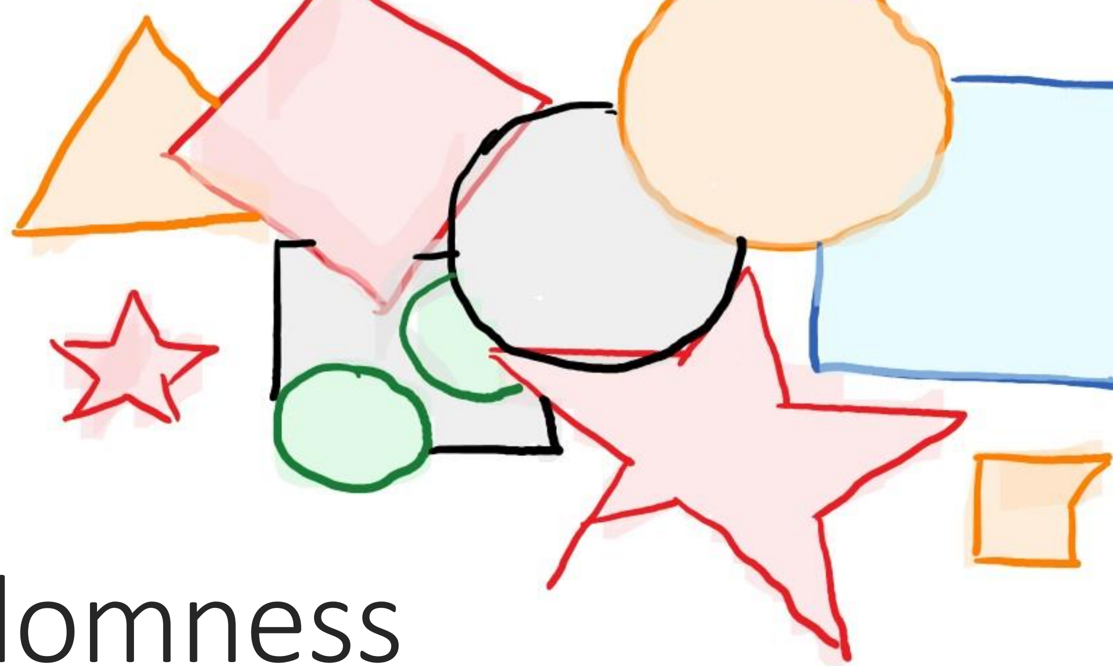


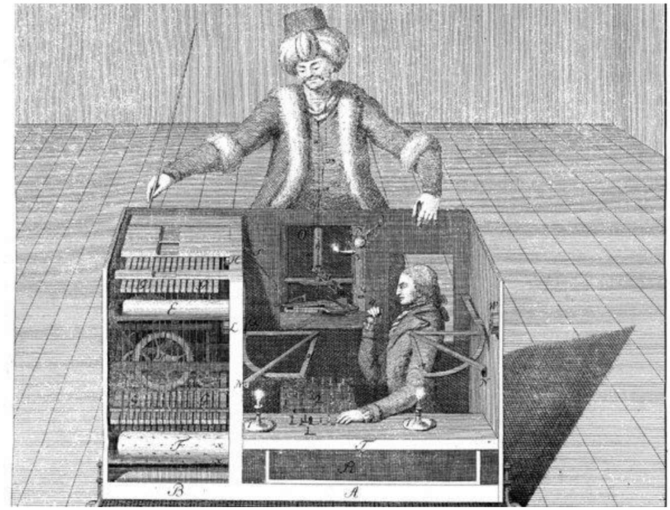
Certifiable randomness from a single quantum device

THOMAS VIDICK

CALIFORNIA INSTITUTE OF TECHNOLOGY

Joint work with Zvika Brakerski (Weizmann), Paul Christiano, Urmila Mahadev, and Umesh Vazirani (UC Berkeley)

Quantum Computing 1.0



- [Wiesner'83,Bennett-Brassard'84] Information-theoretic security in quantum cryptography
- [Shor'94],[Aharonov-Ben-Or,Gottesman,Shor,Preskill '96-97] Fault-tolerant quantum computers can factor in polynomial time
- [Bernstein-Vazirani'97] Quantum computing as a challenge to the efficient Church-Turing thesis

[… 20 years pass …]

Quantum Computing 2.0

- [Preskill'18] The NISQ era
- No fault-tolerance in sight…

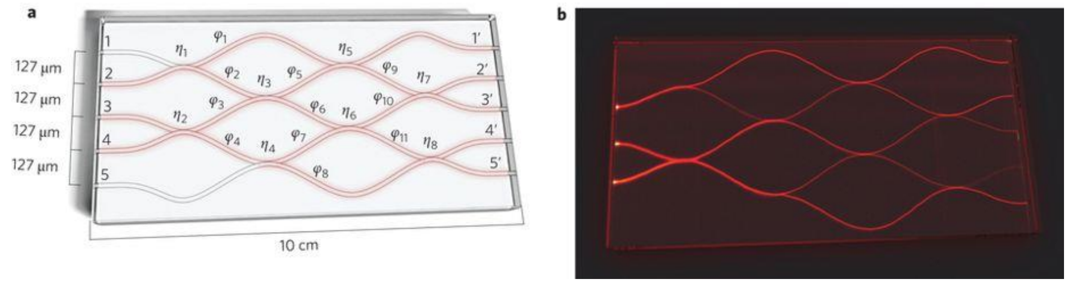
Google 72-qubit "Bristlecone" chip

Demonstrating quantum advantage in the NISQ era

- [Aaronson-Arkhipov'10]
  Boson Sampling

[Bremner-Jozsa-Shepherd'10]
Instantaneous Quantum Computation (IQP)

- [Boixo et al.'16]
  Random quantum circuits



- Artificial tasks designed for 50-60 qubit devices
- Verification does not scale; poor tolerance to errors
- Limited characterization of quantum device

verifiable quantumness ?

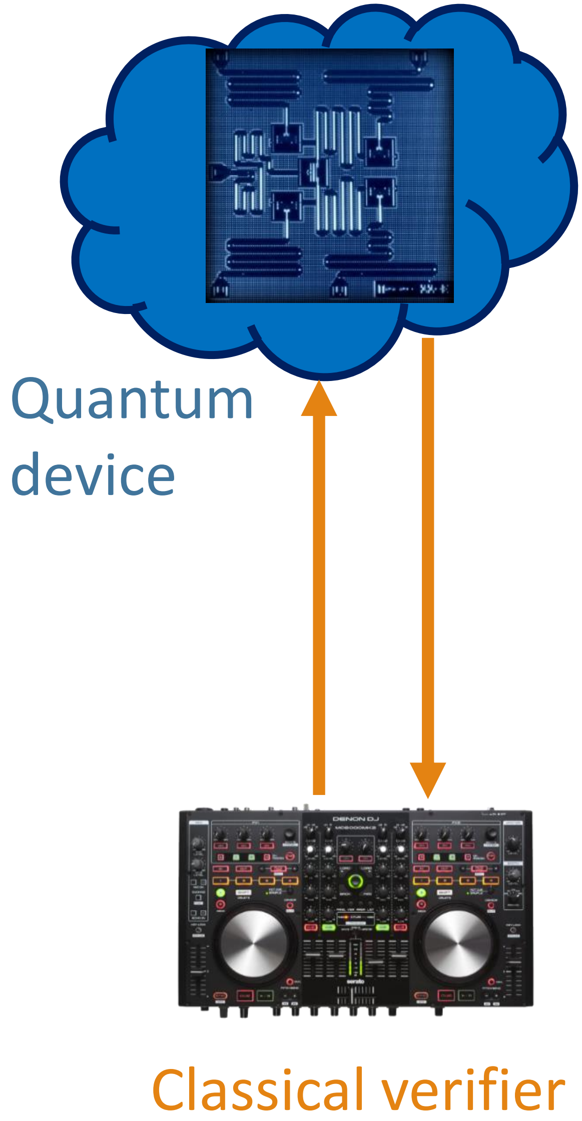
50 noisy qubits:
verified quantum advantage

2000 perfect qubits (× 100 for QEC)
break ECC

A new proposal

- Assumptions:
  - Quantum device is computationally bounded
  - Verifier has trapdoor information for post-quantum secure cryptographic scheme

- Goals:
  - Efficient verification
  - Characterization of device
  - Useful task



Protocol for certifying quantumness

Verifier

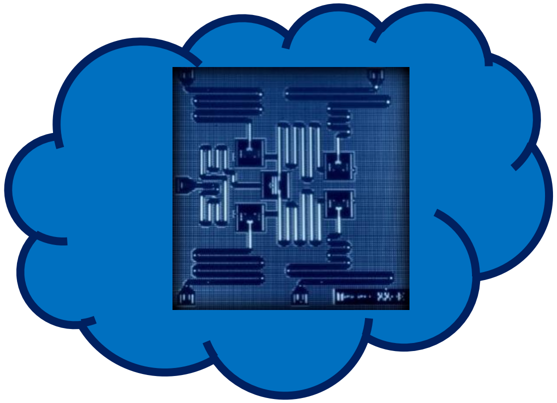
public parameters pk

commitment y

challenge $0/1$

response r_0/r_1

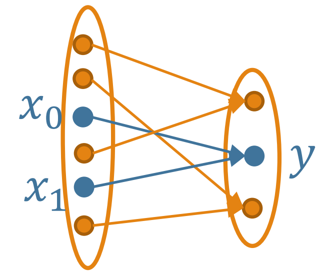
Device



- Verifier uses trapdoor t_k to check device's responses
- Show: No poly-time (classical or quantum) procedure can compute *both* r_0 and r_1
- Conclude: Classical device cannot succeed with probability $\gg \frac{1}{2}$: classical devices can be rewound!
- Protocol *forces* efficient device to implement *collapsing* measurement

Trapdoor claw-free functions

Function $f: \{0,1\}^{n+1} \to \{0,1\}^n$ such that:



- f is two to one
- Hard to find *claws :* pairs (x_0, x_1) s.t. $f(x_0) = f(x_1)$
- Given trapdoor t_k, can invert y and find x_0, x_1 s.t. $f(x_0) = f(x_1) = y$

- Prepare uniform superposition over $|x\rangle$, evaluate f and measure outcome y:

$$\frac{1}{\sqrt{2}}|x_0\rangle + \frac{1}{\sqrt{2}}|x_1\rangle$$

- Measure in computational basis: x_0 or x_1
- Measure in Hadamard basis: d such that $d \cdot (x_0 \oplus x_1) = 0$
- LWE instantiation with hardcore bit property:

hard to find $(x_0$ or $x_1)$ *and* $(d$ s.t. $d \cdot (x_0 \oplus x_1) = 0)$

Protocol for certifying quantumness

Verifier

public parameters pk →

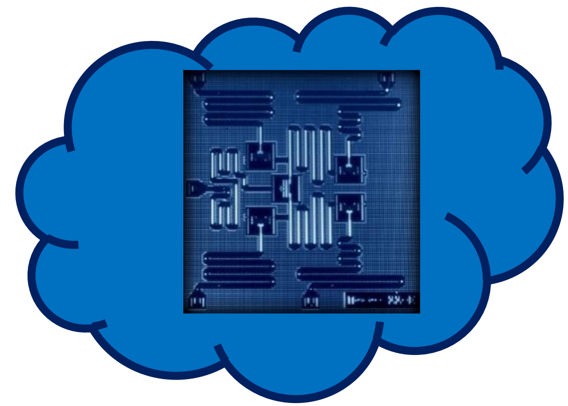
← *commitment* y

challenge $c = 0/1$ →

$c = 0$: x_0 or x_1 ←

$c = 1$: d s.t. $d \cdot (x_0 \oplus x_1) = 0$

Device



- Verifier uses trapdoor t_k to invert y and check answers
- Hardcore bit property: no poly-time device can answer both challenges
- Successful device must be quantum!

Certified randomness expansion

- Quantum devices *can* generate randomness
- Can we *prove* that the outcome is random?

- [Colbeck'09,…] Bell inequality violation certifies generation of randomness
- [MS'15,AFDFRV'18] Violation → mutually unbiased measurements

  → randomness accumulation

Protocol for certified randomness expansion

Verifier

public parameters pk →

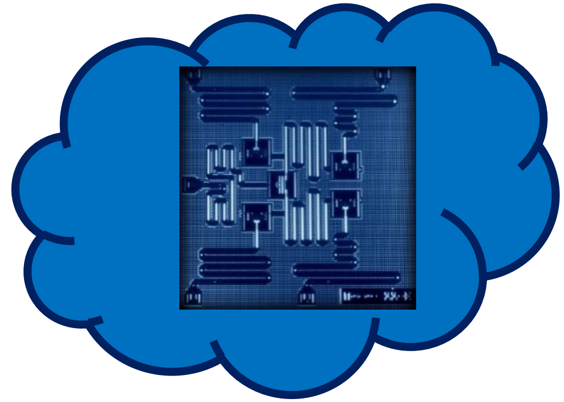
← *commitment* y

challenge $c = 0/1$ →

← $c = 0$: x_0 or x_1

$c = 1$: d s.t. $d \cdot (x_0 \oplus x_1) = 0$

Device



- Verifier and device interact for N rounds:
  - In most rounds, $c = 0$. Verifier records device's choice of pre-image
  - With small frequency, select $c = 1$ and check equation
  - Pseudorandomly refresh crypto keys after each equation check
- Verifier extracts randomness from $c = 0$ (preimage) rounds

Protocol for certified randomness expansion

Verifier

public parameters pk →

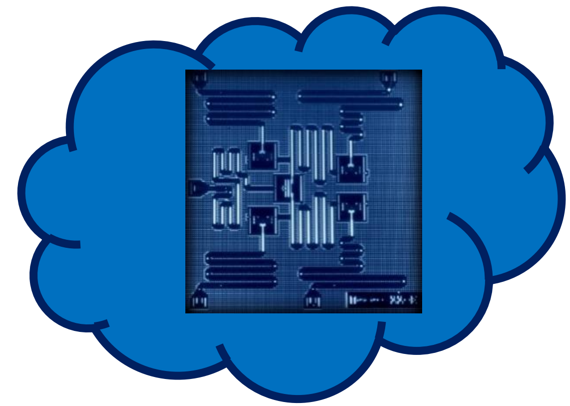
← *commitment* y

challenge $c = 0/1$ →

← $c = 0$: x_0 or x_1

$c = 1$: d s.t. $d \cdot (x_0 \oplus x_1) = 0$

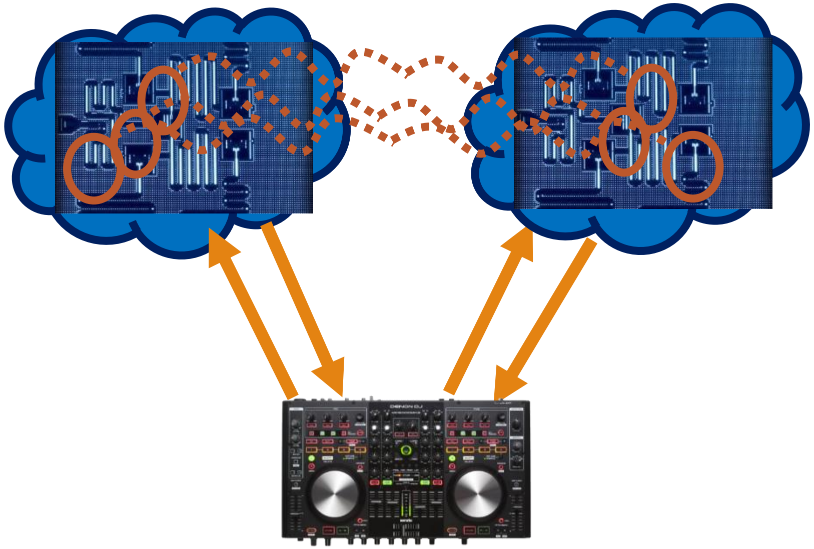
Device



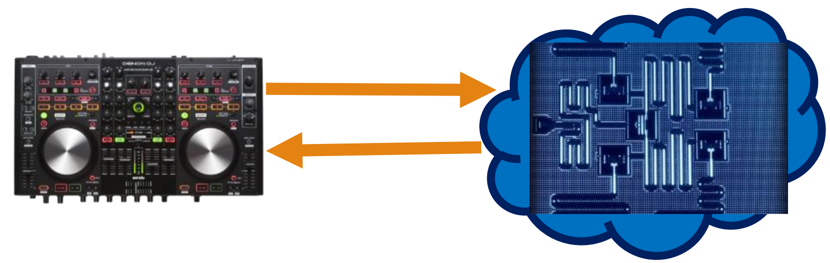
- Security proof: hardcore bit property → device's measurements unbiased
- In each round, device measures an "effective qubit"
  - In the computational basis if $c = 0$ (outcome is preimage choice)
  - In the Hadamard basis if $c = 1$ (outcome is equation validity)
- Valid equation → "effective qubit" is in $|+\rangle$ state

  → computational basis measurement generates randomness
- Randomness accumulation requires delicate adaptation of [MS'15,ADFRV'18]

Certifying quantum devices



- Two entangled devices
  - Bell inequality violation implies
    EPR pair + Pauli measurements (rigidity)
  - Certified randomness expansion [VV,MS’14]
  - Device-independent cryptography [VV,MS’14]
  - Delegated computation [RUV’13,CGJV’17]



- Single computationally bounded device
  - Certified qubit → certified randomness
  - [Mahadev’18] Homomorphic encryption
  - [Mahadev’18] Verified delegation
  - … more to come !?

Summary and open questions

- Classical verifier has four-message interaction with untrusted device
- Device succeeds in test + device does not break PQC assumption
  → device measured a qubit!
- N-round protocol generates $\Omega(N)$ bits of min-entropy
  Randomness secure from *unbounded* adversary entangled with device

- Out-of-the box implementation based on LWE requires 100s of qubits
  Can the protocol be fine-tuned?
- Removing interaction: publicly verifiable randomness
- Stronger rigidity results, e.g. characterize n-qubit device