Certified Randomness from Quantum Supremacy

Shih-Han Hung (National Taiwan University)
Joint work with Scott Aaronson (UT Austin)
arXiv:2303.01625

2024 Workshop on Quantum Science and Technology
July 1, 2024

Quantum Supremacy (aka Q. Computational Advantage)

A clear speedup from quantum devices compared to classical computers

IBM's Quantum Two (2023)
(three 133-qubit processors)

IBM's Summit (2018)
(200 petaFLOPS)

Give computational tasks (or tests) that certify that the device is able to process quantum info.

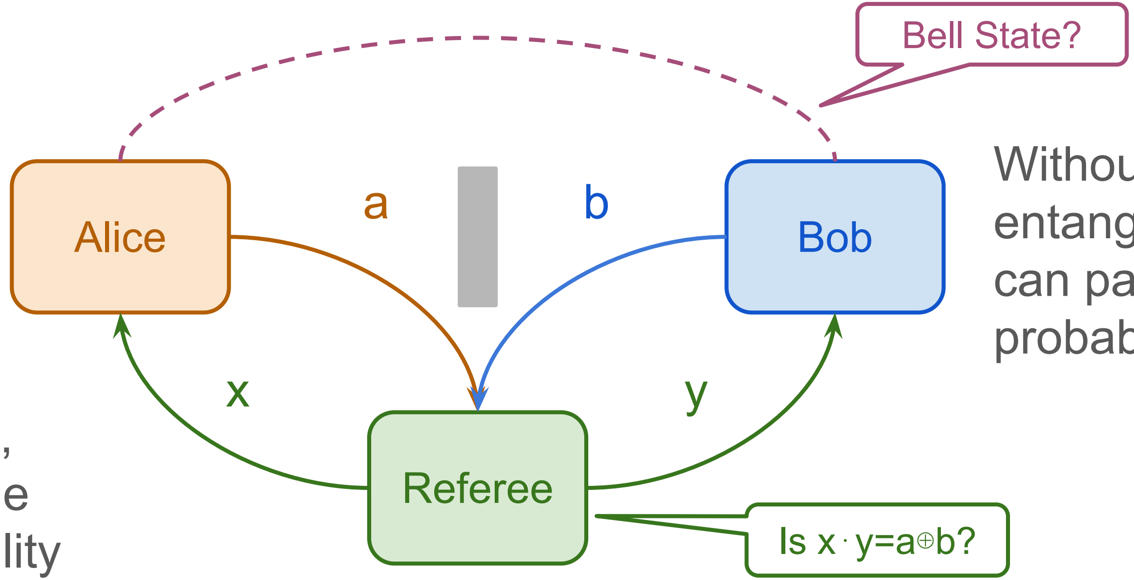
And hard to simulate using a classical (super)computer

Relaxations!

However, giving unconditional separation requires breakthrough in complexity theory!

Bell Tests: Advantage from Quantum Entanglements

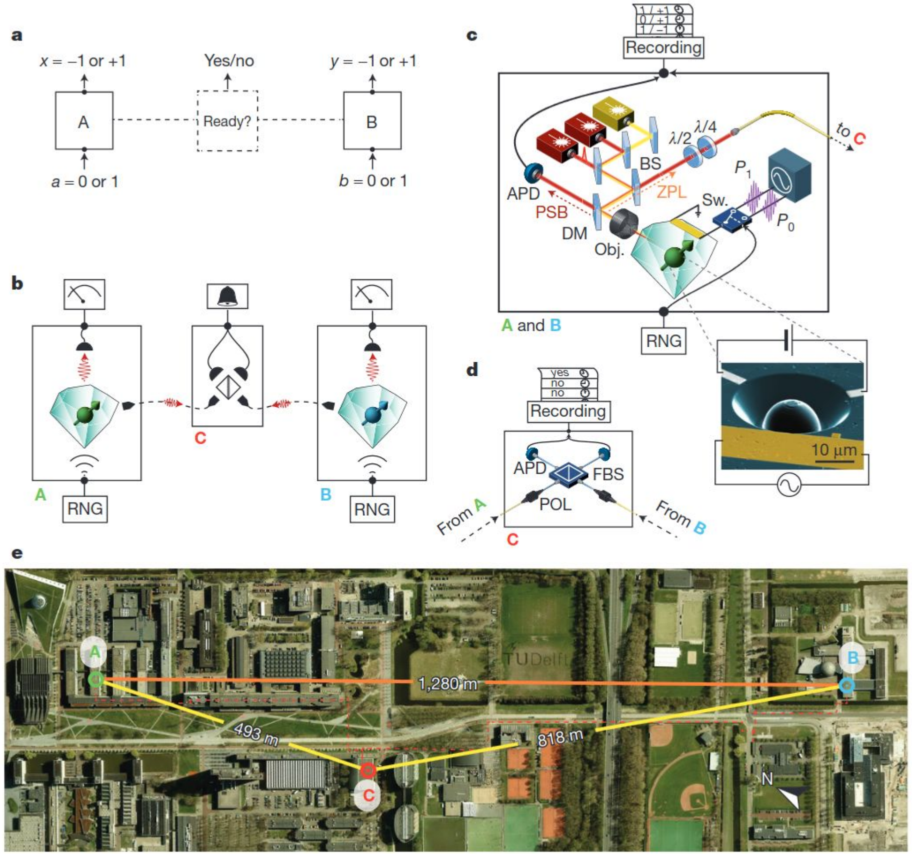
Checks if they share quantum entanglements



Without any entanglement, they can pass the test with probability ≤ 0.75

With a Bell state, they can pass the test with probability ≈ 0.85

Loophole-free Bell tests



Hard to enforce the physical assumption experimentally

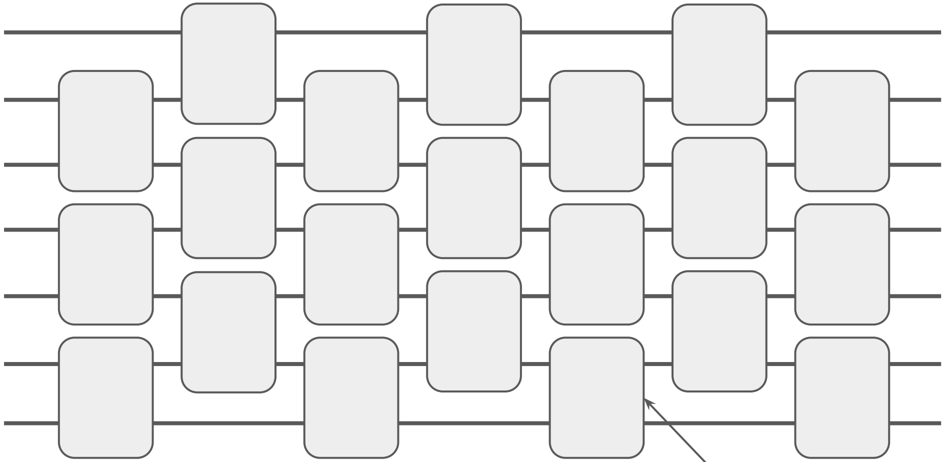
Hensen et al., Nature volume 526, pages 682–686 (2015)

Sampling-Based Supremacy

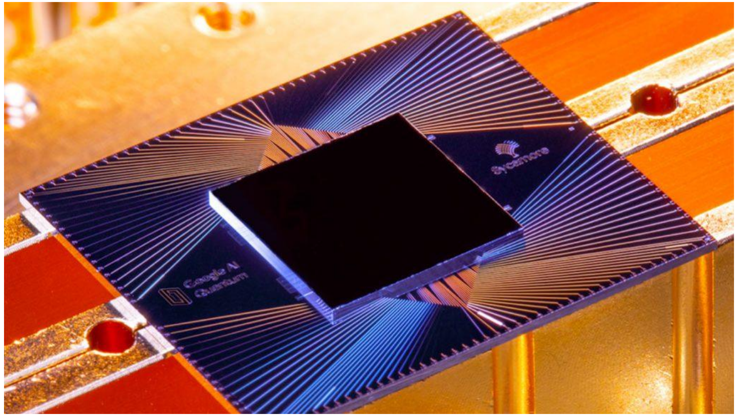
Arute et al., Nature volume 574, pages 505–510 (2019)

Sample from a distribution hard to sample from classical computers

- A random circuit is hard to simulate classically



A random gate over U(4)

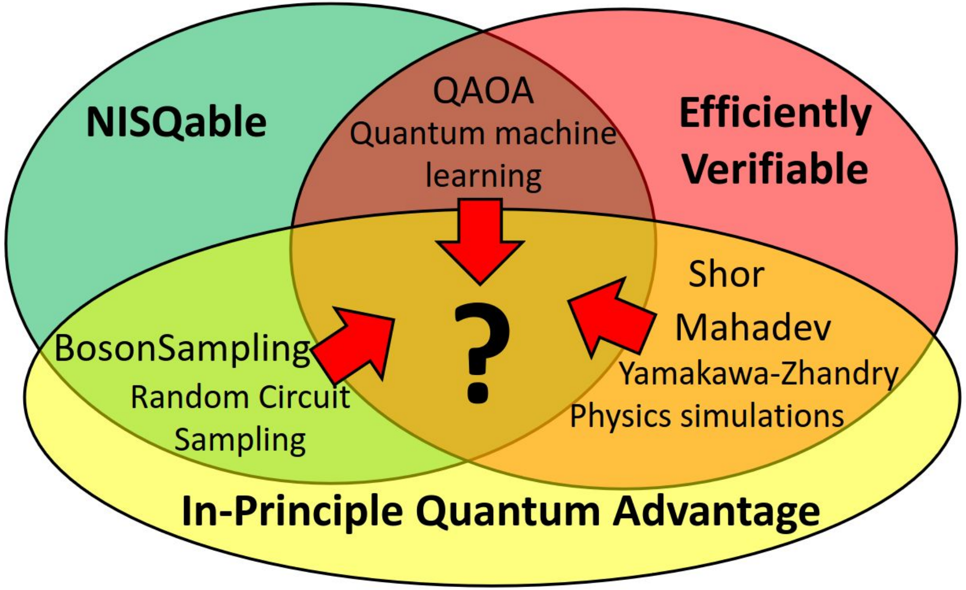


Google's fidelity estimator: Linear Cross-Entropy Benchmark (LXEB)

$$\frac{1}{k}\sum_{i=1}^{k} p_C(z_i) \geq \frac{b}{N}$$

What do we want from supremacy proposals?

Three desired properties from a single experiment:



Aaronson, Zhang, arXiv:2404.14493, 2024

Can Supremacy Lead to Any Useful Applications?

In addition to proving that quantum devices are more powerful, what other applications can we get out of them?

From Bell tests,

- Certified randomness
- Quantum key distribution
- Position verification
- Verifiable delegation of quantum computation
- …

How about single-device proposals?

Certified Random Number Generation

Random Number Generation

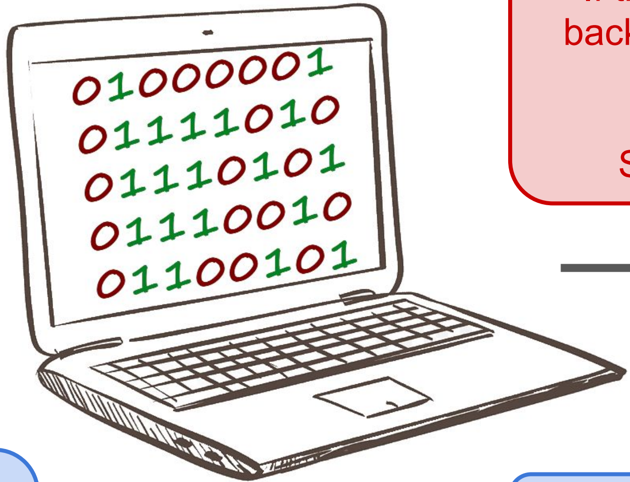
Critical for modern cryptography and algorithms

The output is NOT pseudorandom unless the seed is random!

If the seed is compromised, the attacker can compute the secret bits!

If the pseudorandom generator is backdoored, the attacker knows the secret bits!
Dual_EC_DRBG
Snowden revelations in 2013

01010110

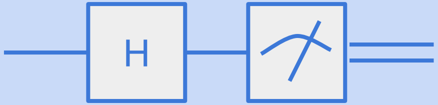


010101101010100...

Seed

Pseudorandom Bits

Using a quantum device?

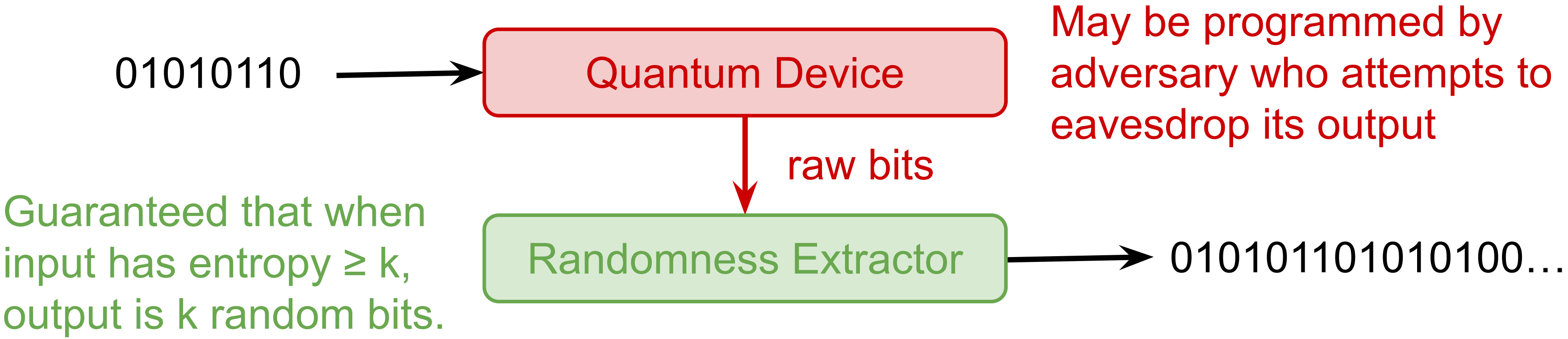


Can we do better? Get truly random bits from a short seed?

https://www.locksleylk.com/2020/quantumPrimer/

Certified Random Number Generation?

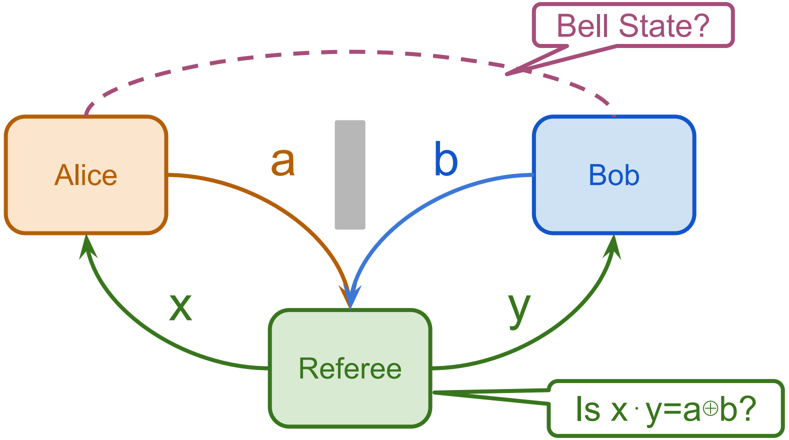
Performed in two steps:



Certified Random # Generation: ∀ device, Test(seed, raw bits) = accept ⇒ entropy ≥ k

How is Certified Randomness related to Q. Supremacy?

The same test can be used to certify random bits!



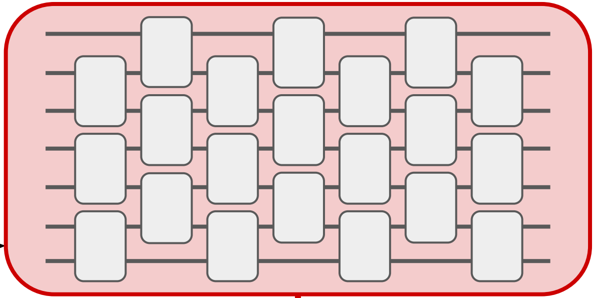
Can an **experimentally feasible** test be used to **efficiently** generate certified random bits?

Pr[accept] ≥ 0.85-ε
⇒ state is O(ε)-close to a Bell state
⇒ entropy/round ≥ 1-O(ε)
☹ Hard to enforce physical assumptions

Some tests based on post-quantum cryptography can be used to generate O(1) random bits/round
☹ Out of reach using a near-term device

Certified Random Number Generation from RCS

01010110



May be programmed by adversary who attempts to eavesdrop its output

raw bits

Guaranteed that when input has entropy ≥ k, output is k random bits.

Randomness Extractor

010101101010100…

Certified Random # Generation: ∀ device, LXEB(C, raw bits) = accept ⇒ entropy ≥ k

Aaronson, H., STOC 2023

Does a Perfect QC Generate Random Bits on RC?

With a truly random circuit C and a perfect QC, $b \approx 2$ and entropy = $n - O(\log n)$, conditioned on C.

For a QC with fidelity $F \leq 1$,

- e.g., QC outputs a sample from C w.p. F and 0 w.p. 1 - F,
- $b \approx 1 + F$ and Shannon entropy $\approx n \cdot F$.

How do we handle an arbitrary device?

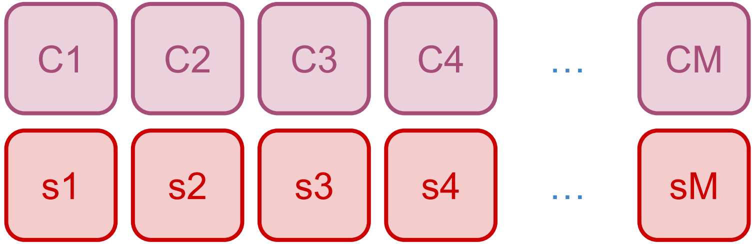
How to Prove LXEB Certifies Random Bits?

Theorem: ∀ device, (LXEB(C, raw bits) = accept ⇒ entropy ≥ k)

Proof sketch:

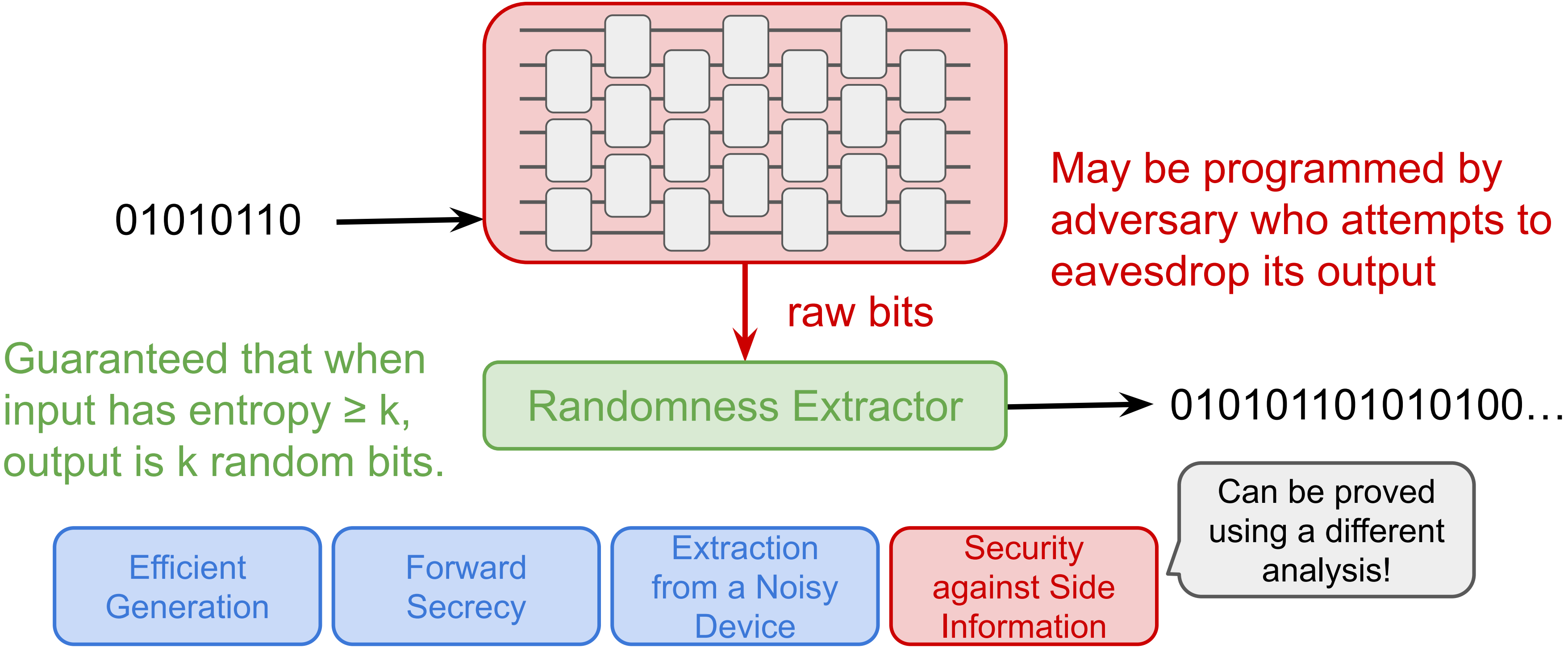
- QC does not have unlimited power ⇒ it cannot solve some problem.
- If a device A violates Theorem, then one can use A to solve the problem.

What problem is hard and can be used to prove Theorem?
Aaronson 2019: Long List Quantum Supremacy Verification (LLQSV)



LLQSV: Distinguish each si is sampled from Ci or uniform, promised one is the case.

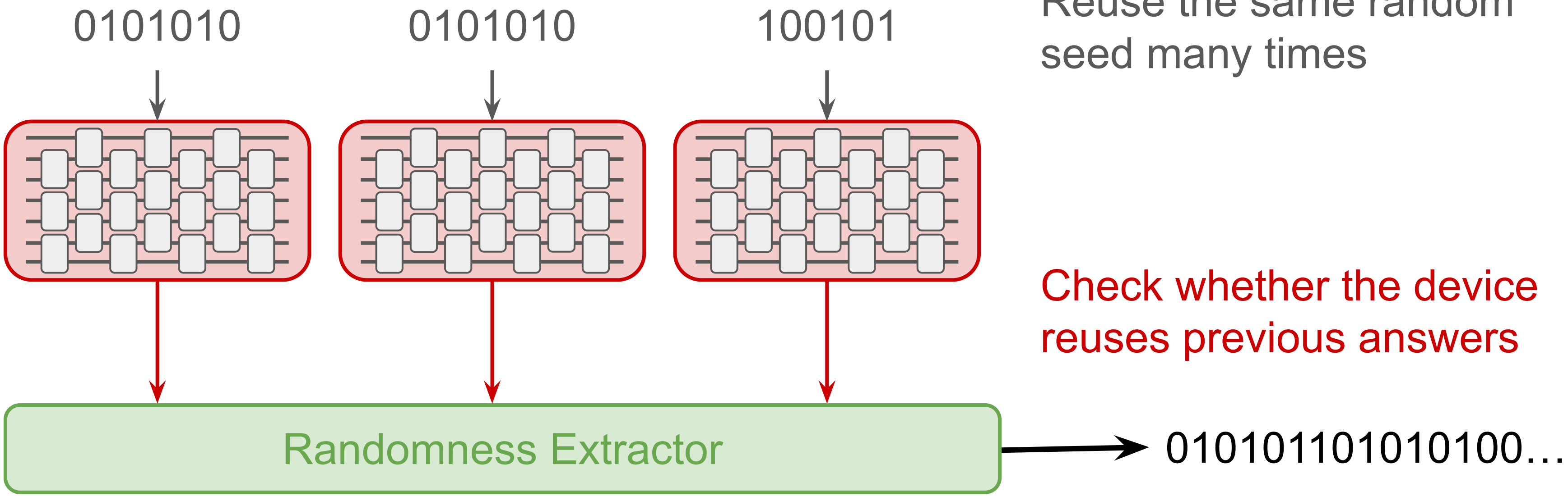
What Security Guarantees do Theorem Offer?



Aaronson, H., STOC 2023

Entropy Accumulation

Can we repeat the protocol to accumulate more random bits?



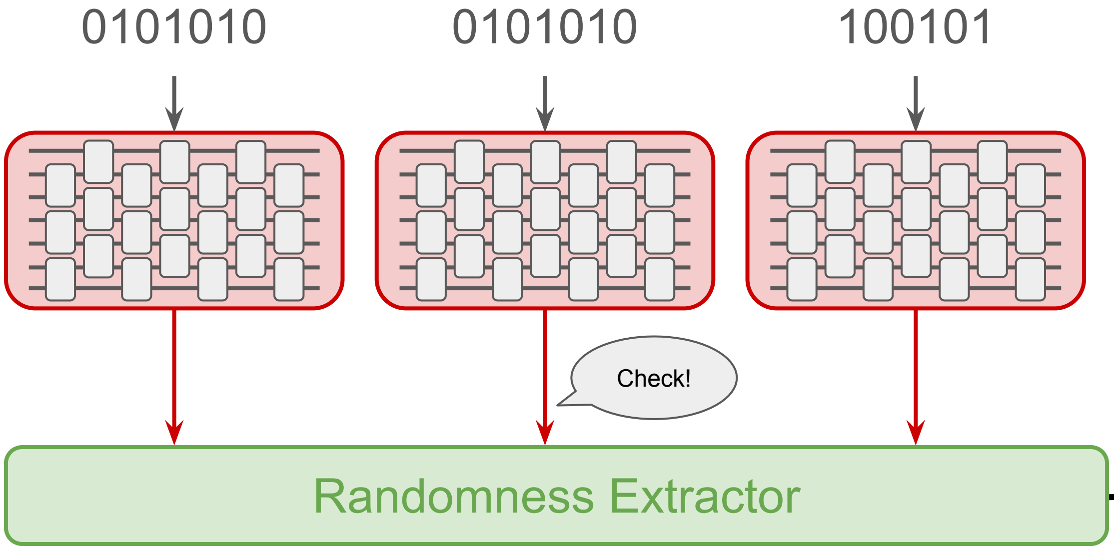
Reuse the same random seed many times

Check whether the device reuses previous answers

Spot Checking

The LXEB verification takes a long time to complete…

Can we only check a small subset of samples?



→ 010101101010100…

Reuse the same random seed many times

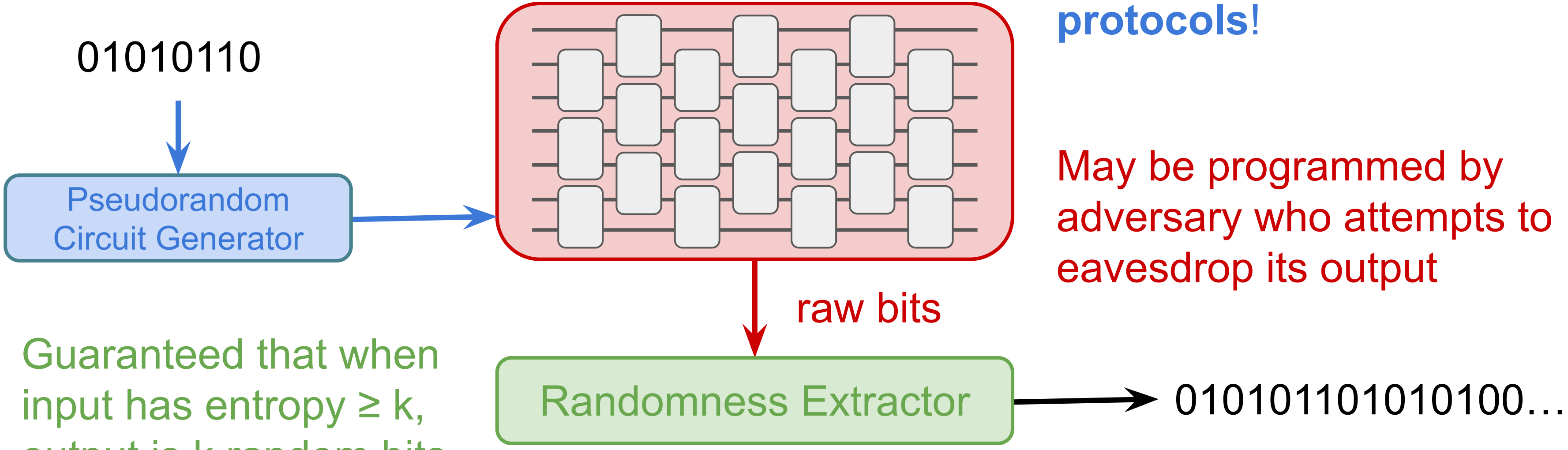
Only checks a small subset of raw bits sampling from the same circuit

Randomness Expansion

Generating random circuits takes a long seed.

Can we generate pseudorandom circuits instead?

The **pseudorandom circuit generator** must be secure against a stronger quantum adversary, called **quantum statistical zero-knowledge (QSZK) protocols**!



May be programmed by adversary who attempts to eavesdrop its output

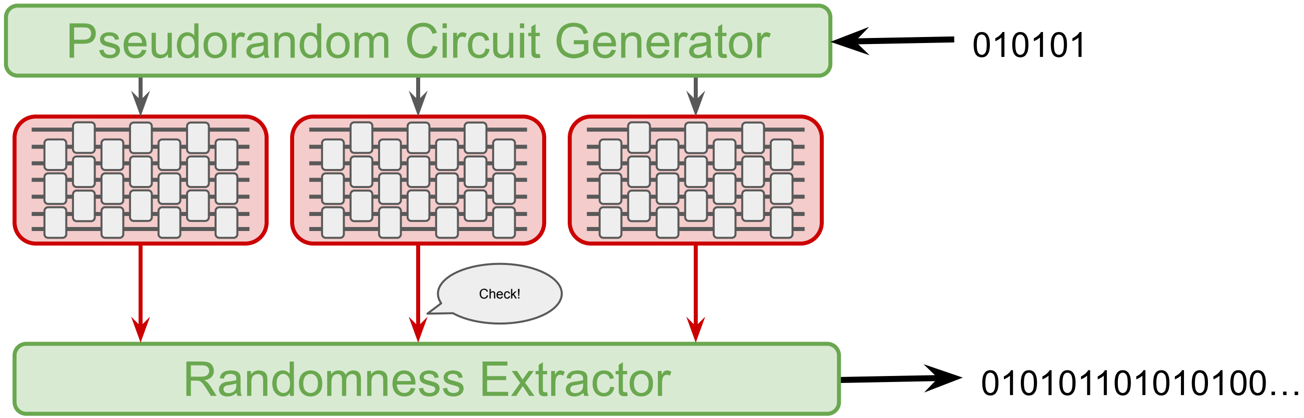
Guaranteed that when input has entropy ≥ k, output is k random bits.

Summary

Summary

The status of quantum supremacy experiments

- Sampling-based supremacy
- Bell tests
- Oracle separations
- Tests based on cryptographic assumptions



Aaronson, H.
STOC 2023,
arXiv:2303.01625

Future Directions

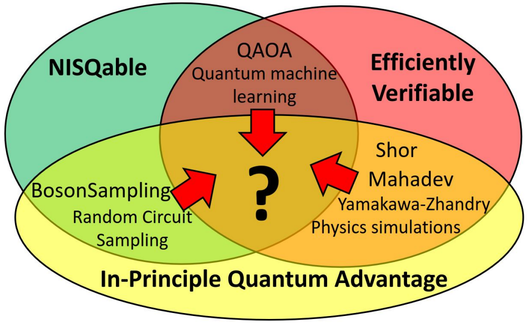
Experimental realizations of our certified random number generation?

Do other (sampling-based) proposals imply certified random number generation?

Other applications from sampling-based supremacy?

Formal connections between certified randomness and supremacy?

New supremacy proposals that achieves the three properties?



Thanks! Questions?