
- Proof of quantumness
- Enforcing a qubit (Jordan’s lemma)
- Randomness protocol
- Verification of quantum computation
- Efficient randomness protocol
- Proof of quantumness without adaptive hardcore bit

Qubit Certification Protocol

[Brakerski, Christiano, Mahadev, V, Vidick 2018]



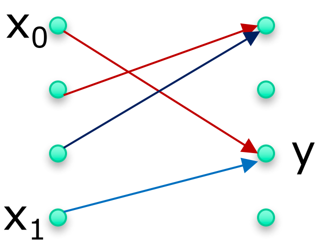


$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{(-1)^c}{\sqrt{2}}\,|1\rangle$$

Uses knowledge of secret key to figure out c

Knows only encryption of c

Trapdoor claw-free functions

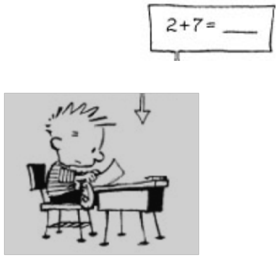


Pair of functions $f_0, f_1: \{0,1\}^n \rightarrow \{0,1\}^m$

- Injective, same image
- Hard to find claw (x_0,x_1,y): $f_0(x_0) = f_1(x_1) = y$
- With knowledge of trapdoor, can invert:

  given y can find x_0,x_1: $f_0(x_0) = f_1(x_1) = y$

Qubit Certification Protocol

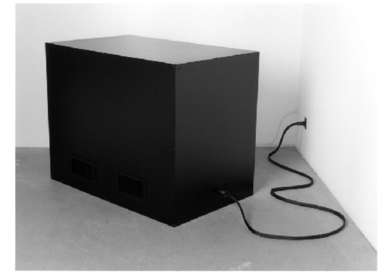


f →

y ←

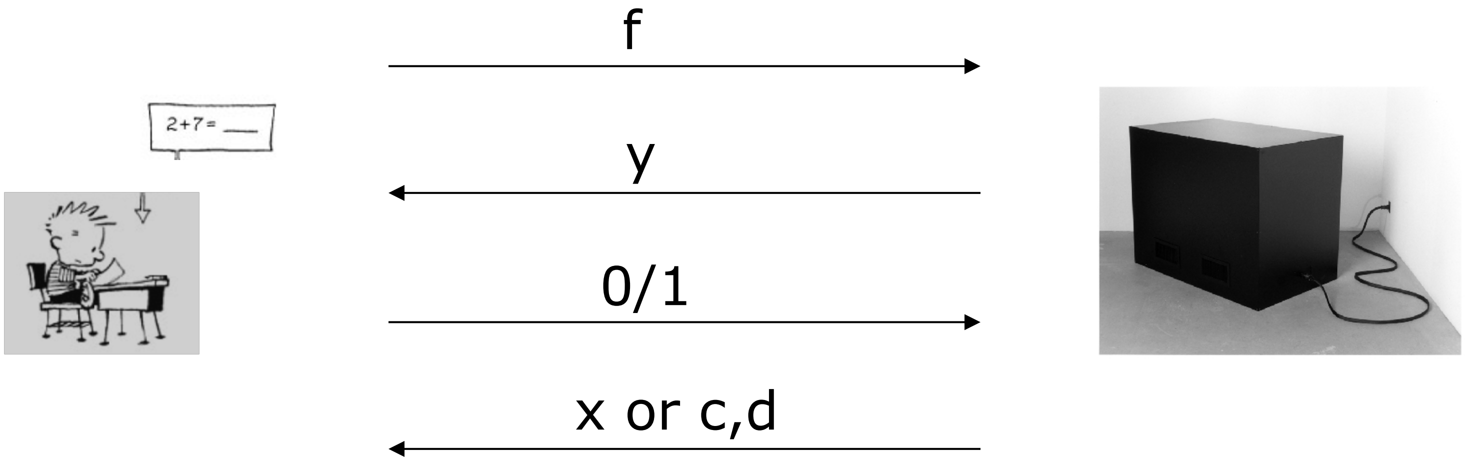
0/1 →

x or c,d ←



- Prover creates superposition $\sum_x |0\rangle|x\rangle\,|f_0(x)\rangle + |1\rangle|x\rangle|f_1(x)\rangle$
- Prover measures 3rd register to get: $(|0\rangle|x_0\rangle + |1\rangle|x_1\rangle)\;|y\rangle$
- If challenge = 0, prover measures in standard basis
- If challenge = 1, measures 2nd register in Hadamard basis: Measurement outcome = d. New state = $|0\rangle + (-1)^c\,|1\rangle$ where c=d(x_0+x_1). Measure 1st register to get c.

Proof of Quantumness



- Quantum computer can answer either challenge
- No polynomial time classical or quantum (!) computer can answer both challenges. i.e. x and c,d
- Classical prover can be rewound. So if it can answer either challenge, it can answer both!

Proof of Quantumness

For a classical computer to succeed it must provide:
a preimage x and c,d: $d(x_0 + x_1)=c$

Based on strong new kind of hard core bit property – adaptive hard core bit:

For trapdoor claw-free function based on LWE: knowledge of a preimage x, and a better than 50-50 guess for $d(x_0+x_1)$ for **any** choice of d ➔ an efficient algorithm to find claw and therefore break LWE.

Adversary gets to choose d = which bit is hard core after seeing particular TCF f_0 & f_1 chosen by verifier & y

Proof heavily leverages a technique for LWE called leakage resilience.

LWE (Learning with errors)

random matrix $A \in \mathbb{Z}_q^{m \times n}$, $s \in \mathbb{Z}_q^n$

noise vector $e \in \mathbb{Z}_q^m$ from suitable Gaussian distr.

$$t = As + e$$

$$\begin{array}{cc} & n \\ m & \begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} \end{array} \begin{bmatrix} s \end{bmatrix} + \begin{bmatrix} \\ e \\ \\ \end{bmatrix} = \begin{bmatrix} \\ t \\ \\ \end{bmatrix}$$

LWE assumption: distribution over (A, t) is computationally indistinguishable from (A, u) for uniform $u \in_R \mathbb{Z}_q^m$

TCF from LWE.

Fix LWE sample $(A, t) = (A, As+e)$

$$f_0(x) = Ax + e_0$$
$$f_1(x) = Ax + e_0 + t$$

Two Issues:

1) Output is a distribution – call it (noisy) NTCF
2) If $e = 0$ then $f_1(x) = A(x+s) + e_0$

so $f_1(x) = f_0(x+s)$

But $e \neq 0$.

Solution: sample e_0 from much wider Gaussian than e, so that distributions for $f_0(x+s)$ and $f_1(x)$ essentially indistinguishable

Claw-free: $x_0 - x_1 = s$

Using NTCF to create superposition

LWE sample: $t = As + e$

$$\sum_{x \in \mathbb{Z}_q^n} |0\rangle|x\rangle + |1\rangle|x\rangle$$

$$\Big\downarrow \text{compute } f$$

$$\sum_{x \in \mathbb{Z}_q^n} \sum_{e_0 \in \mathbb{Z}_q^m} |0\rangle|x\rangle|Ax + e_0\rangle + |1\rangle|x\rangle|Ax + e_0 + t\rangle$$

Measure 3rd register: $\frac{1}{\sqrt{2}}|0\rangle|x_0\rangle + \frac{1}{\sqrt{2}}|1, x_0 - s\rangle$

Note: all entries are in $\mathbb{Z}_q$.

Use $\log q$ qubits to represent each entry.

Adaptive Hardcore Bit

$\boxed{t = As + e}$

Knowledge of preimage $\overset{x_0 \text{ or } x_1}{\overset{\shortparallel}{x}}$ & better than 50-50 guess for $d(x_0 + x_1)$ for any choice of d
$\Rightarrow$ efficient algorithm to break LWE.

$x_1 = x_0 - s$ does not mean $d(x_0 + x_1) = d \cdot s$ } Binary vs mod q.

Since we know a preimage, say x_0, can use it to efficiently compute d' : $d' \cdot s = d(x_0 + x_1)$.

So want to show $d' \cdot s$ hardcore bit for LWE.

Adaptive Hardcore Bit

$d' \cdot s$ is hardcore bit for LWE $\quad t = As + e$

for d' that might be chosen based on t.

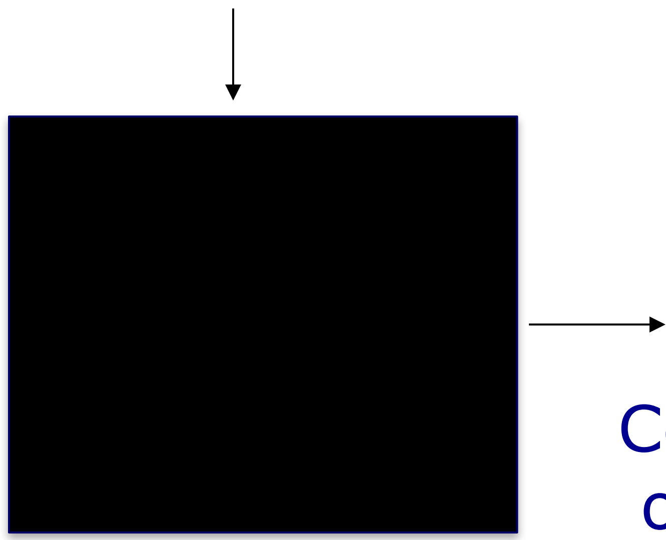
Use leakage resilience: $\quad A$ indist $BC + E$

By leftover hash lemma, even given Cs, any bit of s close to uniform.

Exploit binary nature of d' + fourier analytic argument to prove adaptive hardcore bit.

Certifiable Quantum Random Number Generator

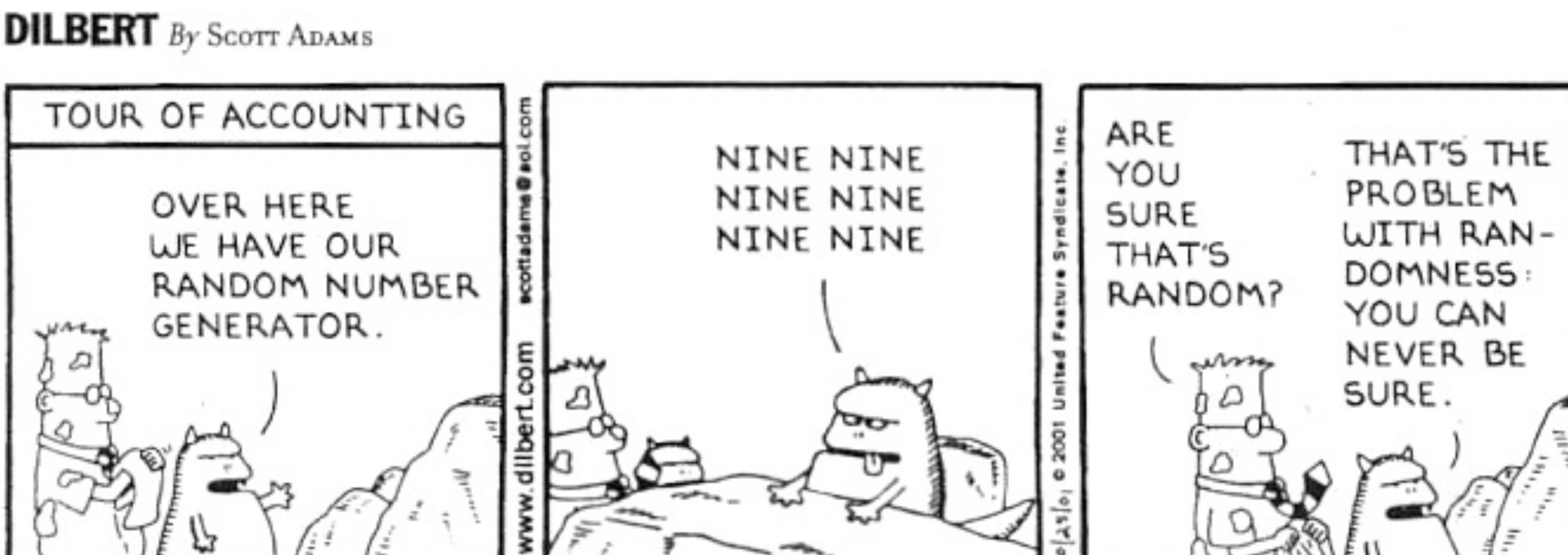
log n random bits



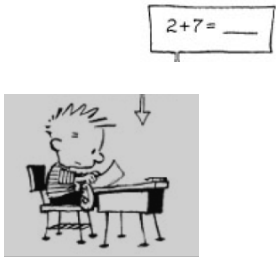
n bits

110100010111...

Certifies that this particular output string is random!!



Certifiable random numbers

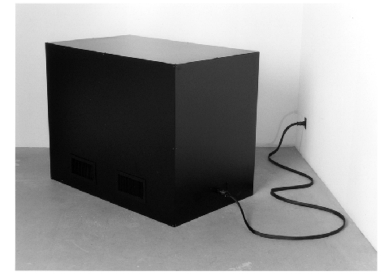


f

y

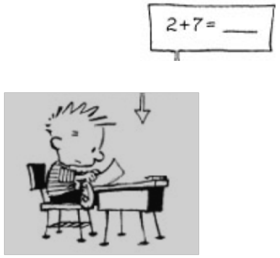
0/1

x_0 or x_1 / d: $d(x_0+x_1)=0$



- Choose f pseudorandomly.
  Use 0-challenges to generate randomness
  Use a few 1-challenges to keep device honest

Certifiable random numbers

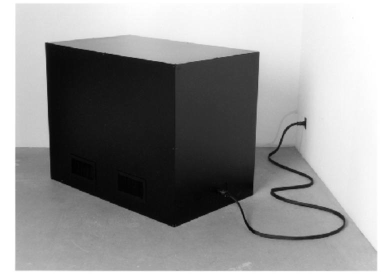


f

y

0/1

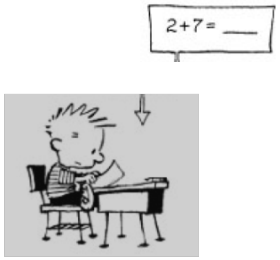
x_0 or x_1 / d: $d(x_0+x_1)=0$



- Choose f pseudorandomly.
  Use 0-challenges to generate randomness
  Use a few 1-challenges to keep device honest

- If the prover is unable to break cryptography during the protocol, then this must produce statistical randomness, not pseudorandomness.

Certifiable random numbers

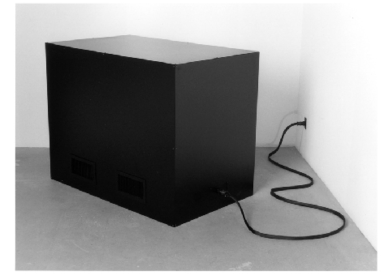


$\xrightarrow{f}$

$\xleftarrow{y}$

$\xrightarrow{0/1}$

$\xleftarrow{x_0 \text{ or } x_1 \;/\; d:\ d(x_0+x_1)=0}$



- Choose f pseudorandomly.
  Use 0-challenges to generate randomness
  Use a few 1-challenges to keep device honest

- Show that quantum device must be effectively measuring a qubit $|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$:

In standard basis if challenge = 0
In Hadamard basis if challenge = 1

Characterizing Prover

- Characterize prover's Hilbert space:
  Prover succeeds ➔ must have a qubit in state |0>, which he measures in standard basis on challenge 1, and Hadamard basis on challenge 0.

- Qubit defined by two anti-commuting measurements i.e. 45 degree.

- Two measurements: $d(x_0+x_1)=0$ or 1
  $x = x_0$ or x_1

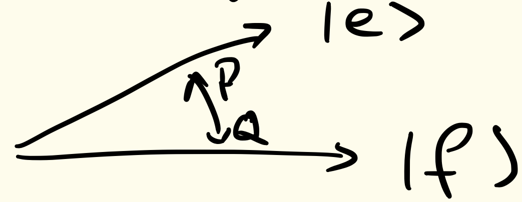
- Hardcore bit property says that the two measurements are almost perfectly uncorrelated.

- Use Jordan's lemma to decompose Hilbert space into direct sum of 2 dim subspaces. Measurements must be 45 degree in most. Now align to get qubit.

Projectors P, Q.

Jordan's Lemma: decompose Hilbert space into direct sum of 2D subspaces, pairing up e-vectors of PQP & QPQ:

$PQP|e\rangle = \lambda|e\rangle$ then $Q|e\rangle = |f\rangle$ is an e-vector of QPQ with evalue λ.



* 2 measurements: $d(x_0+x_1) = 0$ or 1, $x = x_0$ or x_1 define P, Q.
* Adaptive Hardcore bit $\Rightarrow$ measurements almost uncorrelated.

$\Rightarrow$ by ignoring small part of state, most Jordan blocks have Jordan angles $\approx \pi/4$.

* Incur small error to correct all angles to $\pi/4$.
* Align all blocks = global Unitary to define qubit.

Verification of Quantum Computation

[Mahadev 2018]

- Prover creates superposition: $(\alpha|0\rangle|x_0\rangle + \beta|1\rangle|x_1\rangle)$ *and commits* to it by sending image of TCF y.

- The prover is supposed to choose the qubit state to be the ground state of a local Hamiltonian (with only XX, ZZ terms) representing the computation to be performed.

- The verifier chooses to perform either standard basis or Hadamard basis tests.

- The prover cannot control the outcome of the Hadamard basis test, since depends upon $d(x_0 + x_1)$ and prover does not know x_0, x_1 Prover's cheating on Hadamard test equivalent to picking a different superposition to start with.

[Fitzsimmons, Kashefi 2014] had shown that if verifier can force quantum device to prepare one of 8 states, can verify arbitrary quantum computation

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{\omega^{d(x0+x1)}}{\sqrt{2}} |1\rangle$$

[Gheorghiu, Vidick 2019] Use F_8 instead of F_2 for Fourier transform

Use quantum random access codes to prove rigidity.

Proof of Quantumness without Adaptive Hard Core bit

[with Kahanamoku-Meyer, Choi, Yao 2021]

- Modification of the basic protocol to incorporate the CHSH game (Bell test).
- Space-like separation between two players replaced by computational hardness of crypto problem
- Can use x^2 mod N as Trapdoor claw-free function
- Allows discarding of garbage bits without uncomputing
- Proof of concept implementation on Ion Trap QC.

Quantum Advantage From Computational Bell Test

[Kahanamoku-Meyer, Choi, V, Yao 2021].

$$\begin{array}{ccc} \underline{V} & & \underline{P} \\ & \xrightarrow{\quad f \quad} & \\ & \xleftarrow{\quad y. \quad} & |x_0\rangle + |x_1\rangle. \end{array}$$

Ask for preimage **OR**

$$\begin{array}{cc} \xrightarrow{\quad r \in \{0,1\}^n \quad} & |r\cdot x_0\rangle \underbrace{|x_0\rangle}_{\text{Hadamard}} + |r\cdot x_1\rangle |x_1\rangle \\ \xleftarrow{\quad d \quad} & |r\cdot x_0\rangle + (-1)^{d\cdot(x_0+x_1)} |r\cdot x_1\rangle \\ \xrightarrow{\quad \pi/8 \text{ or } -\pi/8 \quad} & \\ \xleftarrow{\quad 0/1. \quad} & \end{array}$$

Efficient Certifiable Randomness

[Mahadev, V, Vidick 2021]

* Generate n bits of randomness with a small variant of qubit certification protocol.
* Test that quantum computer has n qubits of memory.
* Use leakage resilience of LWE to choose at $2^k \to 1$ function in place of 2-1 fn.
* Problem: Hadamard test breaks.
* Solution: use lossy matrix for preimage test & indistinguishable LWE matrix for Hadamard test.

To generate randomness: $\tilde{A} = BC + E$.

V $\qquad\qquad\qquad\qquad$ P

$$\xrightarrow{\tilde{A},\ t = \tilde{A}s + e}$$

$$\xleftarrow{\quad y \quad}$$

$$\xrightarrow{\quad 0 \quad}$$

$$\xleftarrow{\quad x \quad}$$

To test:

V $\qquad\qquad\qquad\qquad$ P

$$\xrightarrow{\quad A,\ t \quad}$$

$$\xleftarrow{\quad y \quad}$$

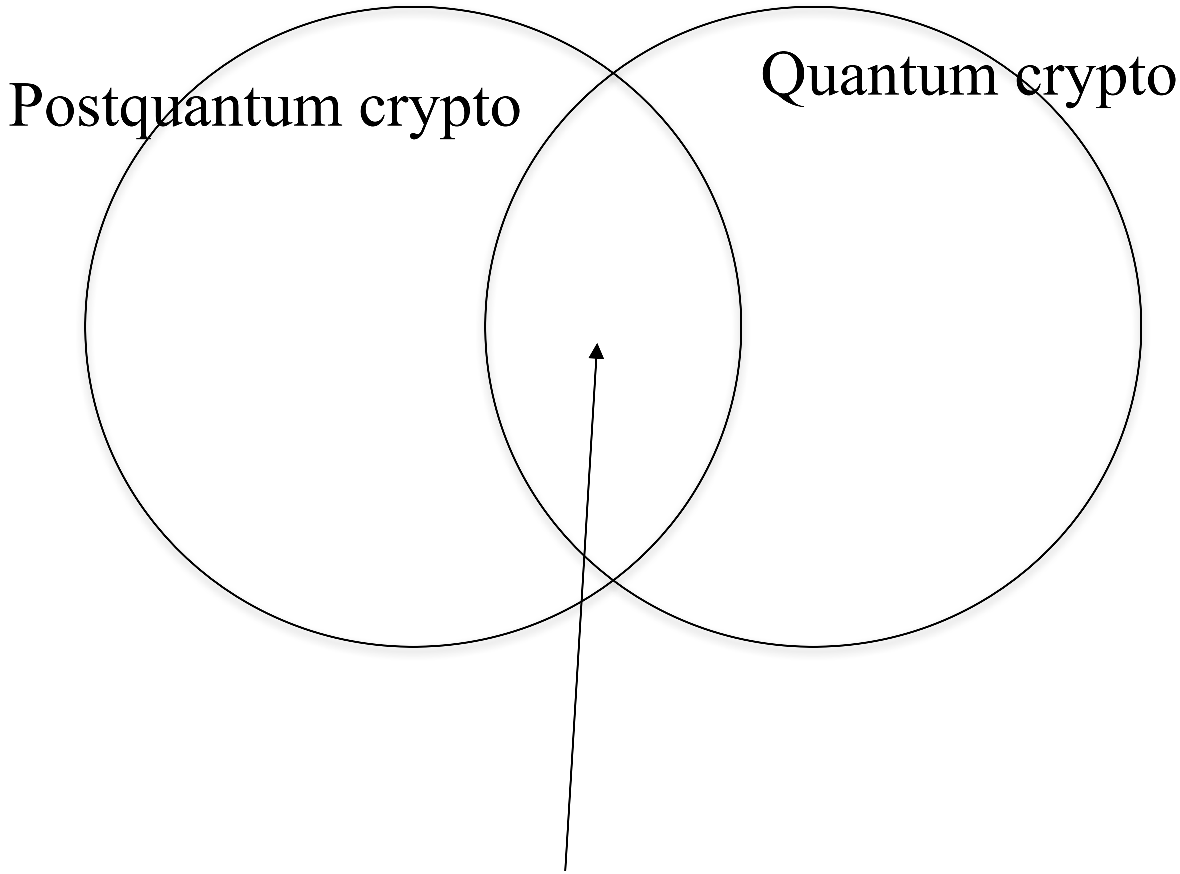
$$\xrightarrow{\quad 1 \quad}$$

$$\xleftarrow{\quad d \quad}$$

check $d(x_0 + x_1) = 0$

Proof tricky since verifier has knowledge of trapdoor, so rules out direct hybrid argument replacing lossy matrix with LWE. Instead use intermediate quantum verifier that does not need trapdoor information.

Discussion



Thank you!