Don't Look Now: Quantum Computing and Cybersecurity

Yi-Kai Liu

NIST / University of Maryland

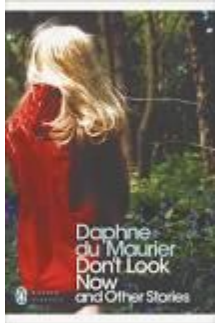
Joint Center for Quantum Information and Computer Science

Two Hot Topics

Quantum computing and cybersecurity

Broad research themes (from the past 5 years, to the next 5 years)
- Post-quantum cryptography (and quantum key distribution)
- Building quantum computers (and the "quantum internet")
- The impact of quantum devices on cybersecurity

How is quantum computation different from classical?
- Superpositions and nonlocality – "don't look now"



Part I: Post-Quantum Cryptography and Quantum Key Distribution

Post-Quantum Cryptography (PQC)

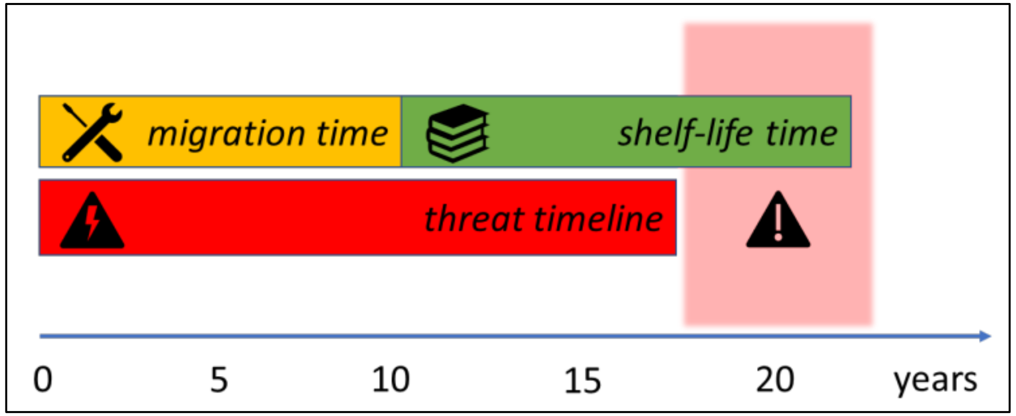
Shor's algorithm (1994): Quantum algorithm for factoring and discrete logs in polynomial time

- Breaks RSA, discrete log and elliptic curve cryptosystems
- Breaks TLS, IPSec key establishment, digital signatures and certificates

Late 1990s-early 2000s: Quantum fault-tolerant computation is possible in principle

- A huge engineering challenge

Time to deploy post-quantum cryptography…



Mosca and Piani, Global Risk Institute 2021 Quantum Threat Timeline Report

Post-Quantum Cryptography (PQC)

Needs: Public-key encryption / key establishment, digital signatures

- Used throughout the internet (TLS, IPSec, certificate chains, many other systems)

Many candidates:

- Lattice-based crypto (e.g., NTRU, LWE-based schemes, also signatures)
- Code-based crypto (e.g., McEliece, newer ideas)
- Multivariate crypto (mainly signatures, e.g., HFEv-, UOV, and newer variants)
- Isogenies of supersingular elliptic curves
- Hash-based signatures (stateful and stateless)
- Others (e.g., signatures based on secure MPC)

PQCrypto 2022
The 13th International Conference on Post-Quantum Cryptography
September 28–30, 2022

NIST PQC Standards

Open, competition-like process, started in 2016

- Round 3 began in July 2020
- Standards announcement coming soon
- https://csrc.nist.gov/Projects/post-quantum-cryptography

See also: NIST project on "Migration to PQC"

- https://www.nccoe.nist.gov/

One of the biggest Internet transitions ever

- We need and appreciate your help…

Some Directions for Research

- PQC deployment
  - How to ease the process of migrating legacy systems to PQC?
- Security in the real world
  - How to build end-to-end secure systems around PQC?
  - Side-channel attacks, combined with cryptanalysis
    (targeting the combination of a hardware vulnerability and a crypto vulnerability)
- Security against quantum adversaries
  - Quantum algorithms for number theoretic problems (e.g., ideal lattices, isogenies)
  - Techniques for proving security, e.g., in the quantum random oracle model

What about QKD?

Quantum key distribution (QKD)

- Generate a shared secret key, or abort if eavesdropper is present
- Information-theoretic security, with some caveats
- Already demonstrated/deployed in some cities, and ground-satellite links

Caveats	Potential solutions
Limited range	Trusted repeaters, quantum repeaters, quantum internet…
Vulnerability to side-channel attacks	Better single-photon sources/detectors, better protocols (e.g., decoy-state QKD, MDI-QKD)
Vulnerability to denial-of-service attacks	

Technological Foundations of QKD

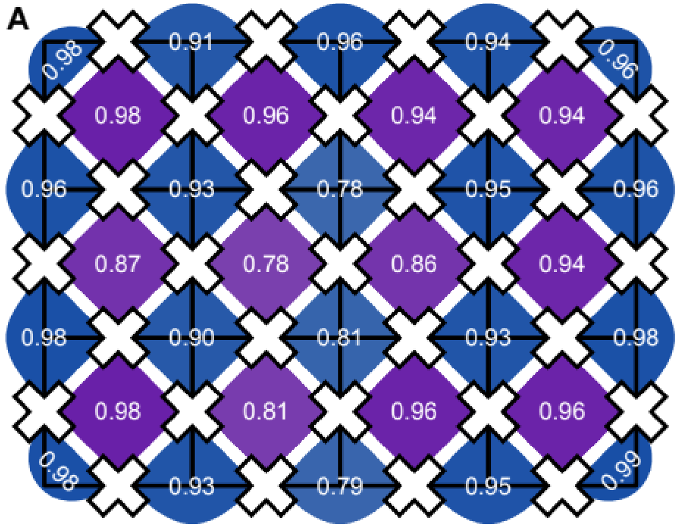
Technology	Examples	Desirable characteristics
Single-photon sources	Attenuated lasers, semiconductor quantum dots	Deterministic, on-demand, no multi-photon emissions
Single-photon detectors	Avalanche photodiodes, superconducting transition-edge sensors, superconducting nanowires	High efficiency, few dark counts, fast response, fast reset time

These technologies can potentially do more than QKD

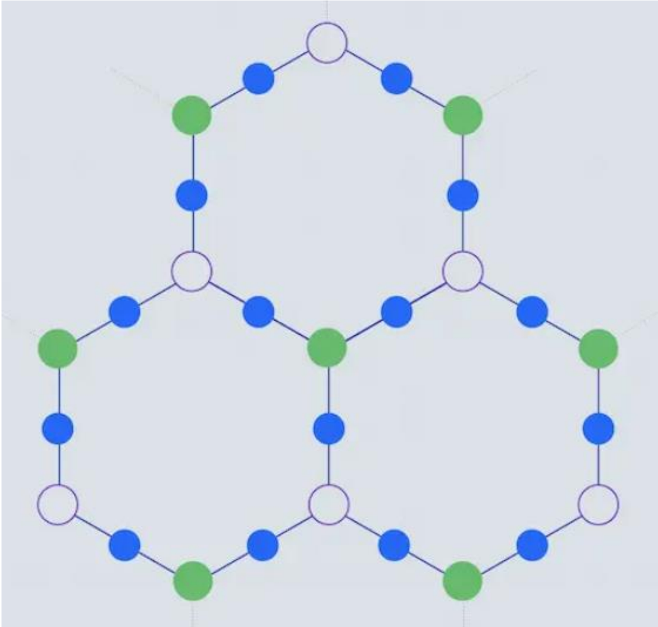
- "Self-testing" of random number generators
- The "quantum internet," and photonic quantum information processing
- (To be continued…)

Part II: Quantum Computers and Networks

Building Quantum Computers

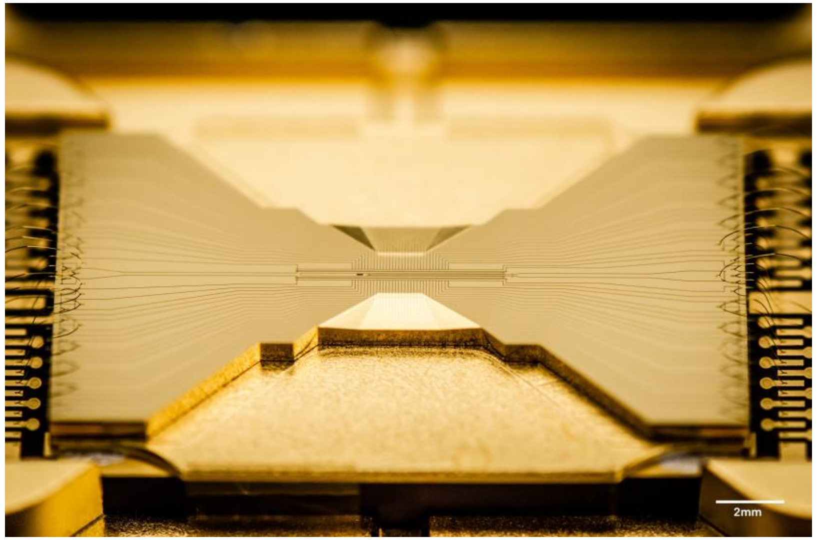


Google – superconducting qubits, quantum supremacy via random circuit sampling (2019)
Satzinger et al, "Realizing topologically ordered states on a quantum processor," Science (2021)

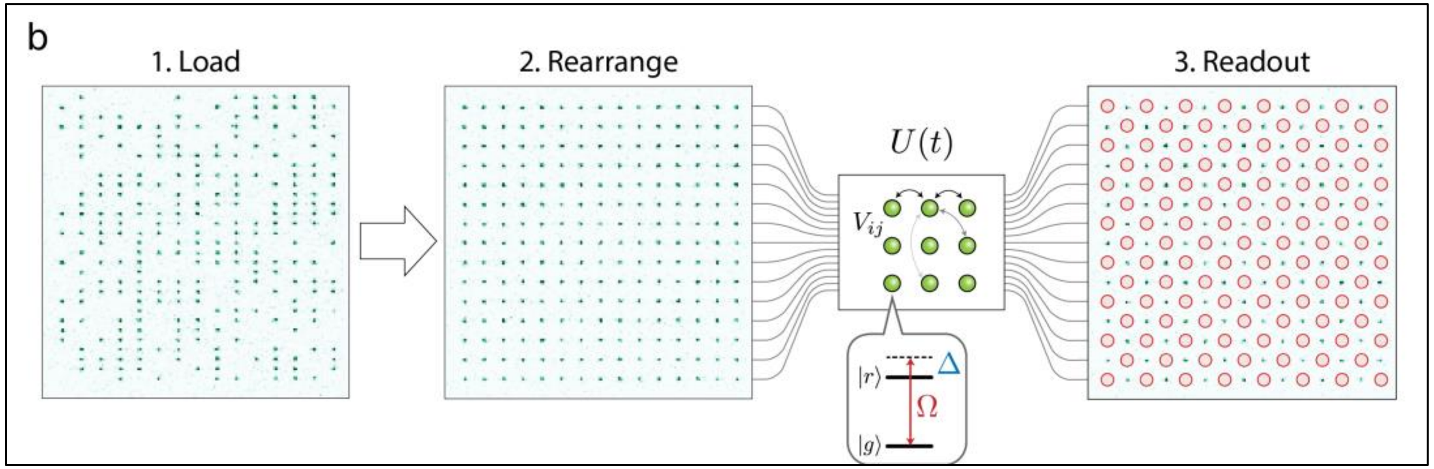


IBM – superconducting qubits
https://research.ibm.com/blog/heavy-hex-lattice

Building Quantum Computers

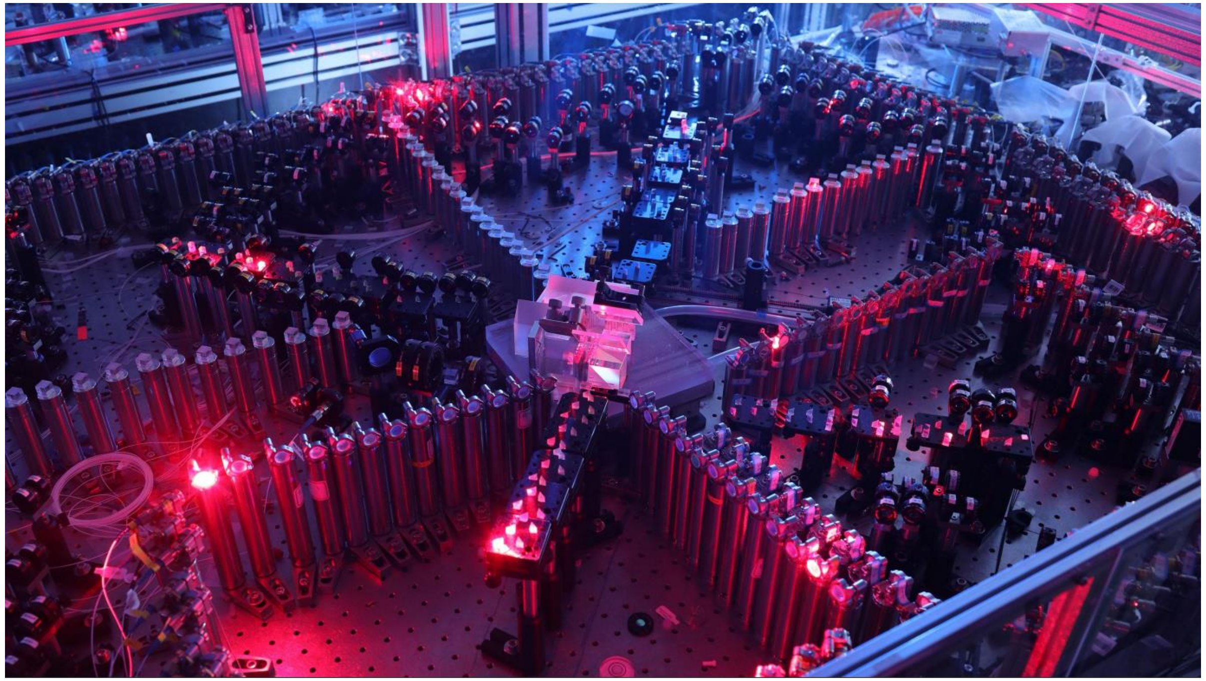


IonQ – trapped ions
Credit: Kai Hudek - IonQ



Greiner, Lukin groups (Harvard) – neutral atoms, optical tweezers
Ebadi et al, “Quantum Phases of Matter on a 256-Atom Programmable Quantum Simulator,” Nature (2021)

Building Quantum Computers



Chao-Yang Lu, Jian-Wei Pan groups (USTC) – Boson sampling
Zhong et al, “Quantum computational advantage using photons,” Science (2020)

And many other approaches:

- Photonic cluster states
- NV centers in diamond
- Quantum dots in semiconductors
- Topological anyons in semi-conductor nanowires

The Next Milestone: Useful Quantum Computers?

Two difficulties: Overcoming noise, and scaling up

Current devices: “NISQ” (noisy intermediate-scale quantum) (Preskill, 2018)

- Hundreds of qubits, gate error rates of .01 or better

- Amazing progress in building bigger/better hardware
- Plans to scale up are becoming more credible

- But still not very useful for many practical applications
- Users are plagued by noise and limited hardware resources

https://upload.wikimedia.org/wikipedia/commons/a/a4/Glass_Half_Full_bw_1.JPG

Applications of Quantum Computers

Using NISQ devices:

Using fault-tolerant quantum computers:

Quantum simulation

Condensed matter physics

Quantum chemistry

Digital quantum simulation

Near-term → **More speculative**

"Quantum supremacy" (boson sampling, random circuit sampling)

Electromagnetic scattering calculations

Quantum machine learning?

Solving certain kinds of linear systems (HHL algorithm)

Shor's algorithm

Other quantum algorithms with large speedups?

Simulating Quantum Systems

Idea: Prepare the N-particle wavefunction, and measure its properties

- Simulating time evolution: analog or digital quantum simulation
- Predicting ground state properties: variational quantum eigensolvers (VQE)
- (Caveat: These problems can be NP-hard, or worse)

	What to simulate?	Compare with existing methods
Condensed matter physics	1-D and 2-D systems (e.g., Hubbard model, high-temp superconductivity)	Tensor networks, DMRG, quantum Monte Carlo
Quantum chemistry	Molecules (electronic structure)	Coupled-cluster method
Materials science	Various	Density functional theory

One example: Seetharam et al, "Digital quantum simulation of NMR experiments," Arxiv:2109.13298

NISQ Devices

Noise is visible to the user

- Gate error rate ε => errors are likely after O(1/ε) gates
- Various strategies for extracting signal from noise, or compensating for noise

https://upload.wikimedia.org/wikipedia/commons/a/a8/TV_noise.jpg

Hardware resources are quite constrained

- Number of qubits, connectivity between qubits
- Barely enough to demonstrate "quantum supremacy" (on artificially-constructed hard problems)
- Not enough for fault-tolerant quantum computation

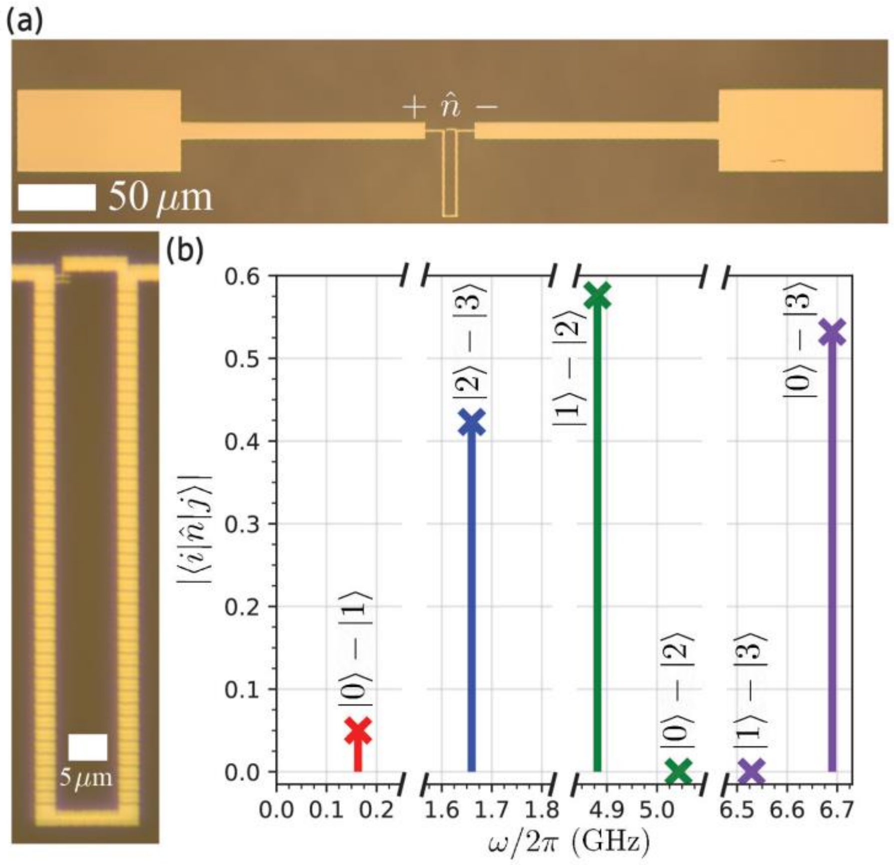
https://upload.wikimedia.org/wikipedia/commons/f/f7/Citizen_SLD-100NR_calculator.jpg

The Path Ahead

Better qubits (lower error rates)

- New designs for superconducting qubits?
- Better materials/designs for quantum dots?
- Topological anyons?

- More connectivity would be nice, but this is hard
- Eventually, need quantum error correction…



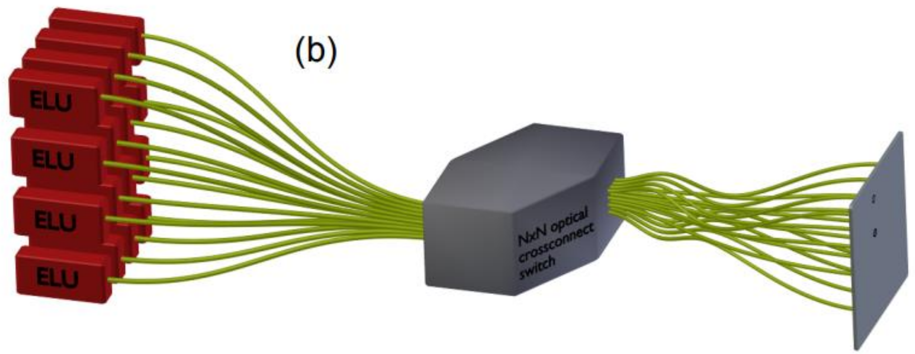
Somoroff et al, "Millisecond coherence in a superconducting qubit," Arxiv:2103.08578

The Path Ahead

More qubits

- Multiple ion traps + photonic entanglement swapping (a.k.a., quantum repeaters)
- On-chip control for superconducting qubits? (e.g., flip-chips)
- 2-D arrays of ions/atoms (e.g., Penning traps, optical tweezer arrays)
- Silicon integrated photonics (for cluster state quantum computation)

This is possible, but certainly not easy



Monroe et al, “Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects,” PRA (2014)

The Path Ahead

Fault-tolerant quantum computation

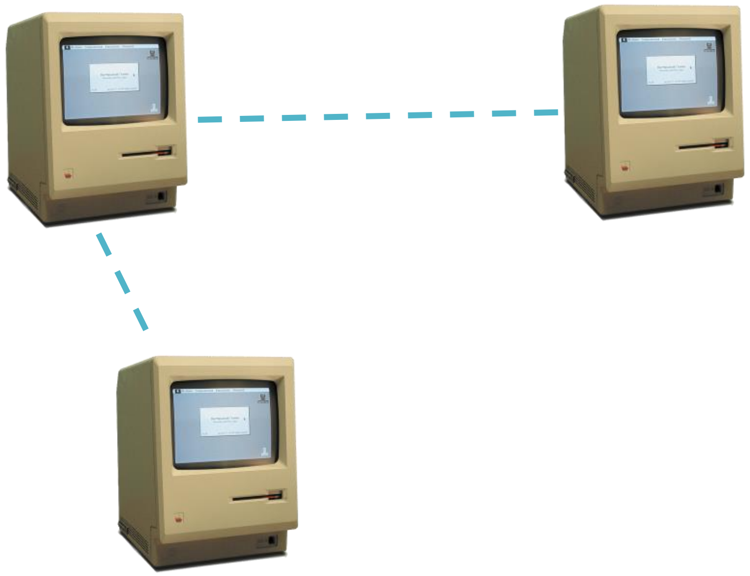
- Quantum error-correcting code: k logical qubits → n physical qubits
- Correct physical errors w/o disturbing the logical state
- Apply logical gates w/o propagating physical errors too badly

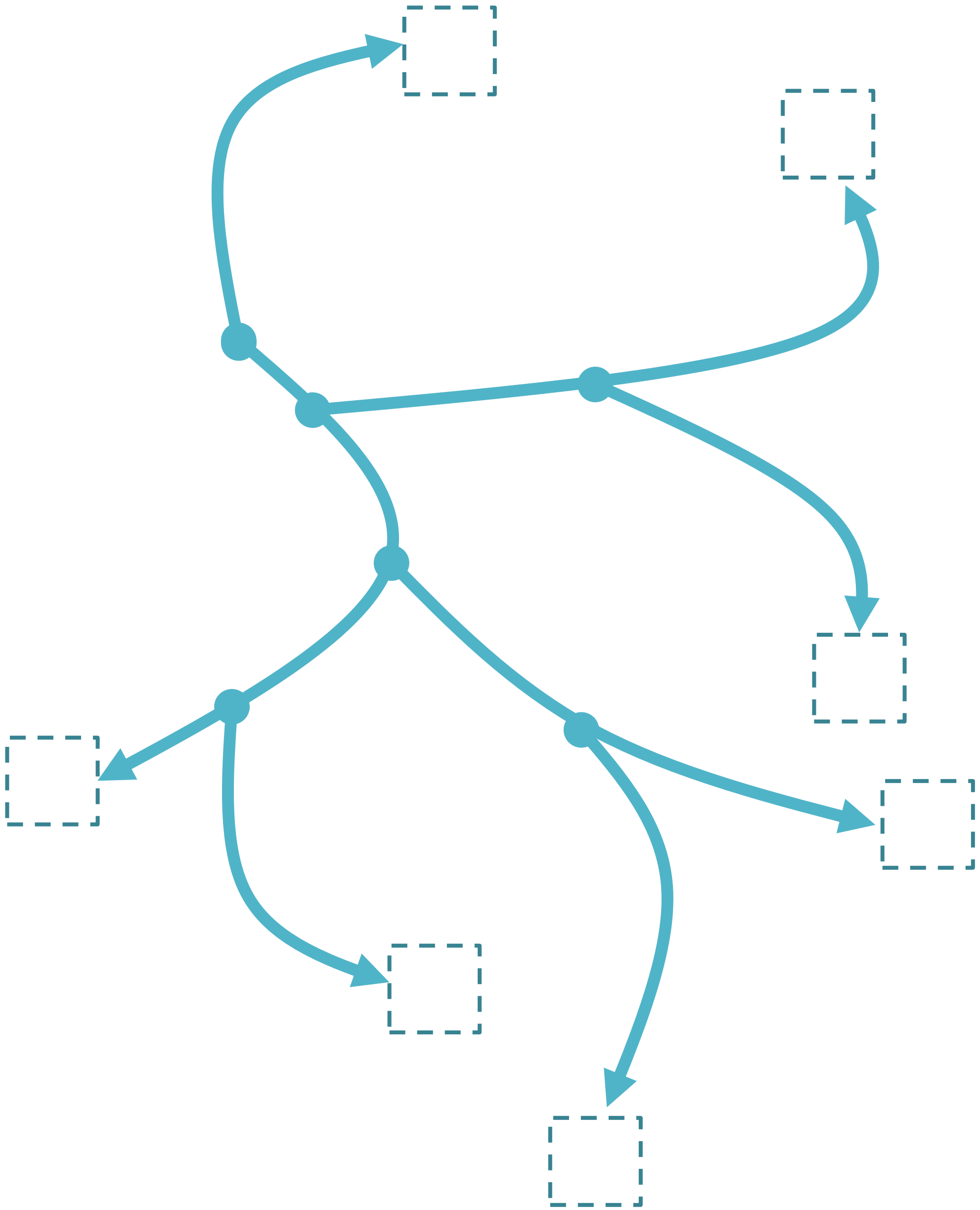
- Key parameters: threshold error rate ε_{th}, overhead n/k
- Some examples/techniques: surface code, QLDPC codes, magic state distillation

- This is when quantum cryptanalysis becomes a threat

Quantum Networks

Two perspectives on what makes a network:





https://upload.wikimedia.org/wikipedia/commons/e/e3/Macintosh_128k_transparency.png

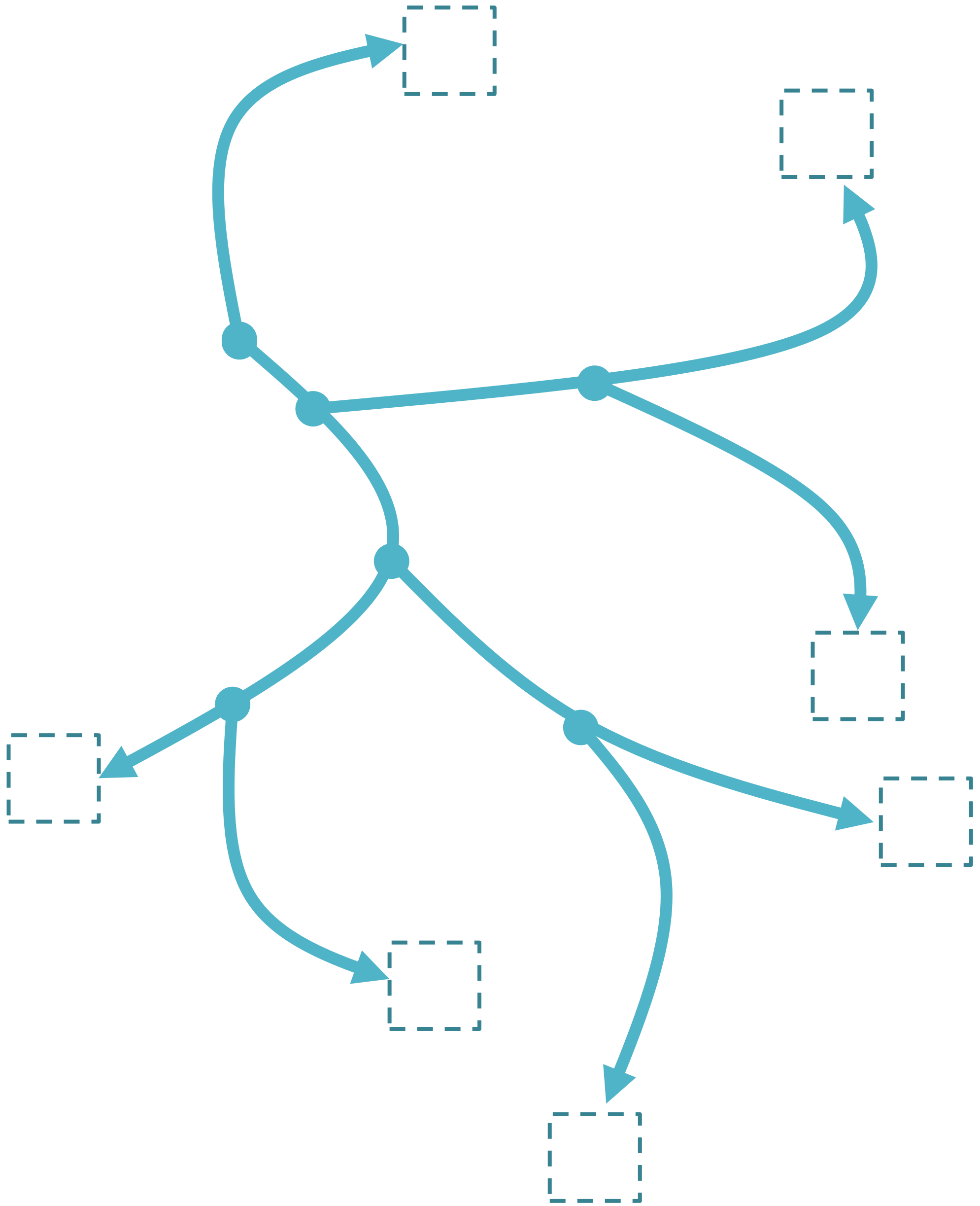
Quantum Networks

What makes a **quantum** network?

- Ability to generate **entanglement** between distant parties, via photons
- The technological successor to QKD?

What can one do with entangled photons?

- Quantum key distribution (QKD)
- Bell tests – disproving “local realism”
- Self-testing of quantum devices
- All-optical quantum repeaters
- Cluster state quantum computation



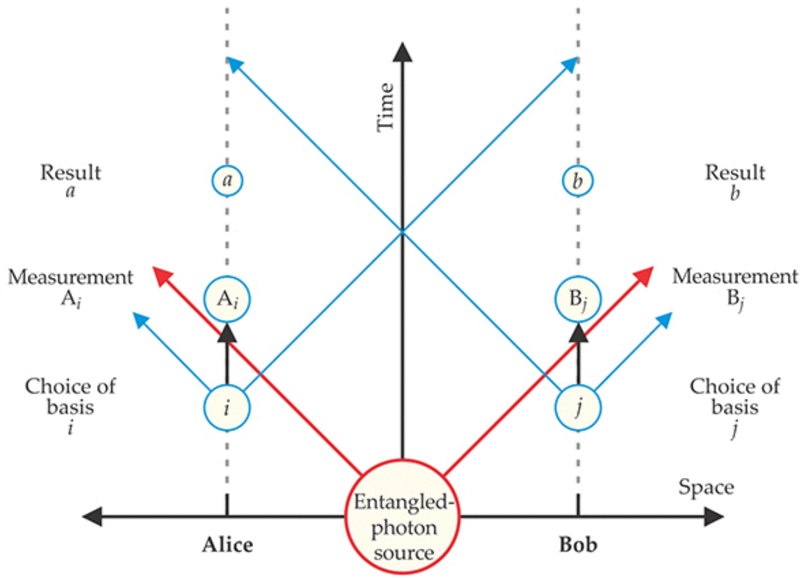
The Path Ahead

A milestone: “Loophole-free Bell test” (2016)

- Enabled by better sources, detectors, q memories
- => Entanglement swapping b/w solid-state qubits
- => Self-testing random number generators

Quantum repeaters

- Extending q networks beyond the distance limit set by photon loss in optical fiber
- Coupling entangled photons to matter qubits (trapped ions, neutral atoms, NV centers)

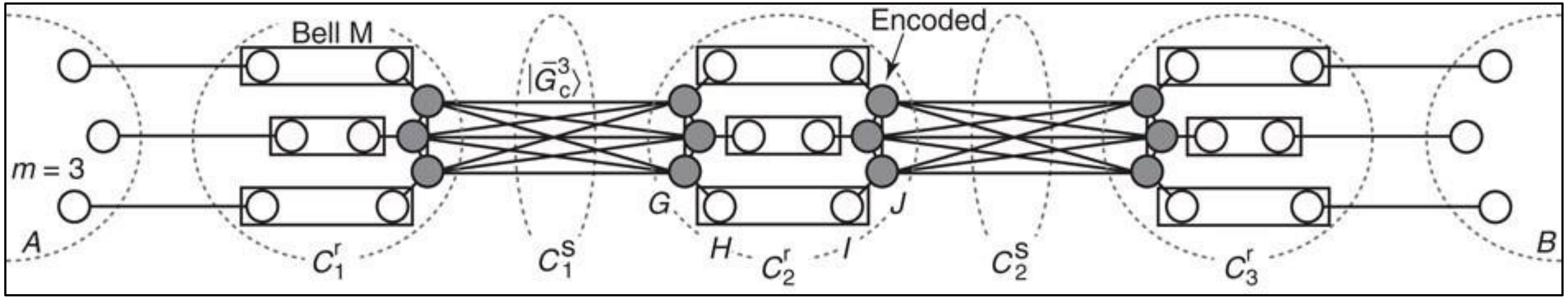


Physics Today (2016), https://doi.org/10.1063/PT.3.3039

The Path Ahead

Photonic cluster states?

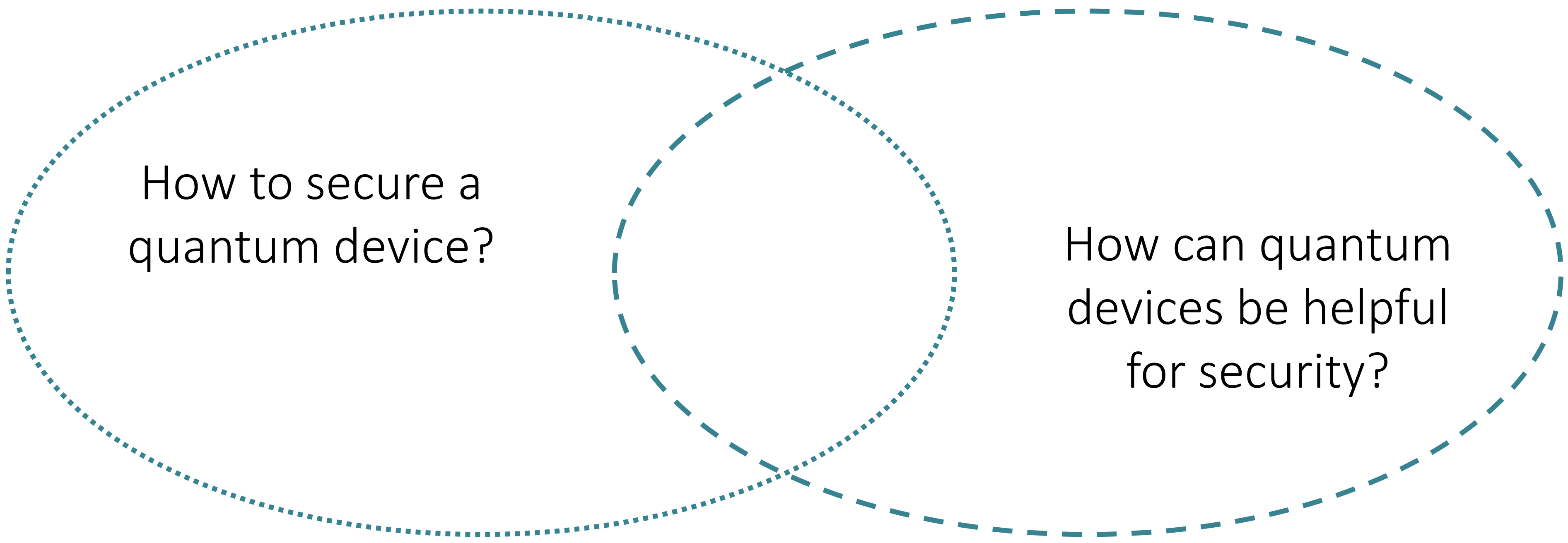
- Surprisingly robust to photon loss (but require lots of photons)
- All-photonic quantum repeaters
- Measurement-based quantum computation
- The promise and perils of silicon integrated photonics



Azuma et al, “All-photonic quantum repeaters,” Nat. Commun. (2015)

Part III: The Impact of Quantum Devices on Cybersecurity

Part III: The Impact of Quantum Devices on Cybersecurity



How to secure a quantum device?

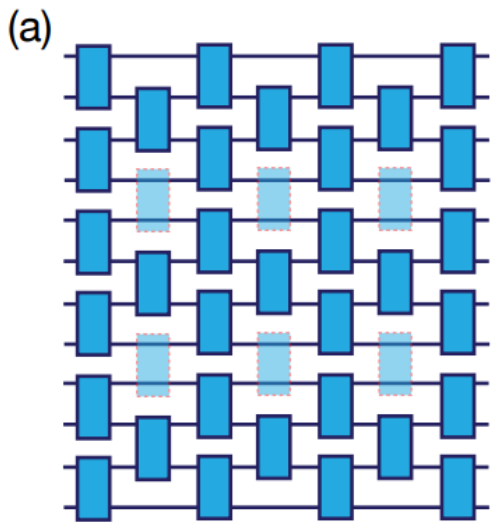
Security = "no surprises"

One problem: Quantum computation is inherently probabilistic

- E.g., quantum supremacy, using "sampling problems"
- Need to infer properties of distributions from samples
- Use cross-entropy benchmarking (XEB)
- **But this can be spoofed!**

Contrast with classical randomized algorithms

- Random coin flips can be simulated deterministically, using a cryptographic pseudorandom generator



Gao et al, "Limitations of Linear Cross-Entropy as a Measure for Quantum Advantage," Arxiv: 2112.01657

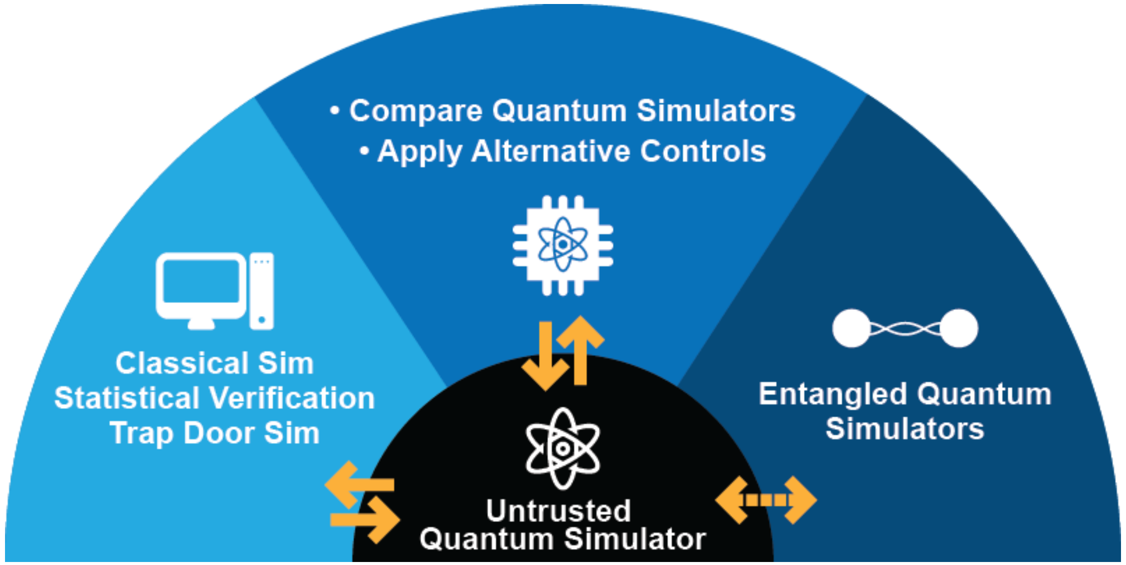
How to secure a quantum device?

How to gain confidence in a quantum computation?

Compare two different implementations

Various pitfalls:

- Classical complexity
- How to “read out” the quantum state?



https://rqs.umd.edu/

Institute for Robust Quantum Simulation

How to secure a quantum device?

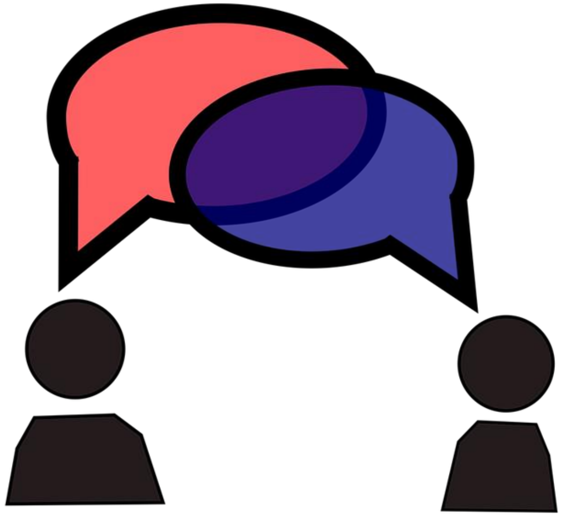
Use techniques from cryptography (e.g., interactive proofs)?

Blind quantum computation (2009) – using quantum verifier

- Measurement-based quantum computation,
  or teleported gates + one-time-pad
- See also "quantum prover interactive proofs"

"Mahadev" protocols (2018) – using classical verifier

- Use trapdoor-clawfree functions (TCF)
- Has other interesting applications, e.g., "deniable encryption"
  - *(Coladangelo et al, Arxiv:2112.14988)*



https://cdn.pixabay.com/photo/2016/03/17/04/34/conversation-1262311_640.png

How to secure a quantum device?

A key subroutine of a “Mahadev-style” protocol: Preparing the states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$

Prover (quantum)		Verifier (classical, knows trapdoor)
Prepare state $\sum_x |x\rangle|f(x)\rangle$	←	Let f = trapdoor clawfree function (TCF), send to prover
Measure 2nd register, get y, send to verifier Remaining state is $|x_0\rangle + |x_1\rangle$	→	Learn y = $f(x_0) = f(x_1)$, compute x_0 and x_1
If requested, measure the state and send the result (x_0 or x_1) to prover. Else, compute $|r \cdot x_0\rangle|x_0\rangle + |r \cdot x_1\rangle|x_1\rangle$	←	Flip a coin. If heads, ask the prover to send a preimage, check it, and accept/reject. If tails, choose random r, send to prover
Measure 2nd register in Hadamard basis, get d, send to verifier Remaining state $|\psi\rangle$ is one of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$	→	Learn d, calculate the state $|\psi\rangle$

How can quantum devices be helpful for security?

- Applications of Bell tests and quantum entanglement
  - Random number generators
  - Self-testing of quantum devices
- Shifting foundations of cryptography
  - Quantum money
  - Secure hardware (OTMs, PUFs)
  - Pseudorandom quantum states
- Cyber-physical systems using quantum sensors
  - GPS, clocks, gyroscopes
  - Interferometric telescopes, quantum illumination

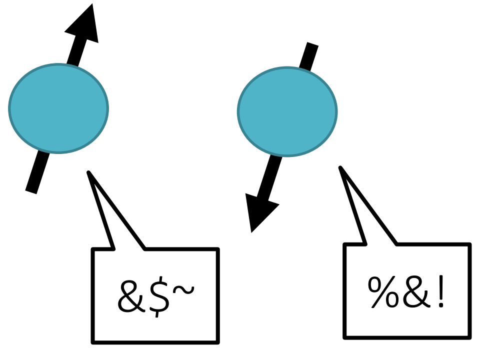
https://www.nist.gov/blogs/cybersecurity-insights

Bell Tests and Quantum Entanglement

Consider a maximally entangled state of two qubits

- Superposition (not a probabilistic mixture)
- Entanglement (“nonlocality”)
- Measurements are intrinsically random/unpredictable

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$



Could there be a more complete description of this?

- **Locality + realism (LR):**
- Measurements of a particle at position x can be predicted deterministically, using only information at position x

The answer is no!

- Quantum experiments produce results that cannot be obtained from any LR model

Bell Tests and Quantum Entanglement

The answer is no!

- Quantum experiments produce results that cannot be obtained from any LR model

Except that some implementations of Bell tests have “loopholes”

- “No-signalling assumption” (if Alice and Bob are nearby)
- “Fair sampling assumption” (if detectors are not sensitive)
- By violating these assumptions, a local realistic (LR) adversary could spoof a Bell test

Hence the significance of the “loophole-free Bell test”

Bell Tests and Quantum Entanglement

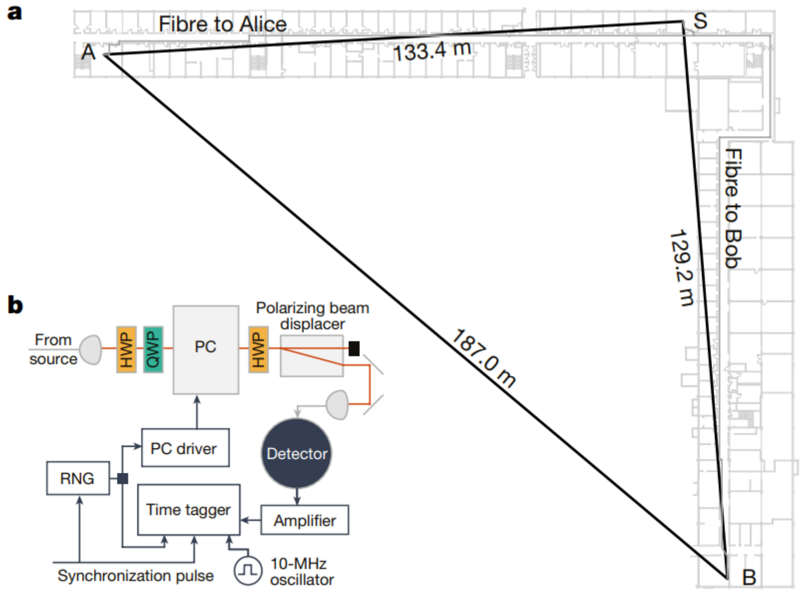
Violating local realism has interesting consequences for information security

Output of Bell test is random/unpredictable, even to an adversary

- Random number generators

The optimal strategy for "passing" the Bell test is "rigid" (unique up to trivial isomorphisms)

- "Self-testing" (certifying that a device is operating correctly)



Bierhorst et al, "Experimentally generated randomness certified by the impossibility of superluminal signals," Nature (2018)

How can quantum devices be helpful for security?

- Applications of Bell tests and quantum entanglement
  - Random number generators
  - Self-testing of quantum devices
- Shifting foundations of cryptography
  - Quantum money
  - Secure hardware (OTMs, PUFs)
  - Pseudorandom quantum states
- Cyber-physical systems using quantum sensors
  - GPS, clocks, gyroscopes
  - Interferometric telescopes, quantum illumination

https://www.nist.gov/blogs/cybersecurity-insights