EXPECTED AND UNEXPECTED DEVELOPMENTS IN QUANTUM COMPUTING

10/4/25

Joke title: Is this whole conference a waste of time?

Samuel Jaques

Rocco Ceselin/Google

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

MAIN QUESTION

When are quantum computers going to break RSA-2048?

That is: when will they vindicate all the research at this conference?

OUTLINE

1. Intro to Quantum computers
2. The “Business as (un)usual” path
3. Possible disruptions to that path

QUANTUM COMPUTERS

A quick introduction

Basics: Qubits

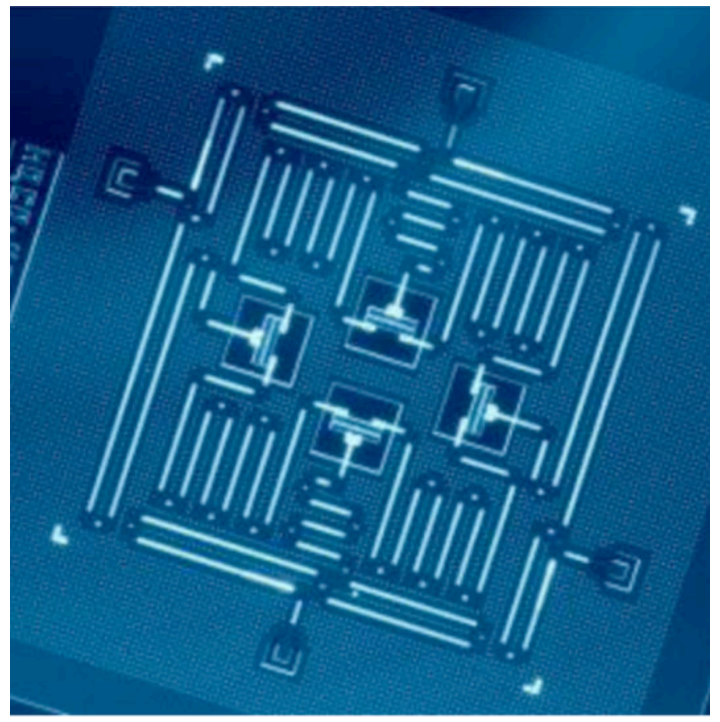
A **qubit** is a device that holds **quantum data**, which can be $|0\rangle$, $|1\rangle$, or any complex linear combination of the two (normalized to 1),

e.g. $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, or $\frac{1}{2}|0\rangle - i\frac{\sqrt{3}}{2}|1\rangle$

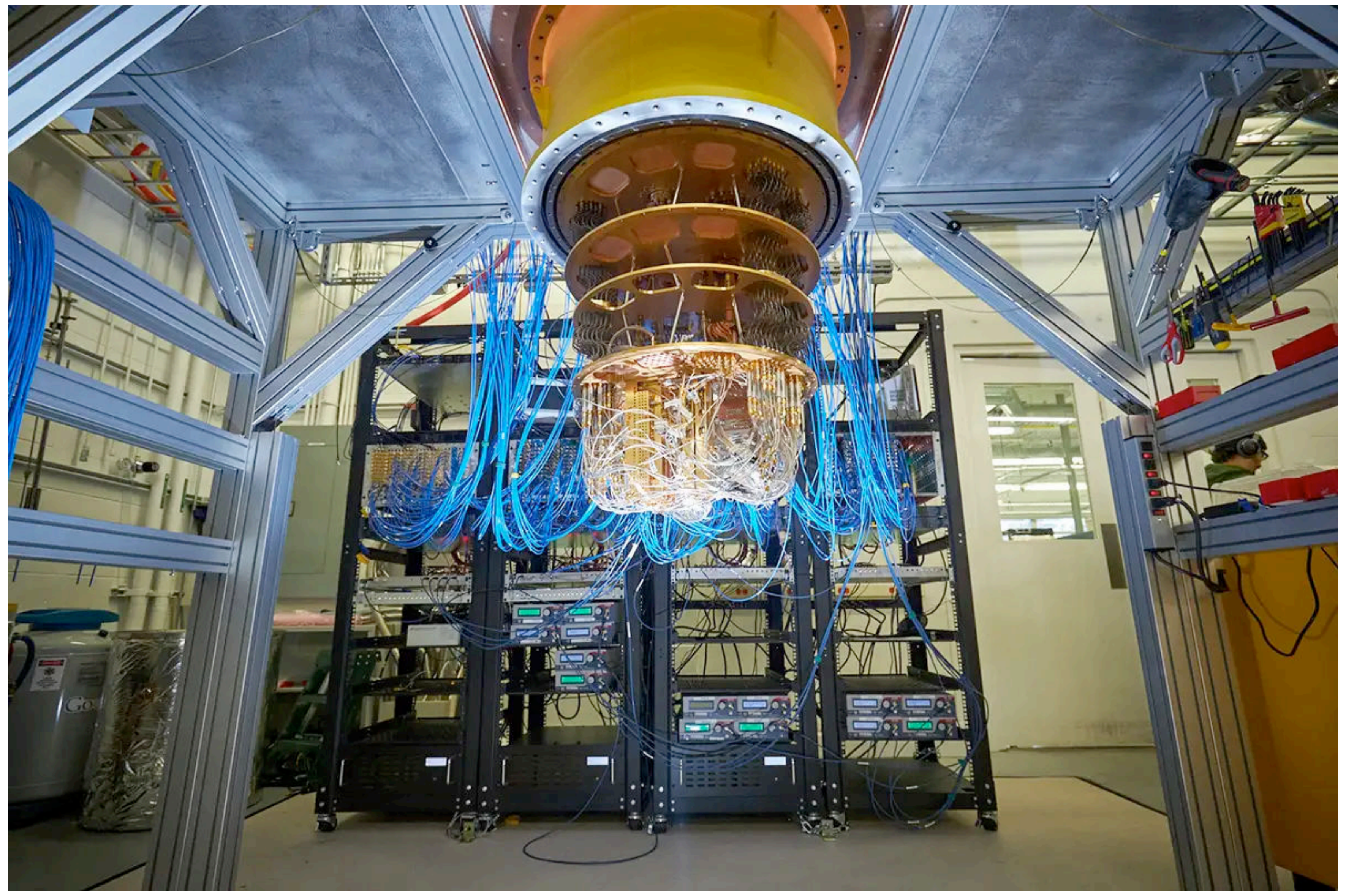
Qubit Types

Any “two-level” quantum system can be a qubit:

Superconducting qubits: A superconducting wire with current flowing in one direction or another



Jay M. Gambetta, Jerry M. Chow, and Matthias Steffen, 2017



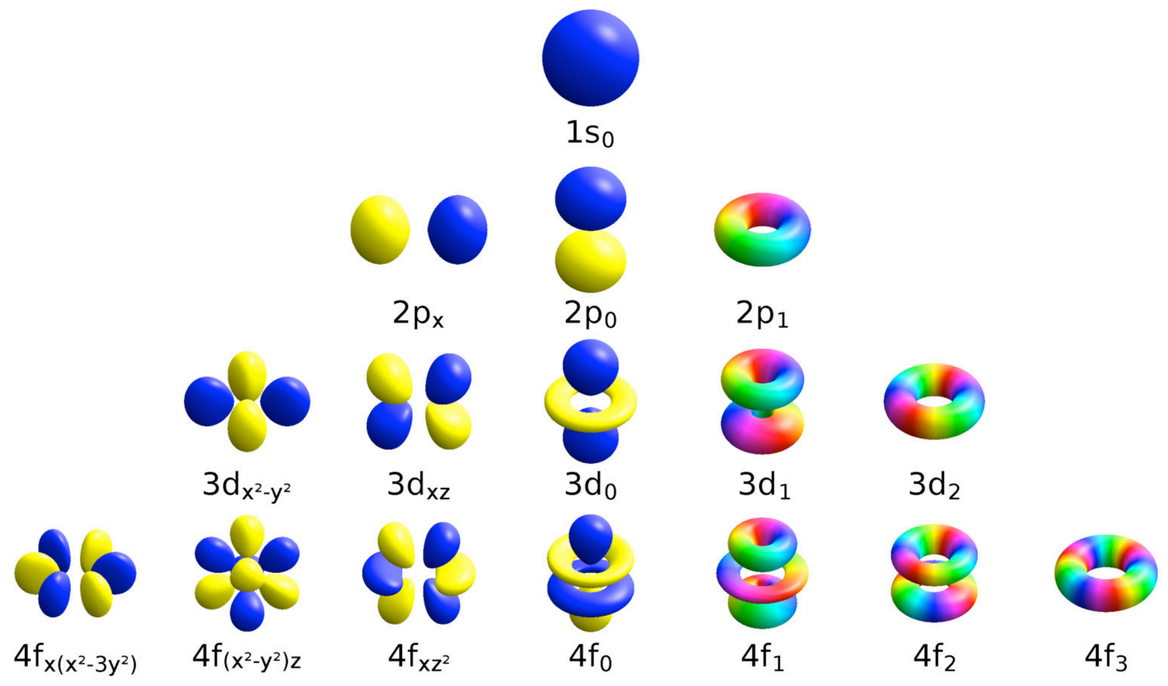
Rocco Ceselin/Google

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

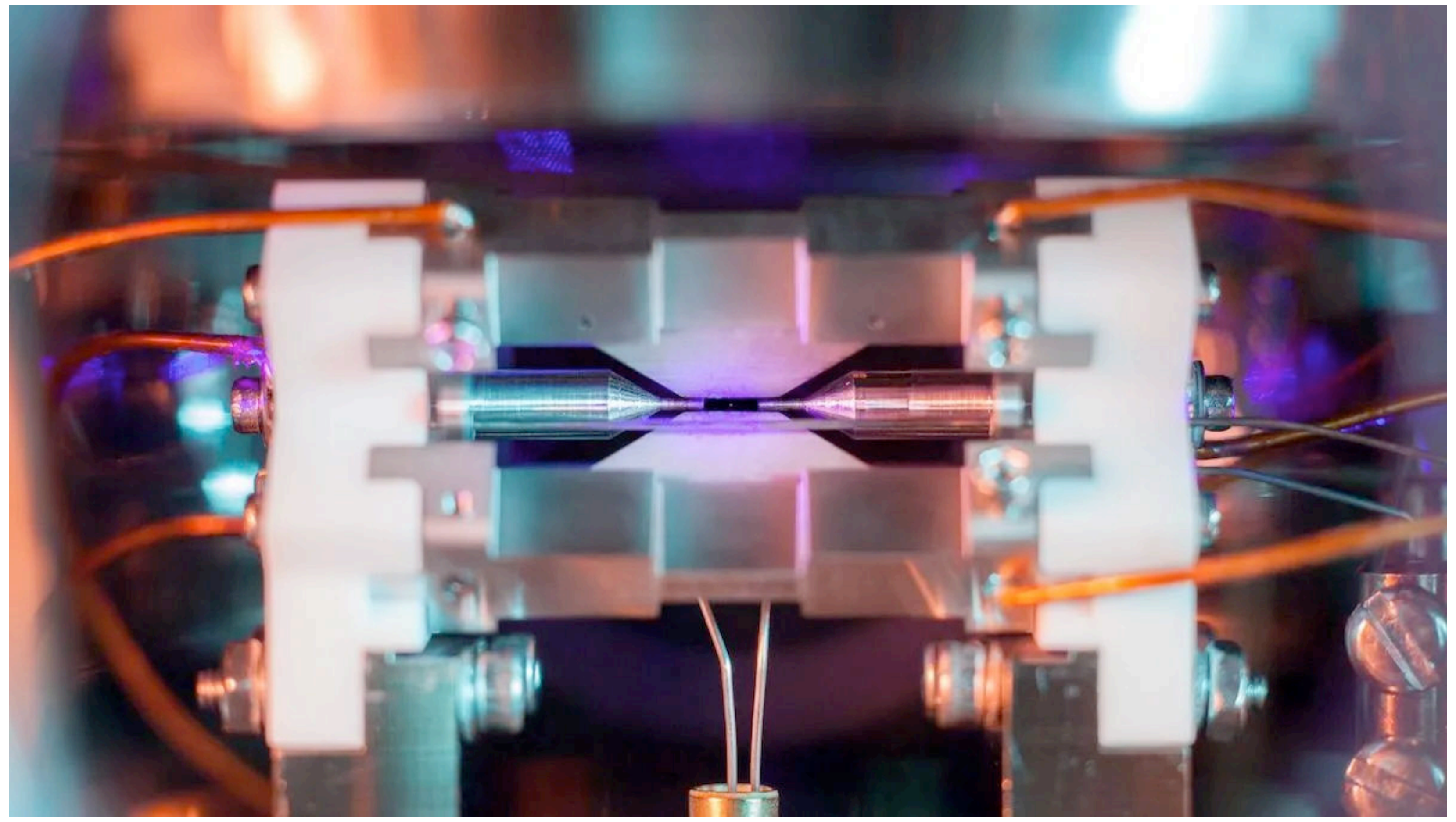
Qubit Types

Any “two-level” quantum system can be a qubit:

Trapped ion qubits: an atom where electrons are either in a high or low energy orbital



Wikipedia user Geek3

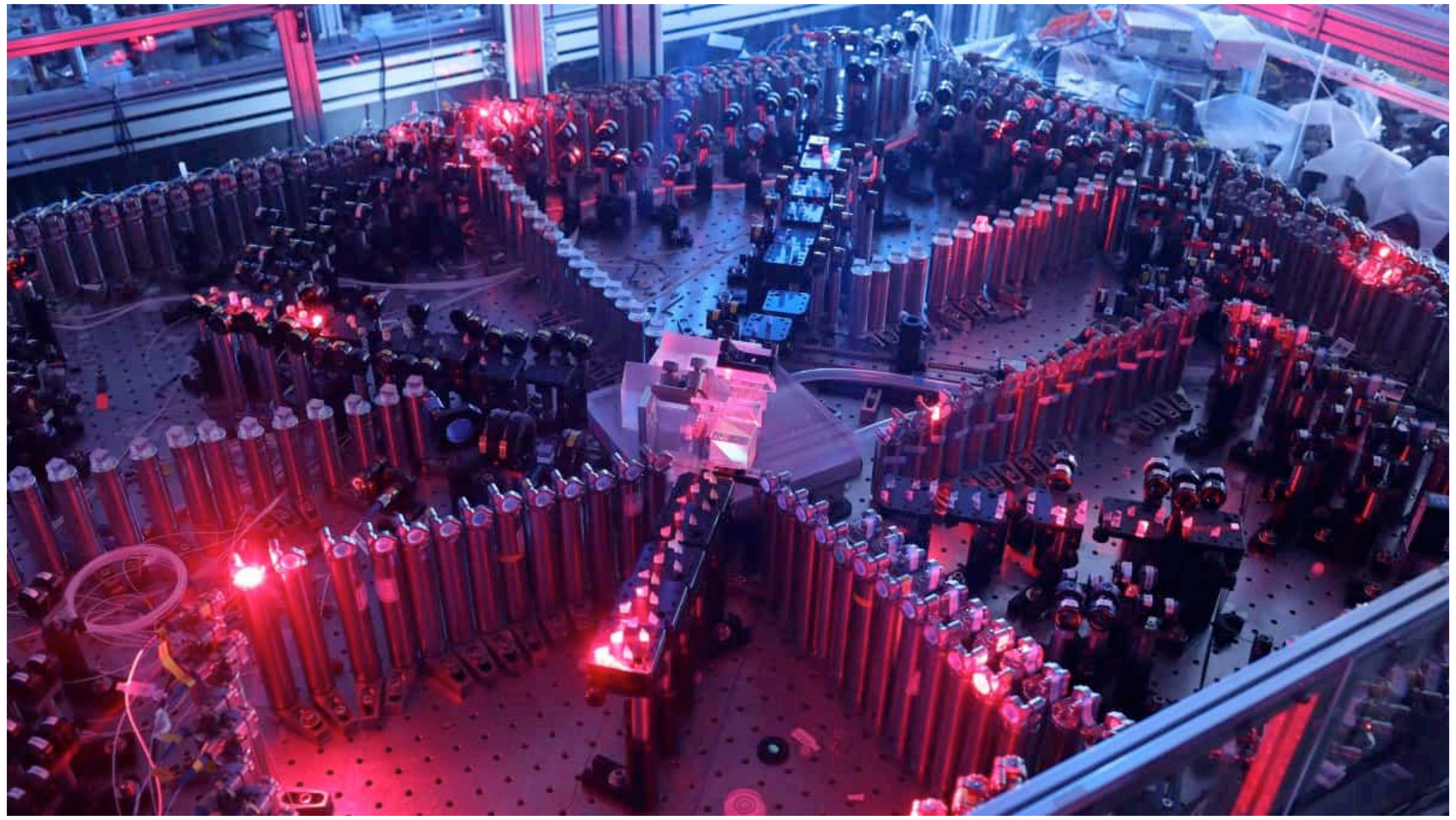


David Nadlinger

Qubit Types

Any "two-level" quantum system can be a qubit:

Photonic qubits: a photon that could be in one of two physical locations (e.g. fibre optic cables)

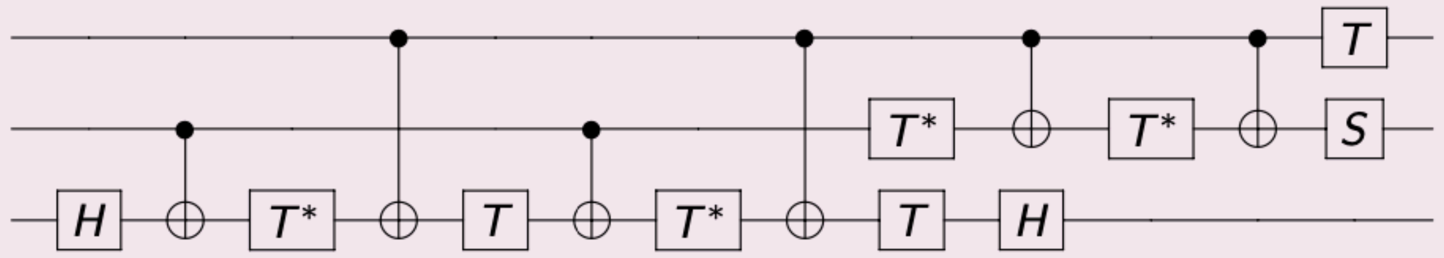


Chao-Yung Lu

Basics: Gates

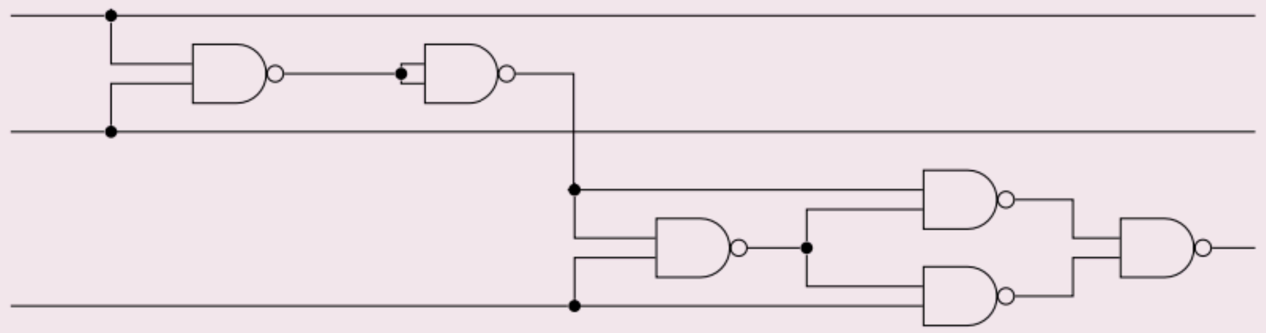
We manipulate the qubits with **gates**, which change the quantum data. Analogous to classical gates, but they are almost always a **process**, not a **device**.

Quantum



Time⟶

Classical

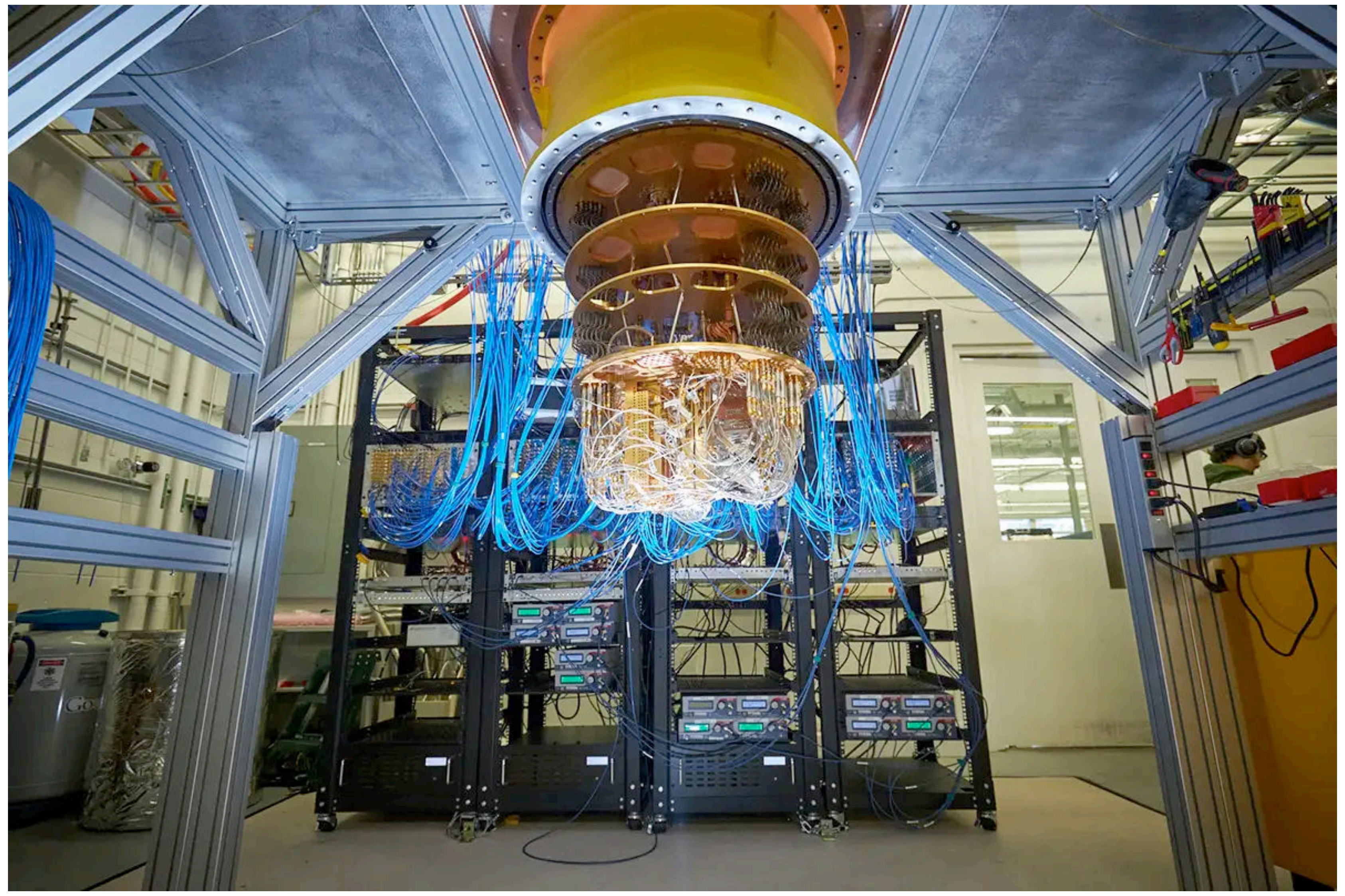


Time/Space⟶

Basics: Noise

Qubits are highly susceptible to noise. Noise is any uncontrolled process which modifies the quantum data.

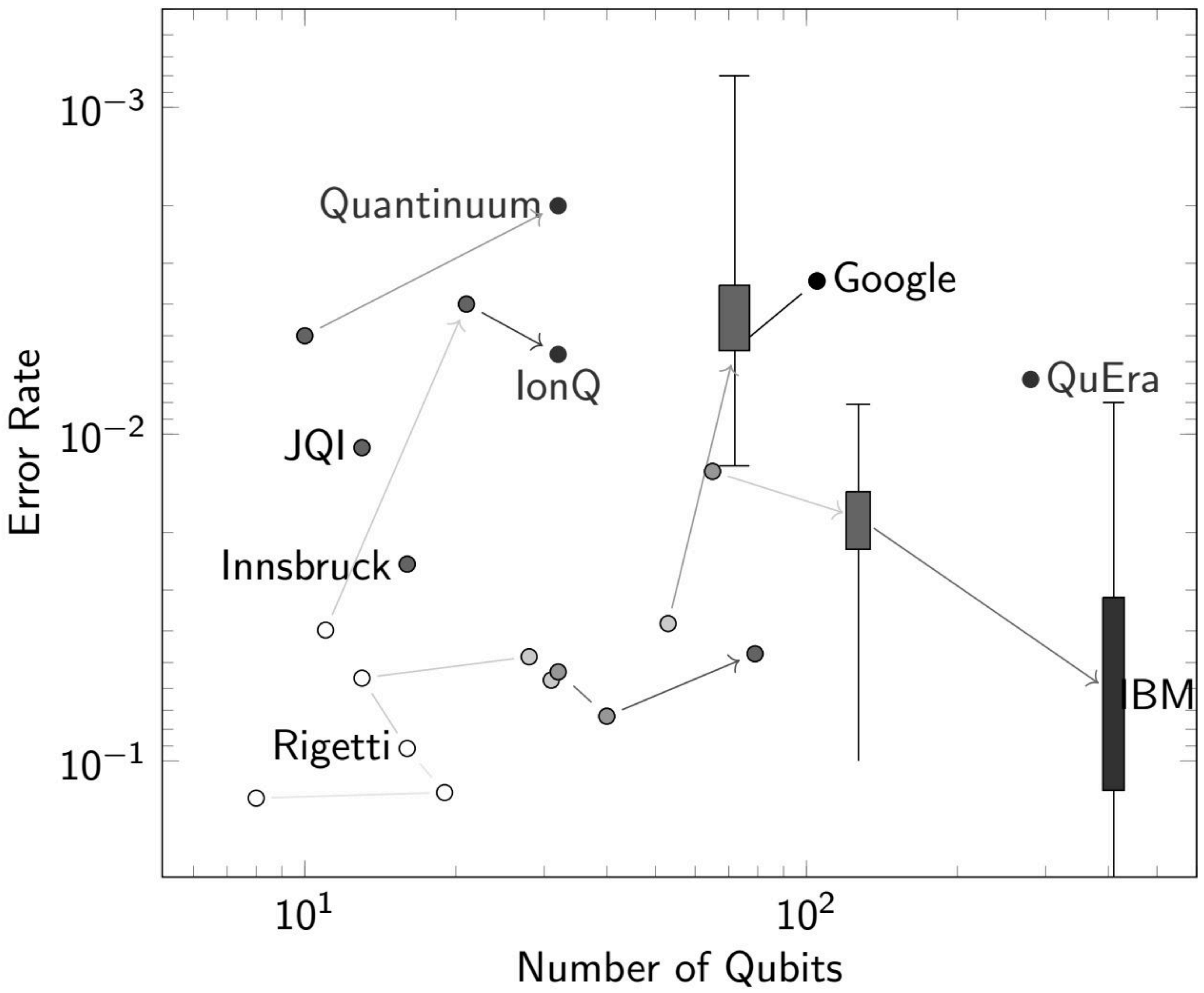
- Classical noise is much easier to deal with: absorbing a small bit of energy won't flip a bit. For qubits, any unwanted interaction causes problems
- Qubits can have "bit flip errors" (similar to classical bit flip) but also "phase flip errors" (no classical analogue) or **any linear combination of the two types**



Rocco Ceselin/Google

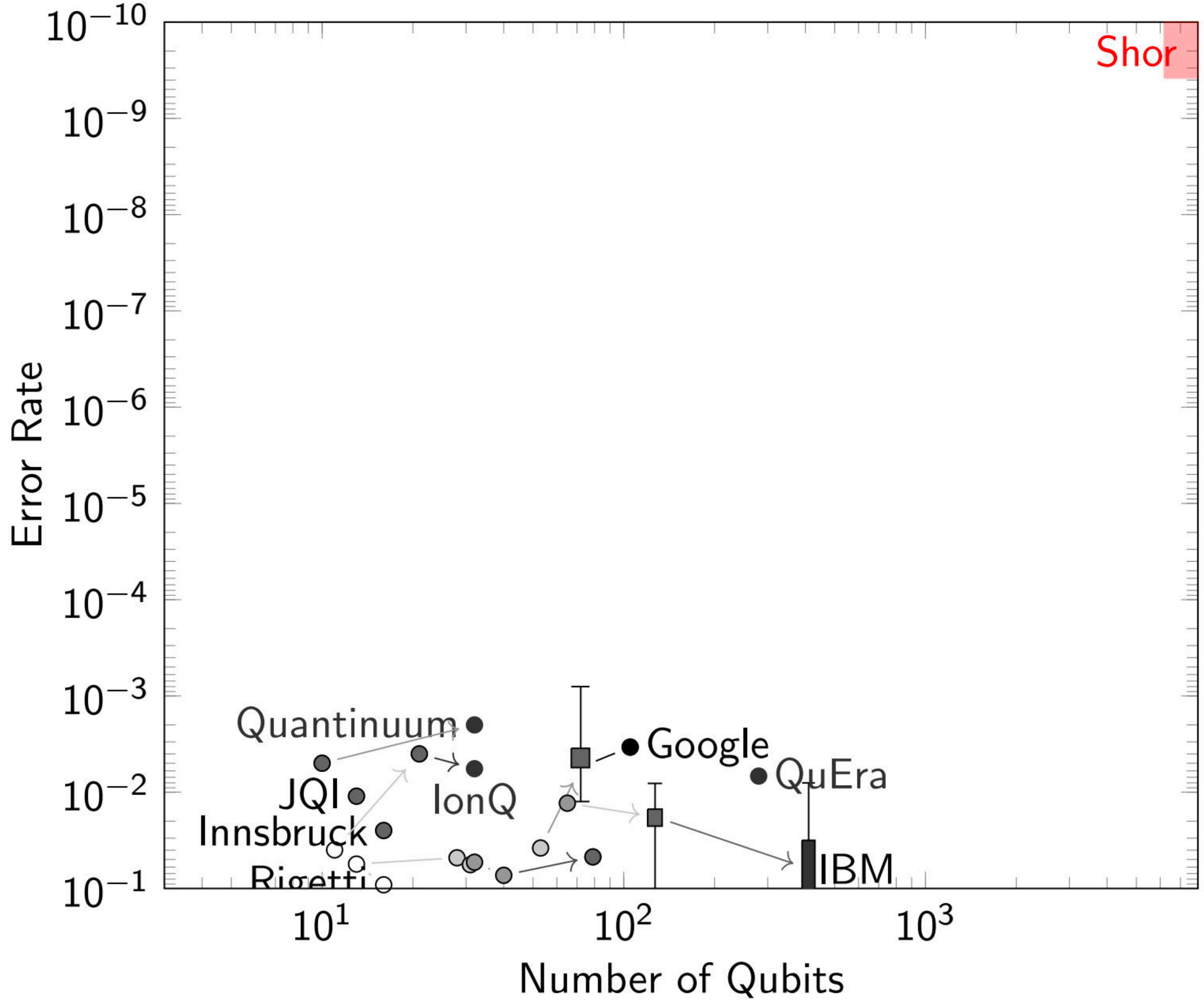
$\lvert 0\rangle \mapsto \lvert 1\rangle$ $\lvert 1\rangle \mapsto \lvert 0\rangle$	
$\lvert 0\rangle \mapsto +\lvert 0\rangle$ $\lvert 1\rangle \mapsto -\lvert 1\rangle$	

Quantum Computing Today



(I had to make dubious assumptions to compress "error rate" to a single number; this is not super precise)

Quantum Computing Today



Error Correcting Codes

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits
  - **Logical qubits**: an abstraction representing the collection of qubits in a code that act like one high-fidelity qubit

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits
  - **Logical qubits**: an abstraction representing the collection of qubits in a code that act like one high-fidelity qubit

Basic assumption:

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits
  - **Logical qubits**: an abstraction representing the collection of qubits in a code that act like one high-fidelity qubit

Basic assumption:
1 qubit with error rates a **billion** times better than today

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits
  - **Logical qubits**: an abstraction representing the collection of qubits in a code that act like one high-fidelity qubit

Basic assumption:
1 qubit with error rates a **billion** times better than today

Is much harder than

Error Correcting Codes

- Quantum error correcting codes are like classical error correcting codes: we protect against noise by encoding the quantum data of one qubit into many qubits
  - **Physical qubits**: physical devices like today's qubits
  - **Logical qubits**: an abstraction representing the collection of qubits in a code that act like one high-fidelity qubit

Basic assumption:
1 qubit with error rates a **billion** times better than today

Is much harder than

1000 qubits with error rates **ten** times better than today

Surface Codes

- Most practical code at the moment
- Uses a 2-dimensional grid of qubits, each connected to its neighbours (easy to build)
- Suppresses errors exponentially in grid width
- Requires repeating cycles of measurement thousands or millions of times per second

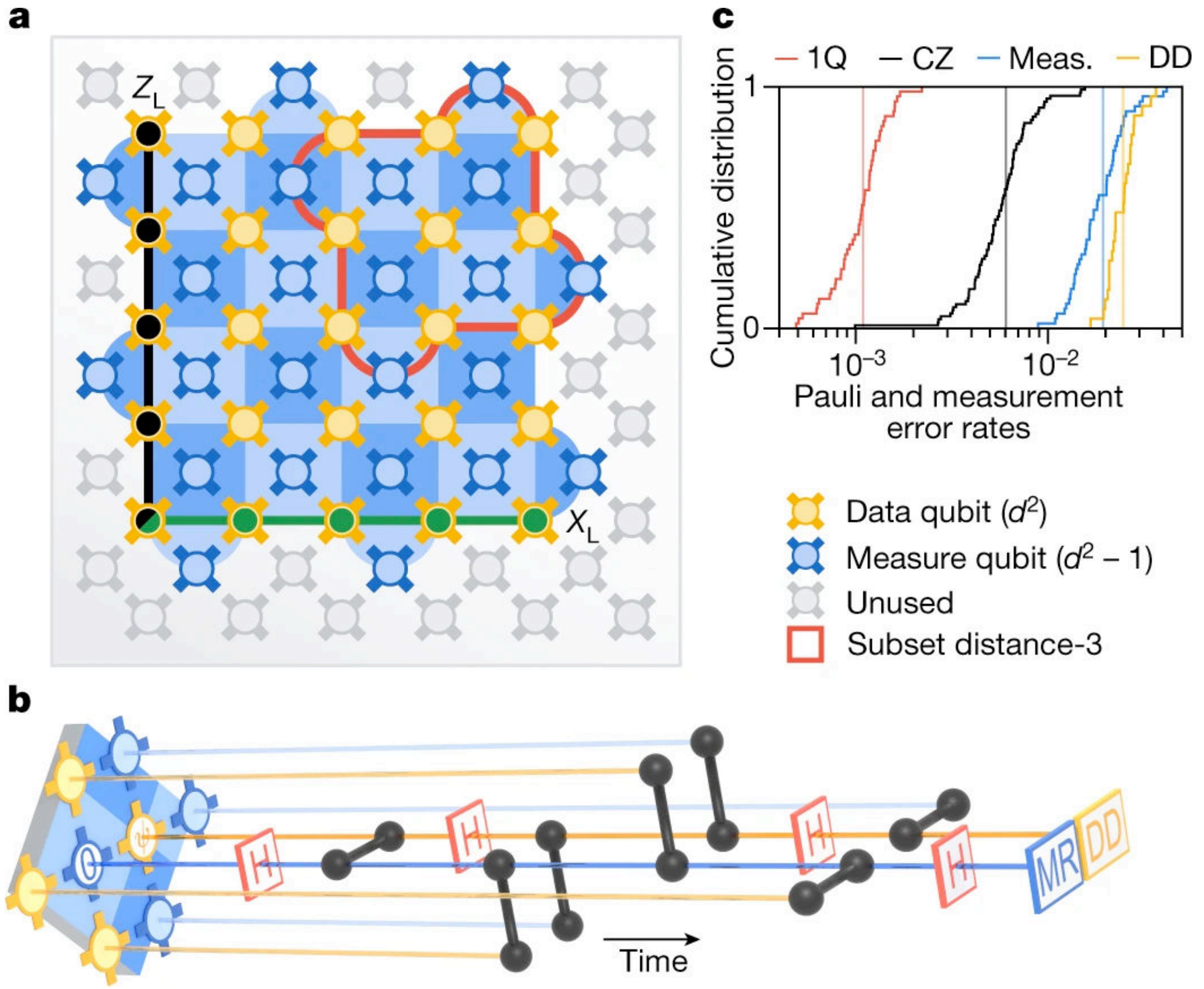


Diagram: Google Quantum AI

Why surface codes?

1. Error detection is fast and simple
2. Physical connectivity is simple (2-d grid of nearest-neighbour connections)
3. We know how to compute on encoded quantum data
4. 1000:1 ratio of physical:logical qubits is good enough
5. Lots of work on optimizing computation in surface codes

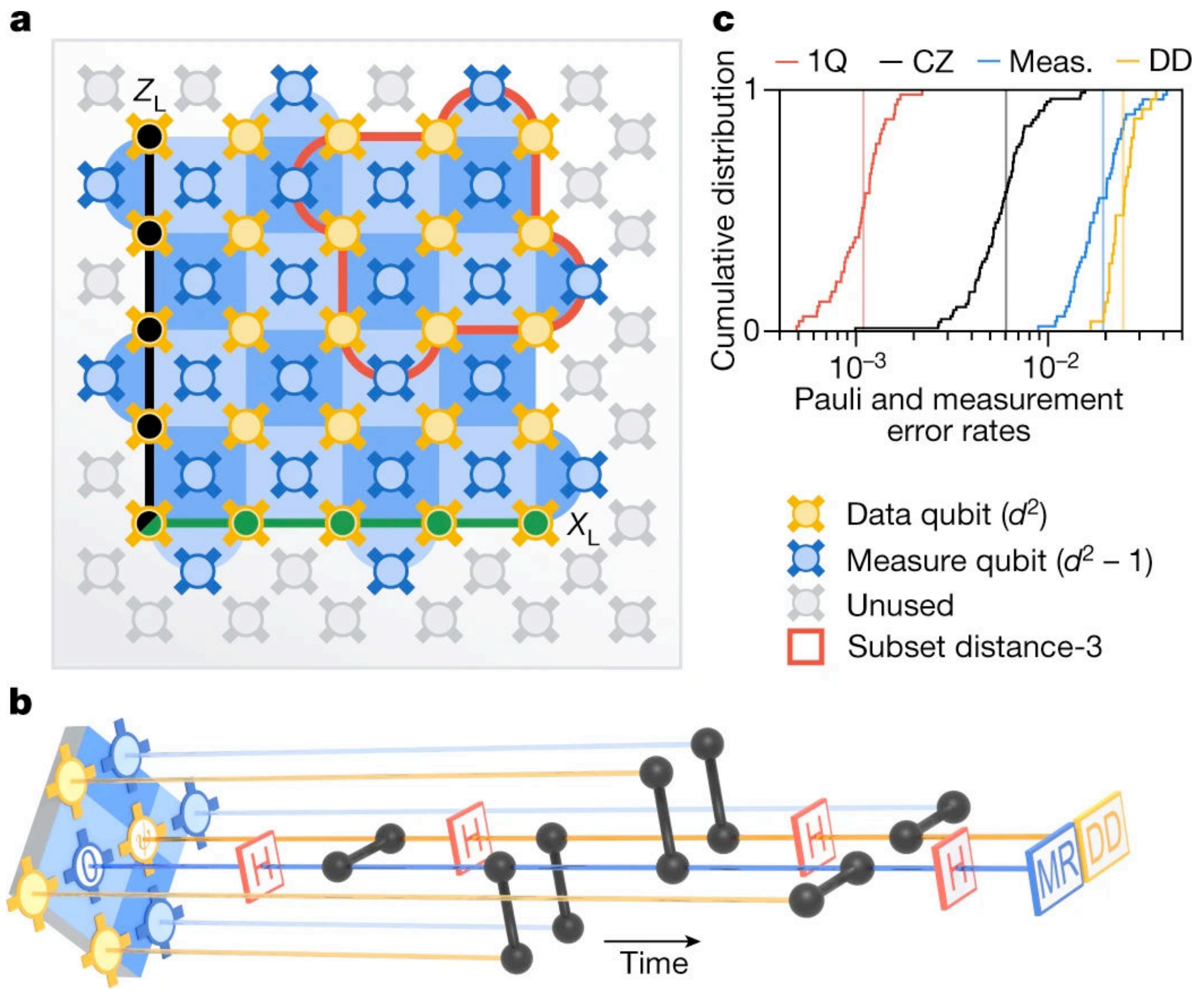
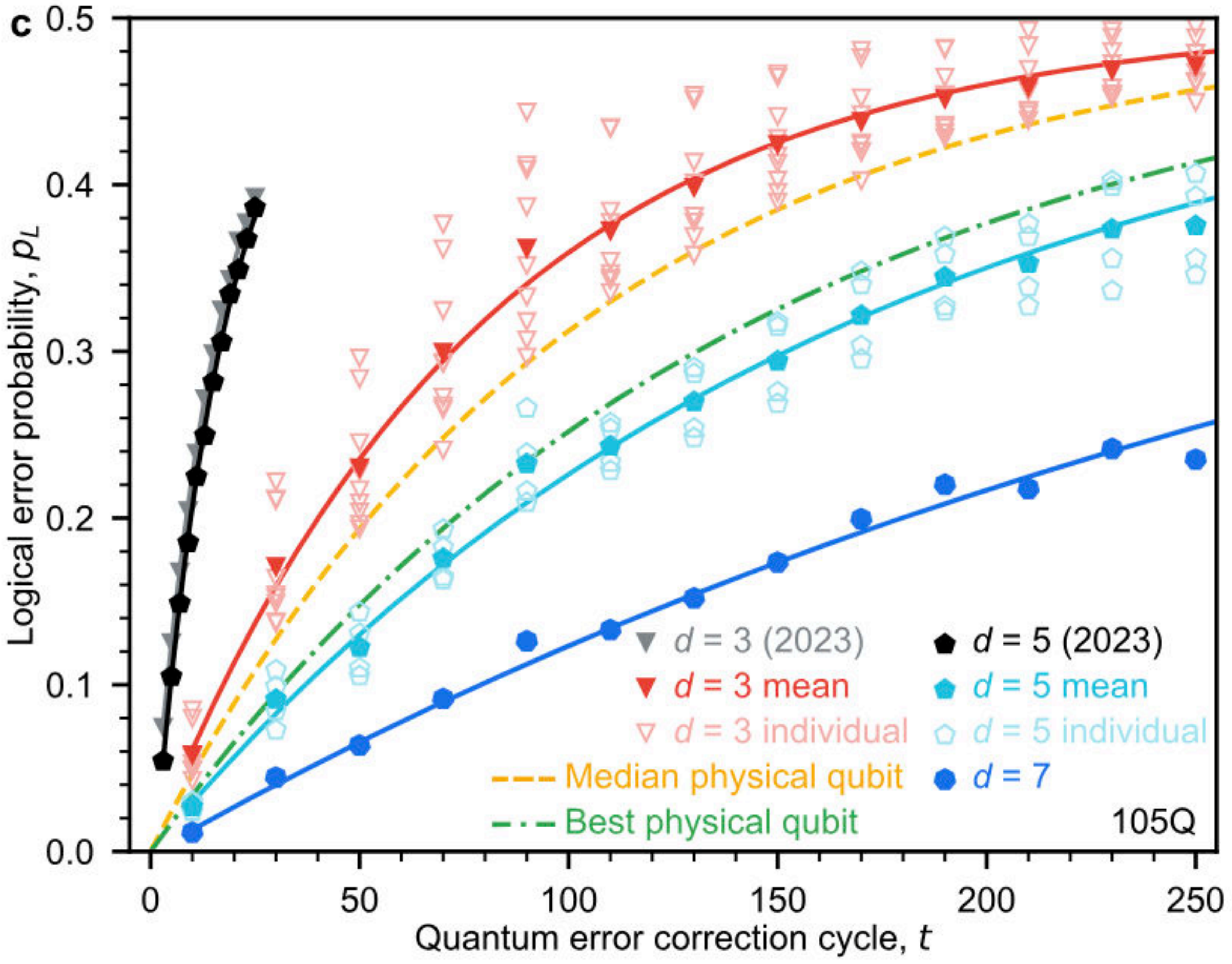


Diagram: Google Quantum AI

Surface codes today



Breakthrough 2024 Experiment from Google Quantum AI:

- Error rate decreases as distance increases
- Logical qubit with smaller errors than physical qubits
- Real-time decoding at 1.1 μs cycle length

Zuchongzhi 3.0: USTC’s Quantum Computer

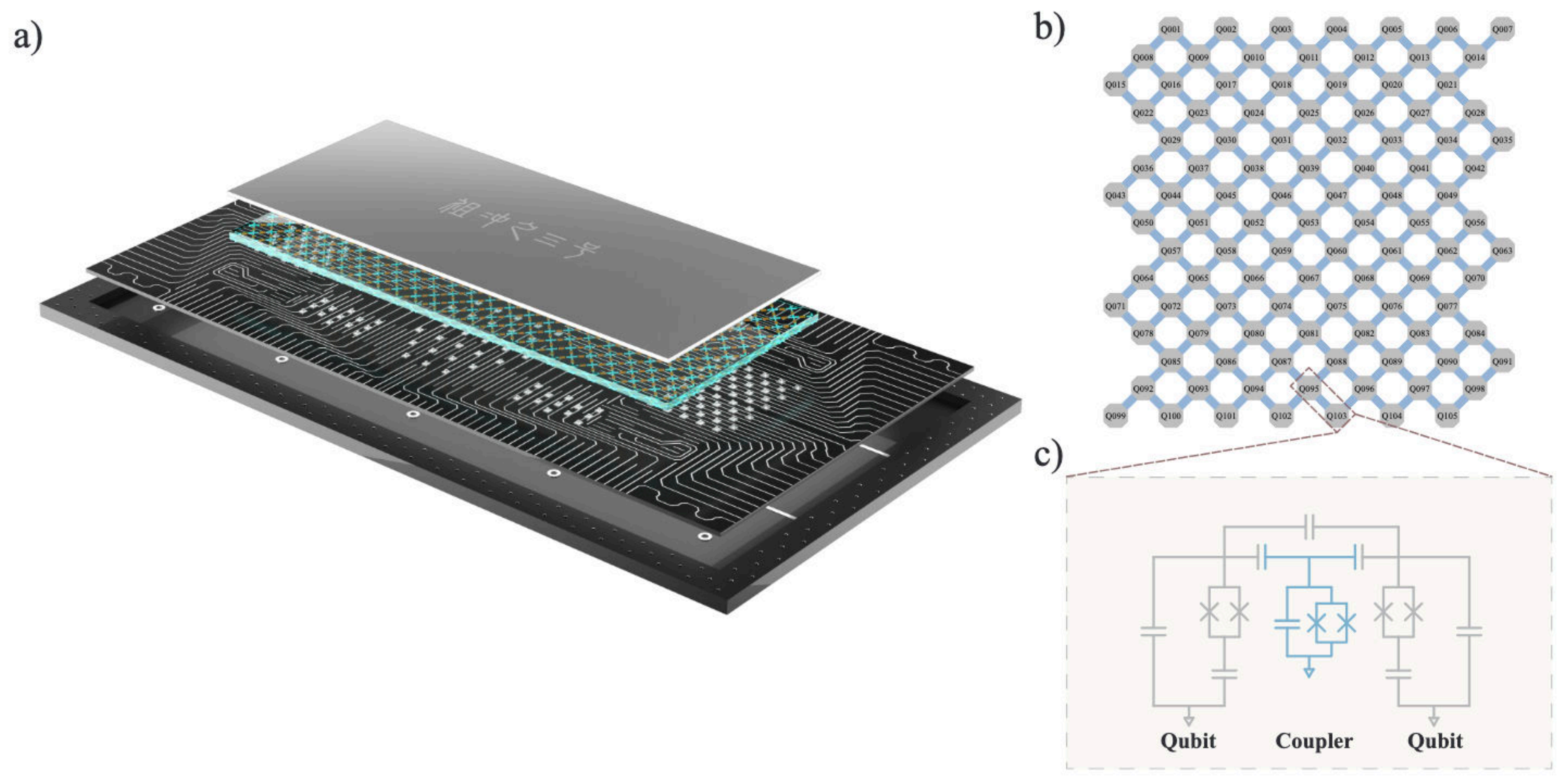
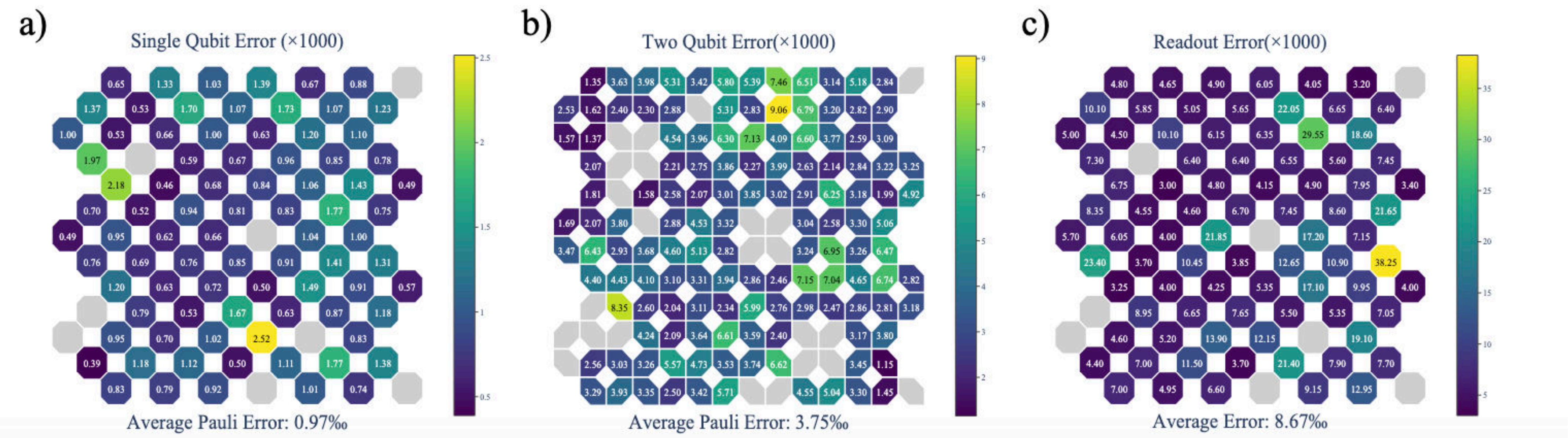
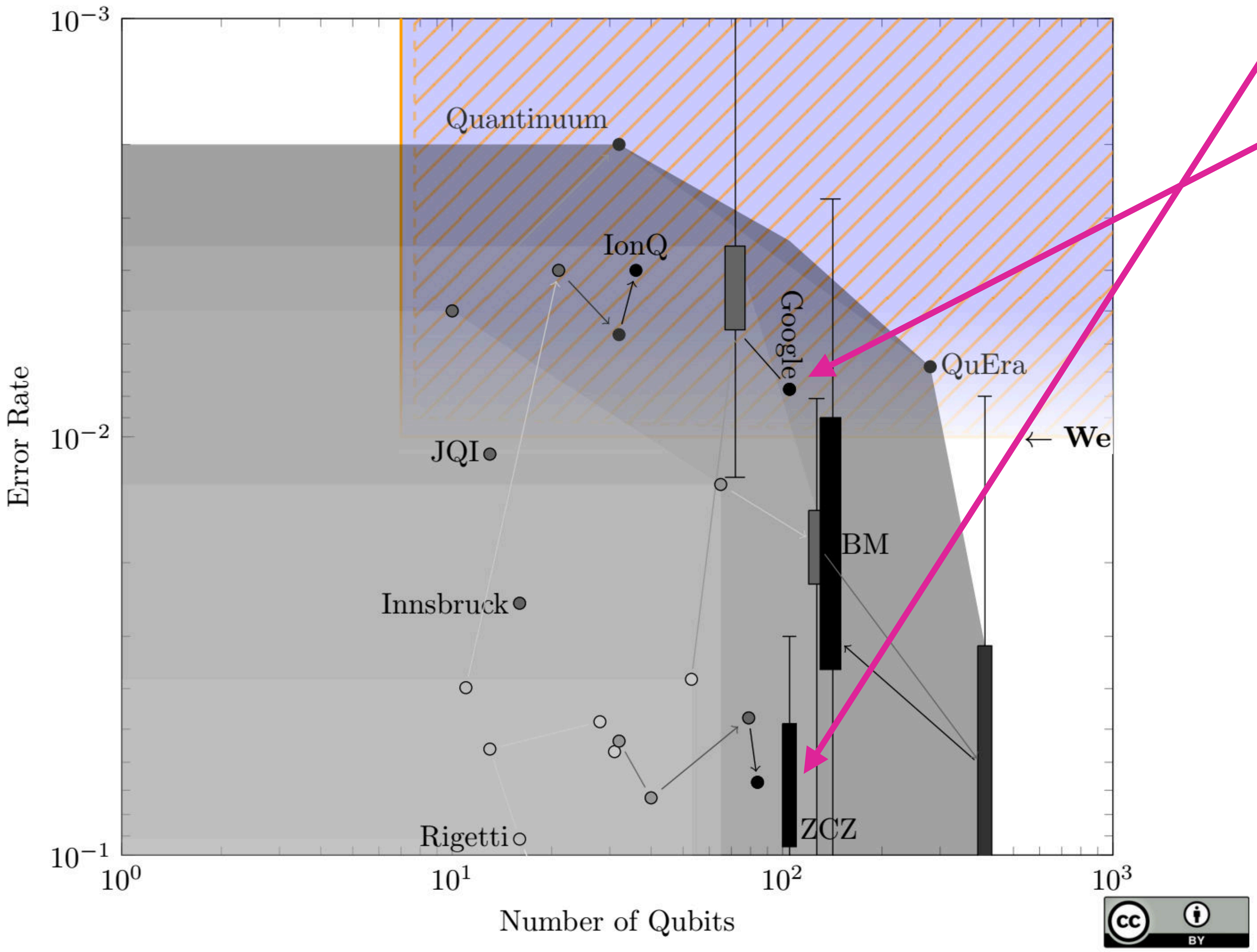


FIG. 1. ***Zuchongzhi* 3.0 quantum processor. a)** The illustration of the *Zuchongzhi* 3.0 quantum processor. The device consists of two sapphire chips integrated using a flip-chip technique. One chip integrates 105 qubits and 182 couplers, while the other is integrated with all the control lines and readout resonators. **b)** The topological diagram of qubits and couplers. Dark gray denotes qubits, light blue denotes couplers. **c)** Simplified circuit schematic of two qubits coupled via a coupler.



- From the abstract: “Our experiments with an 83-qubit, **32-cycle random circuit sampling** on Zuchongzhi 3.0 highlight its superior performance, achieving one million samples in just a few hundred seconds. This task is estimated to be infeasible on the most powerful classical supercomputers, Frontier, which would require approximately 6.4 × 109 years to replicate the task. This leap in processing power places the classical simulation cost six orders of magnitude beyond Google’s SYC-67 and SYC-70 experiments [Nature 634, 328 (2024)], firmly establishing a new benchmark in quantum computational advantage.”

Zuchongzhi 3.0: USTC's Quantum Computer



- ZuChongZhi 3.0 is a superconducting processor (like Google's "Willow")
- Not doing error correction
- Random circuit sampling is impressive but useless

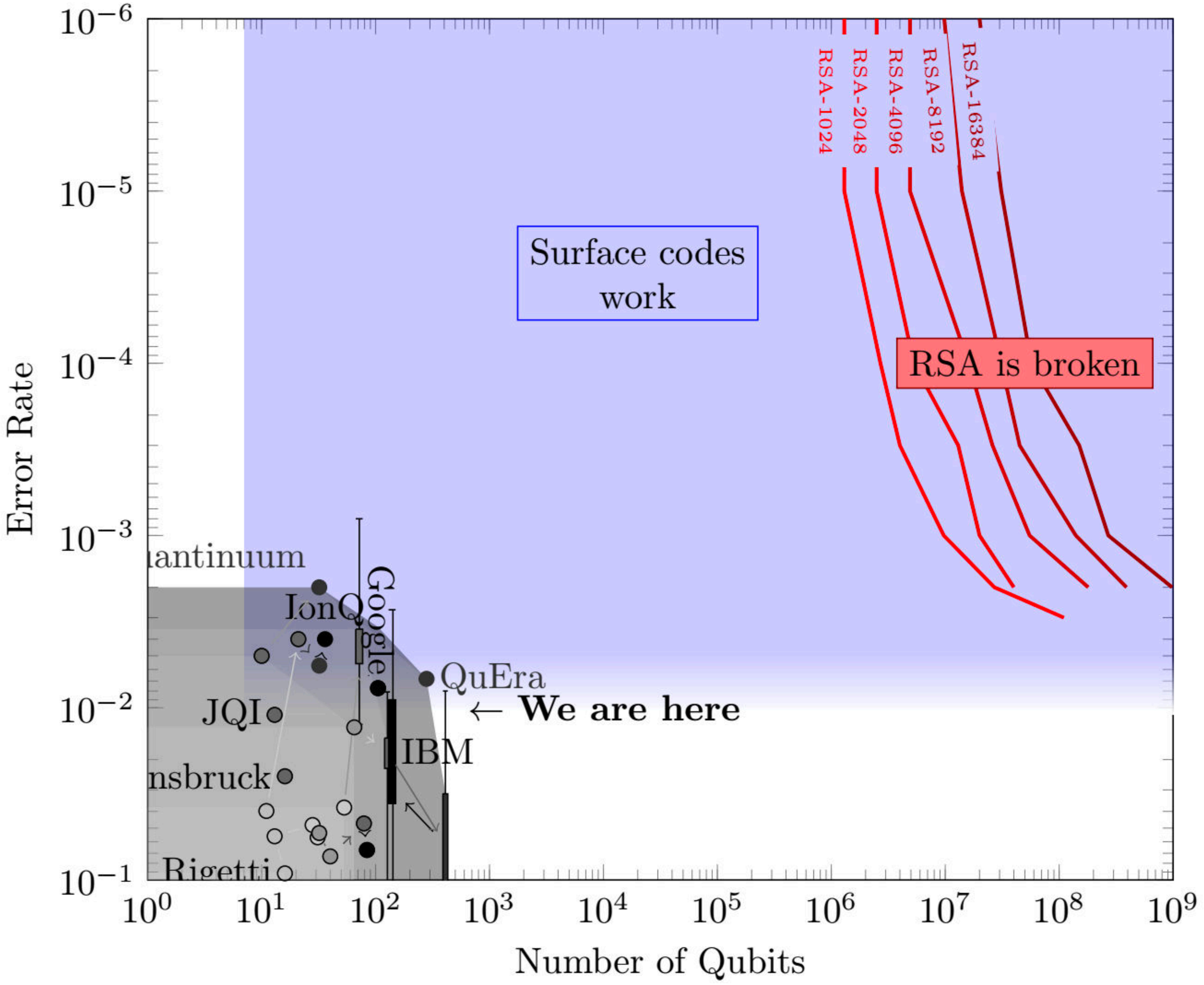
UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

“Business As Usual” Path

1. Superconducting qubits get a bit better
2. The number of these qubits grows exponentially
3. Someone builds enough to factor (roughly 20 million) and we factor

- Engineering challenges:
  - The 200,000x increase in qubit counts
  - Dealing with massive error data throughput (100+ GB/second)
  - Real-time error correction
  - Building a large enough dilution fridge (or connections between fridges)
  - Cosmic rays and other unexpected error events
  - Other unknown challenges?
- For now assume these challenges are solved as they come up

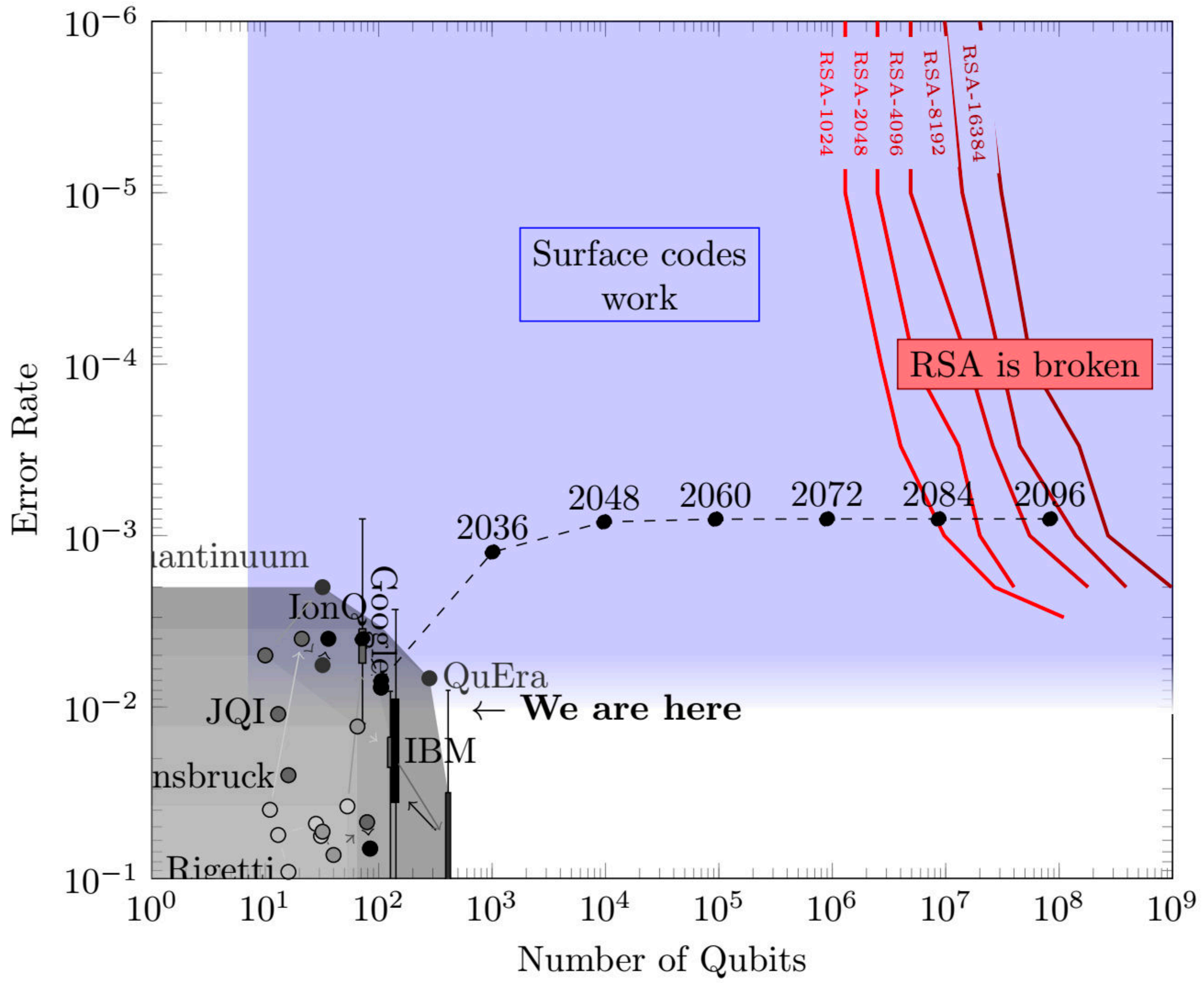
Time-to-break RSA: “Business as usual”



Google went from 72 qubits in 2022 to 105 in 2024
-> 45% increase in 2 years

At that rate…

Time-to-break RSA: “Business as usual”



Google went from 72 qubits in 2022 to 105 in 2024
-> 45% increase in 2 years

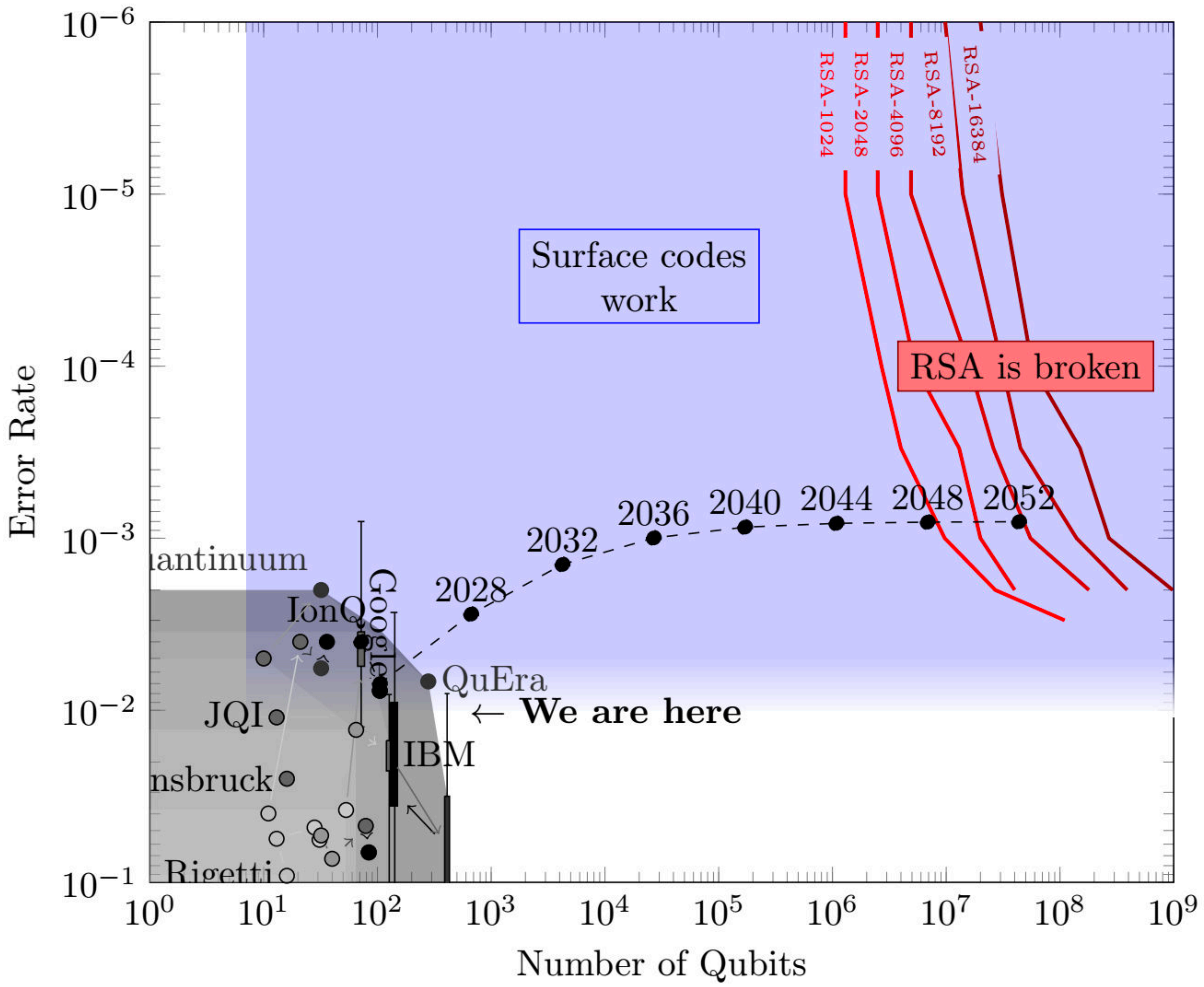
At that rate…

… RSA 2048 breaks in **2088**

(Assuming physical error stalls at about 0.1%)

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Time-to-break RSA: "Business as usual"



To give them credit: they improved a lot of other factors in that 45% qubit increase.

What if quantum computers grow like Moore's law*, doubling qubits every 1.5 years?

RSA-2048 breaks in **2052**

*up to technicalities in Moore's law

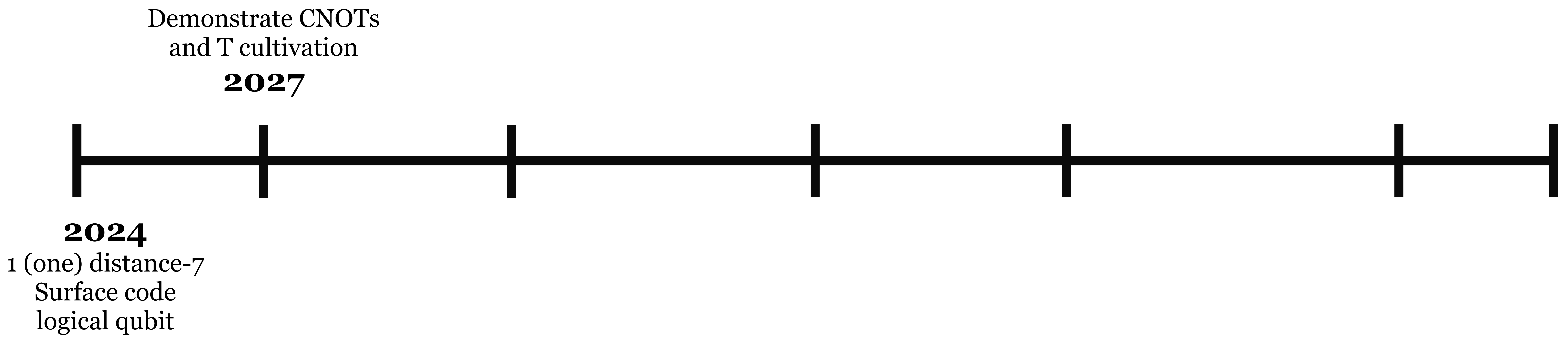
Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:

2024
1 (one) distance-7
Surface code
logical qubit

Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:



Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:

2024
1 (one) distance-7
Surface code
logical qubit

2027
Demonstrate CNOTs
and T cultivation

2032
More and better logical
qubits than we currently
have physical qubits

Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:

Demonstrate CNOTs
and T cultivation
2027

Quantum
computers can
factor 77
2032

2024
1 (one) distance-7
Surface code
logical qubit

2032
More and better logical
qubits than we currently
have physical qubits

Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:

Demonstrate CNOTs and T cultivation
2027

Quantum computers can factor 77
2032

2024
1 (one) distance-7 Surface code logical qubit

2032
More and better logical qubits than we currently have physical qubits

2038
(Halfway)

Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:

2024
1 (one) distance-7 Surface code logical qubit

Demonstrate CNOTs and T cultivation
2027

Quantum computers can factor 77
2032

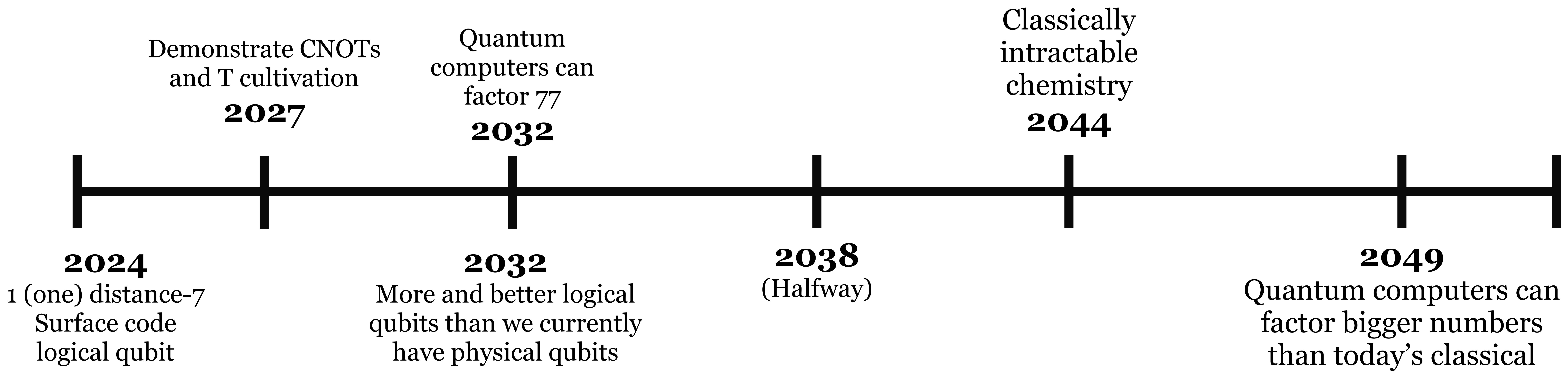
2032
More and better logical qubits than we currently have physical qubits

2038
(Halfway)

Classically intractable chemistry
2044

Milestones

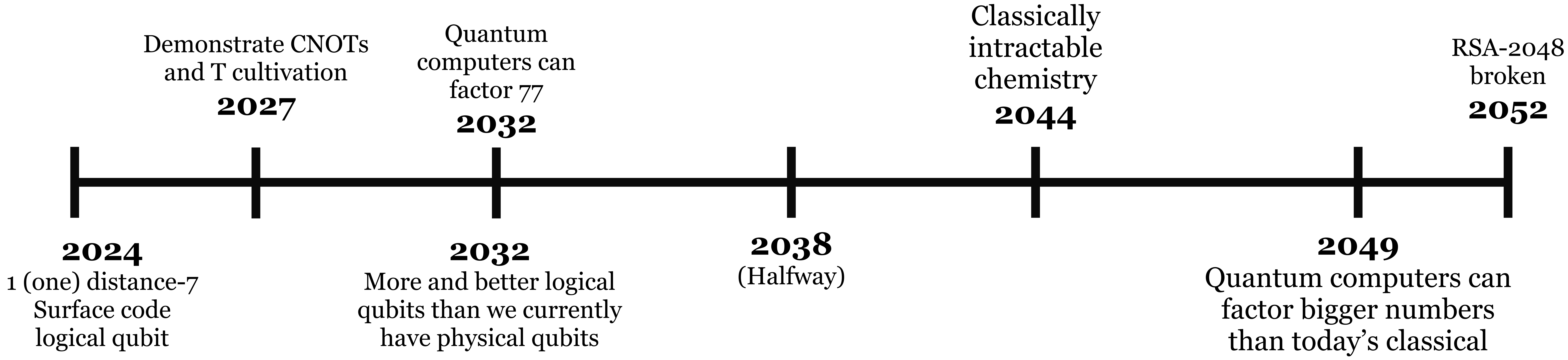
Assume qubits double every 1.5 years and error rate approaches 10^-3:



UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Milestones

Assume qubits double every 1.5 years and error rate approaches 10^-3:



Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael McDc Bohd Feldk Krish Naray Smul Tsun

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

Tra rat pro two up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

This code is not a surface code! It will not scale well!

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael McDc Bohd Feldk Krish Naray Smul Tsun

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

Tra rat prc twc up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

This code is not a surface code! It will not scale well!

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael McDc Bohd Feldk Krish Naray Smul Tsun

Tra rat prc twc

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

This code is not a surface code! It will not scale well!

(Everyone seems to do this now, sorry to pick on Microsoft)

Watch out! Not all logical qubits are created equal

arXiv > quant-ph > arXiv:2411.11822

Search...

Help | Adv

Quantum Physics

[Submitted on 18 Nov 2024 (v1), last revised 19 Nov 2024 (this version, v2)]

Logical computation demonstrated with a neutral atom quantum processor

Ben W. Reichardt, Adam Paetznick, David Aasen, Ivan Basov, Juan M. Bello-Rivas, Parsa Bonderson, Rui Chao, Wim van Dam, Matthew B. Hastings, Andres Paz, Marcus P. da Silva, Aarthi Sundaram, Krysta M. Svore, Alexander Vaschillo, Zhenghan Wang, Matt Zanner, William B. Cairncross, Cheng-An Chen, Daniel Crow, Hyosub Kim, Jonathan M. Kindem, Jonathan King, Michael

qubits using the distance-two [[4,2,2]] code, simultaneously detecting errors and correcting for lost qubits. We also implement the Bernstein-Vazirani algorithm with up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum

up to 28 logical qubits encoded in the [[4,1,2]] code, showing better-than-physical error rates. We demonstrate fault-tolerant quantum computation in our approach, guided by the proposal of Gottesman (2016), by performing repeated loss correction for both structured and random circuits encoded in the [[4,2,2]] code. Finally, since distance-two codes can correct qubit loss, but not other errors, we show repeated loss and error correction using the distance-three [[9,1,3]] Bacon-Shor code. These results begin to clear a path for achieving scientific quantum advantage with a programmable neutral atom quantum processor.

I just said the best was 1 logical qubit!?

This code is not a surface code! It will not scale well!

(Everyone seems to do this now, sorry to pick on Microsoft)

Changing The Timeline

Assume qubits double every 1.5 years and error rate approaches 10^-3:

2024
1 (one) distance-7 Surface code logical qubit

Demonstrate CNOTs and T cultivation
2027

Quantum computers can factor 77
2032

2032
More and better logical qubits than we currently have physical qubits

2038
(Halfway)

Classically intractable chemistry
2044

2049
Quantum computers can factor bigger numbers than today's classical

RSA-2048 broken
2052

Changing The Timeline

Assume qubits double every 1.5 years and error rate approaches 10^-3:

2024
1 (one) distance-7 Surface code logical qubit

Demonstrate CNOTs and T cultivation
2027

Quantum computers can factor 77
2032

2032
More and better logical qubits than we currently have physical qubits

2038
(Halfway)

2041
BSI predicts quantum computers can break RSA-2048

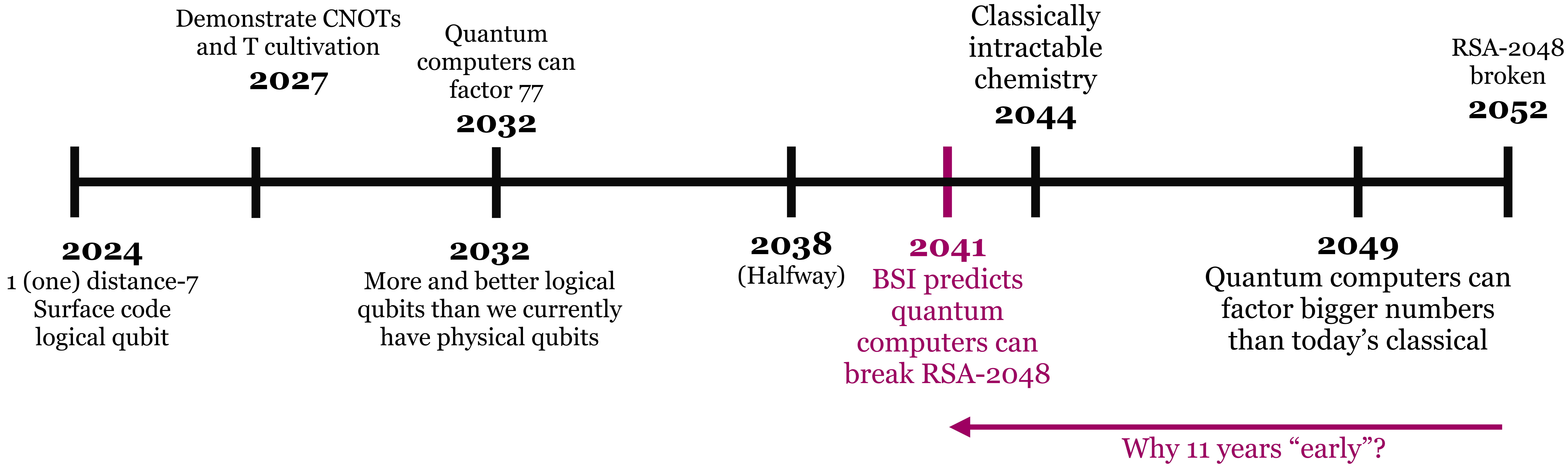
Classically intractable chemistry
2044

2049
Quantum computers can factor bigger numbers than today's classical

RSA-2048 broken
2052

Changing The Timeline

Assume qubits double every 1.5 years and error rate approaches 10^-3:

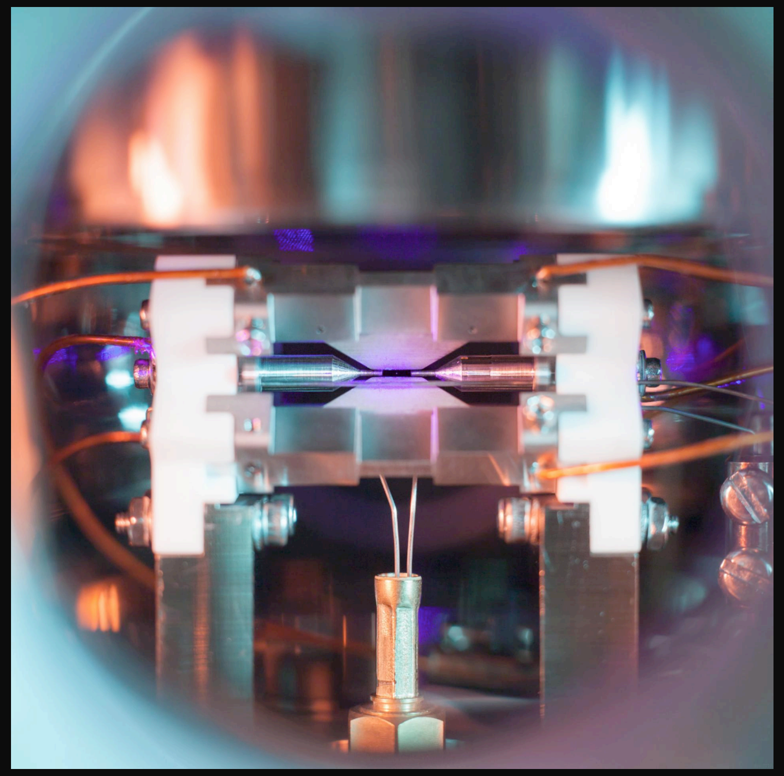


CHANGING THE TIMELINE

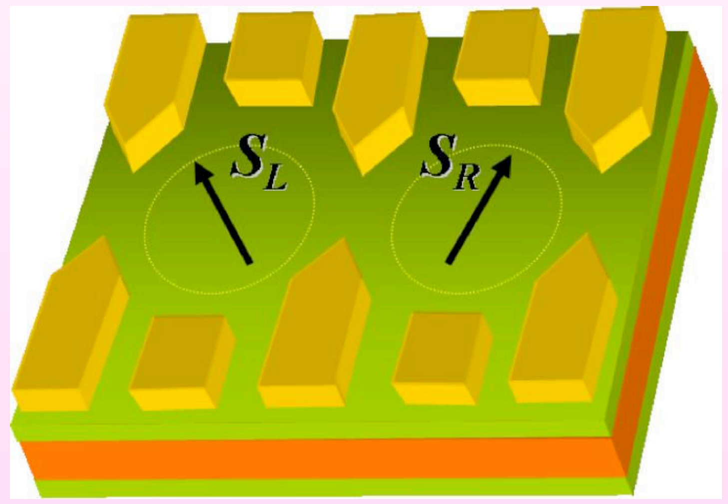
1. Better hardware
2. Better codes
3. Better algorithms
4. Better implementations

1. Better Hardware

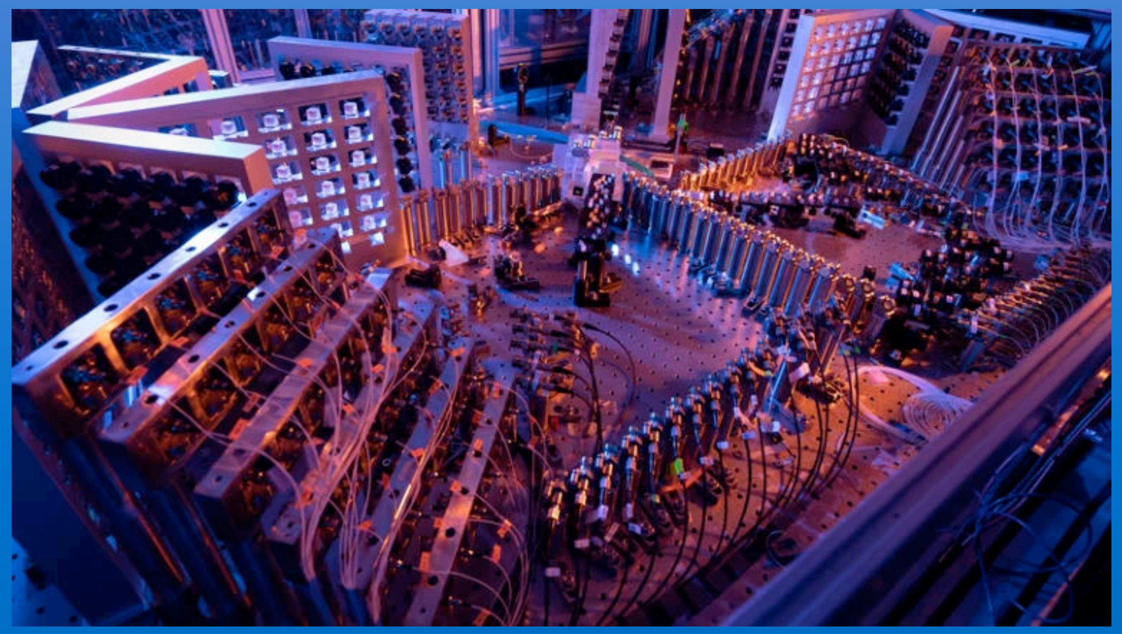
Are superconducting qubits the "transistor" or the "vacuum tube"?



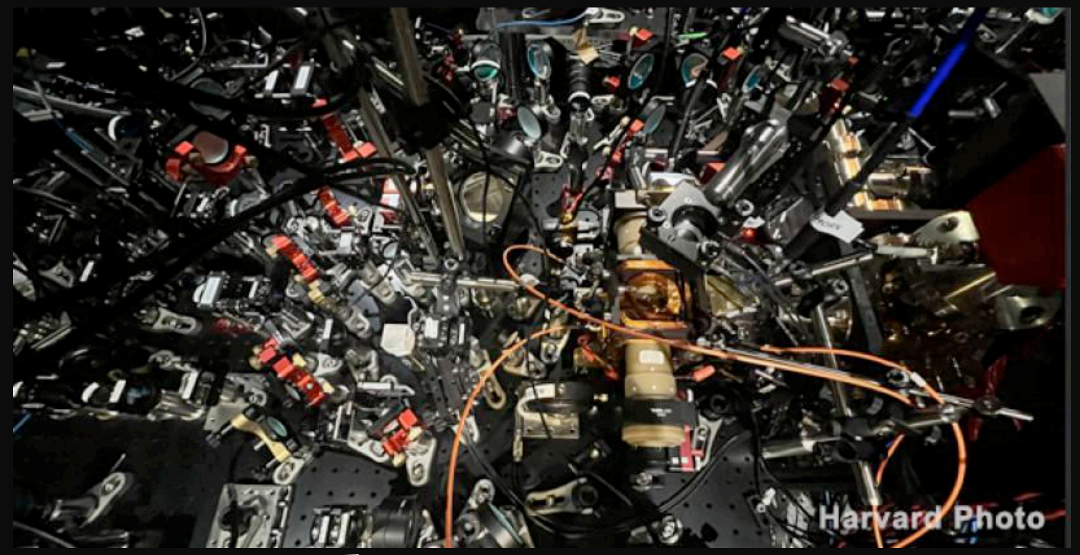
Trapped Ions
Photo: David Nadlinger



Silicon
Diagram: Vitaly Golovach



Photonics
Photo: Chao-Yang Lu



Neutral Atom Arrays
Photo: Harvard photos

It's still early days!

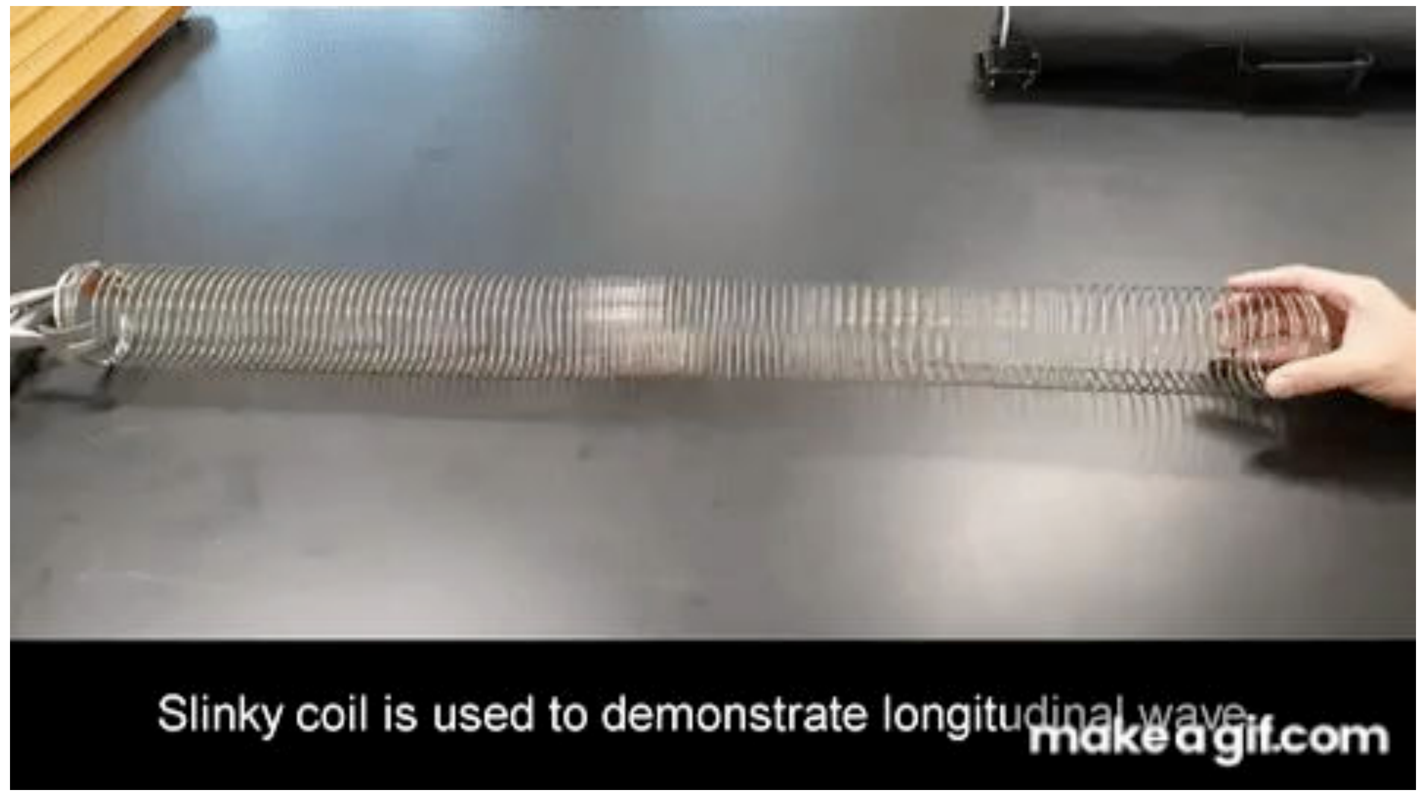
Topological Qubits

Idea: build a device where the qubit uses “Majorana quasiparticles” which are inherently stable against noise

Rough idea: A “quasiparticle” is when many particles interact in way that looks mathematically like another particle

E.g.: waves on water

Majorana quasiparticles involve many “real” particles so a lot of the real particles must suffer noise to cause noise in the quasiparticle



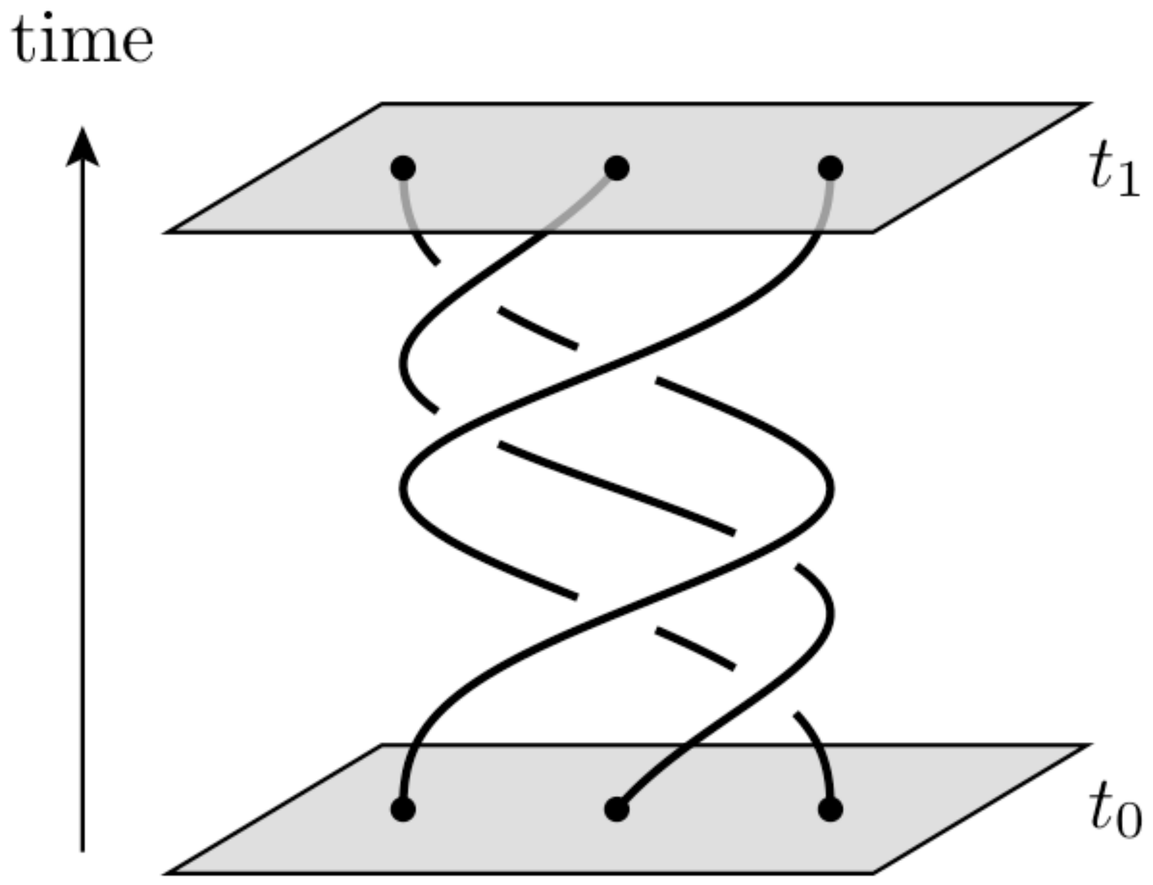


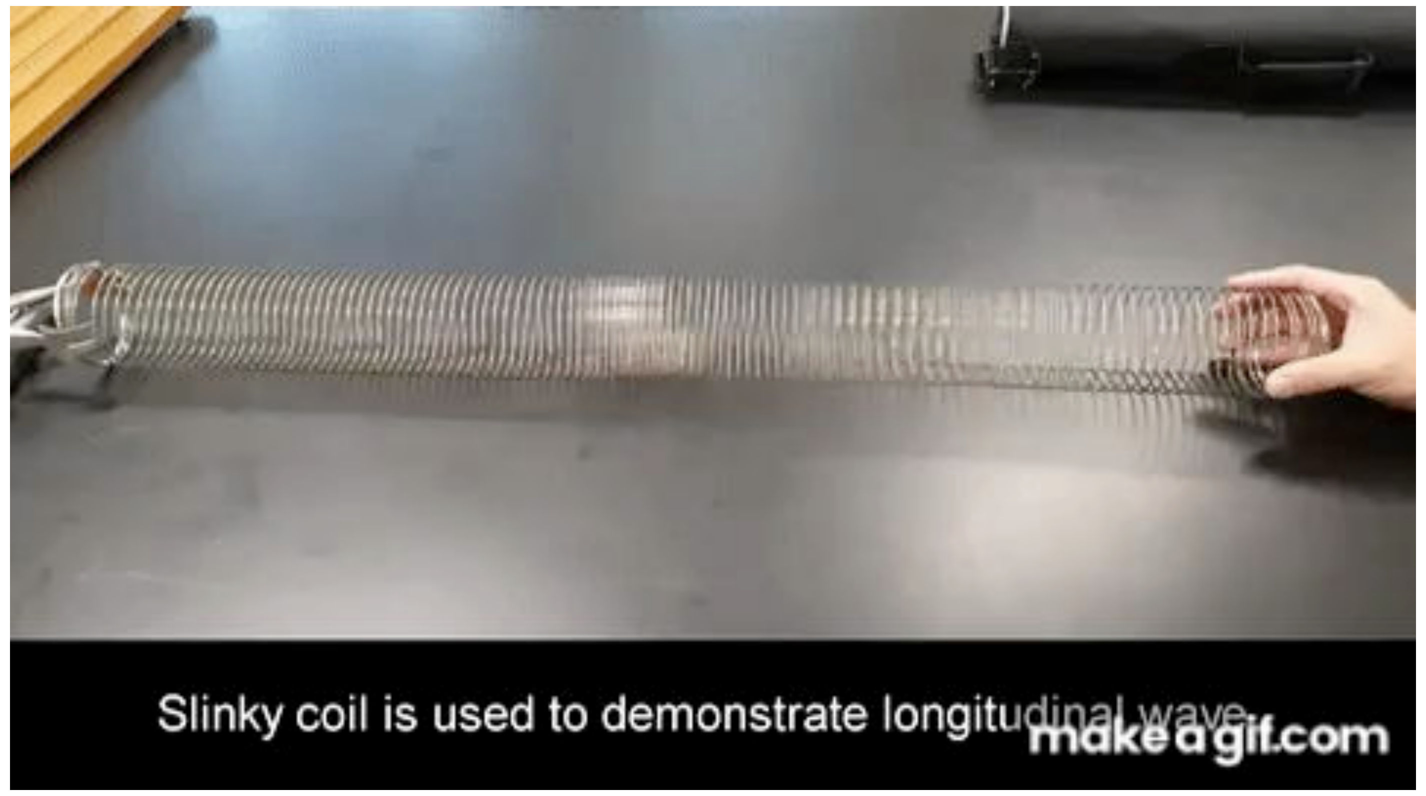
Diagram: Simon Burton

Topological Qubits

Idea: build a device where the qubit uses “Majorana quasiparticles” which are inherently stable against noise

Rough idea: A “quasiparticle” is when many particles interact in way that looks mathematically like another particle
    E.g.: waves on water

Majorana quasiparticles involve many “real” particles so a lot of the real particles must suffer noise to cause noise in the quasiparticle



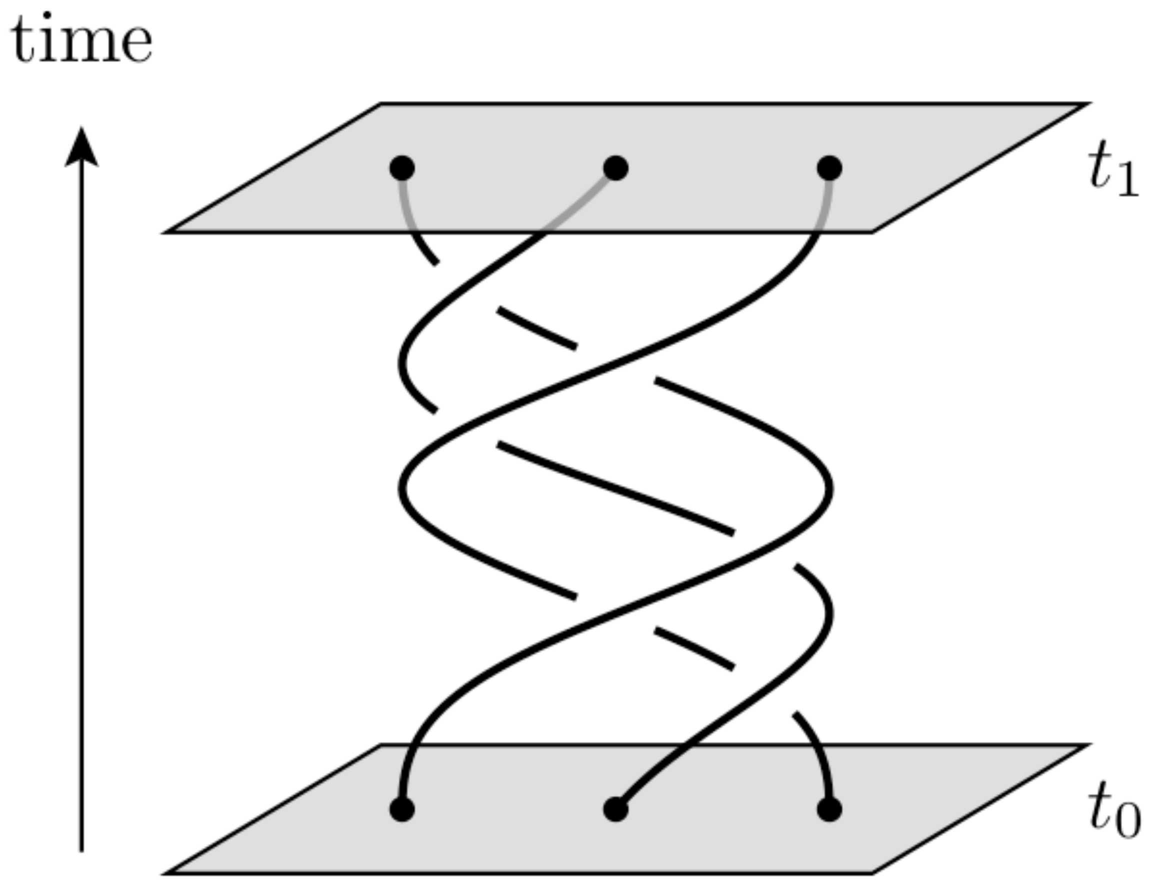


Diagram: Simon Burton

Did Microsoft make topological qubits?

quantum computing. It is an indium arsenide-aluminium hybrid device that admits superconductivity at low temperatures, and shows some signals of hosting boundary Majorana zero modes.[2][non-primary source needed] Majorana zero modes have the potential

Photo: John Brecher

Did Microsoft make topological qubits?

quantum computing. It is an indium arsenide-aluminium hybrid device that admits superconductivity at low temperatures, and shows some signals of hosting boundary Majorana zero modes.[2][non-primary source needed] Majorana zero modes have the potential

NEWS | 19 February 2025

nature

Microsoft claims quantum-computing breakthrough — but some physicists are sceptical

Photo: John Brecher

Did Microsoft make topological qubits?

quantum computing. It is an indium arsenide-aluminium hybrid device that admits superconductivity at low temperatures, and shows some signals of hosting boundary Majorana zero modes.[2][non-primary source needed] Majorana zero modes have the potential

NEWS | 19 February 2025

nature

Microsoft claims c computing breakt some physicists ar

nature portfolio

Peer Review File

In my opinion, these experiments are very interesting and certainly relevant for the condensed matter community working on topological superconductors and Majorana states. What I do NOT like is the way the article is written which, sometimes subtly and sometimes more crudely, uses a language and wording that at all times leads the reader to think that we are dealing with a measurement that demonstrates parity in a topological qubit based on Majorana states. The examples are many and here I highlight only a few:

Did Microsoft make topological qubits?

quantum computing. It is an indium arsenide-aluminium hybrid device that admits superconductivity at low temperatures, and shows some signals of hosting boundary Majorana zero modes.[2][non-primary source needed] Majorana zero modes have the potential

NEWS | 19 February 2025

nature

Microsoft claims c computing breakt some physicists ar

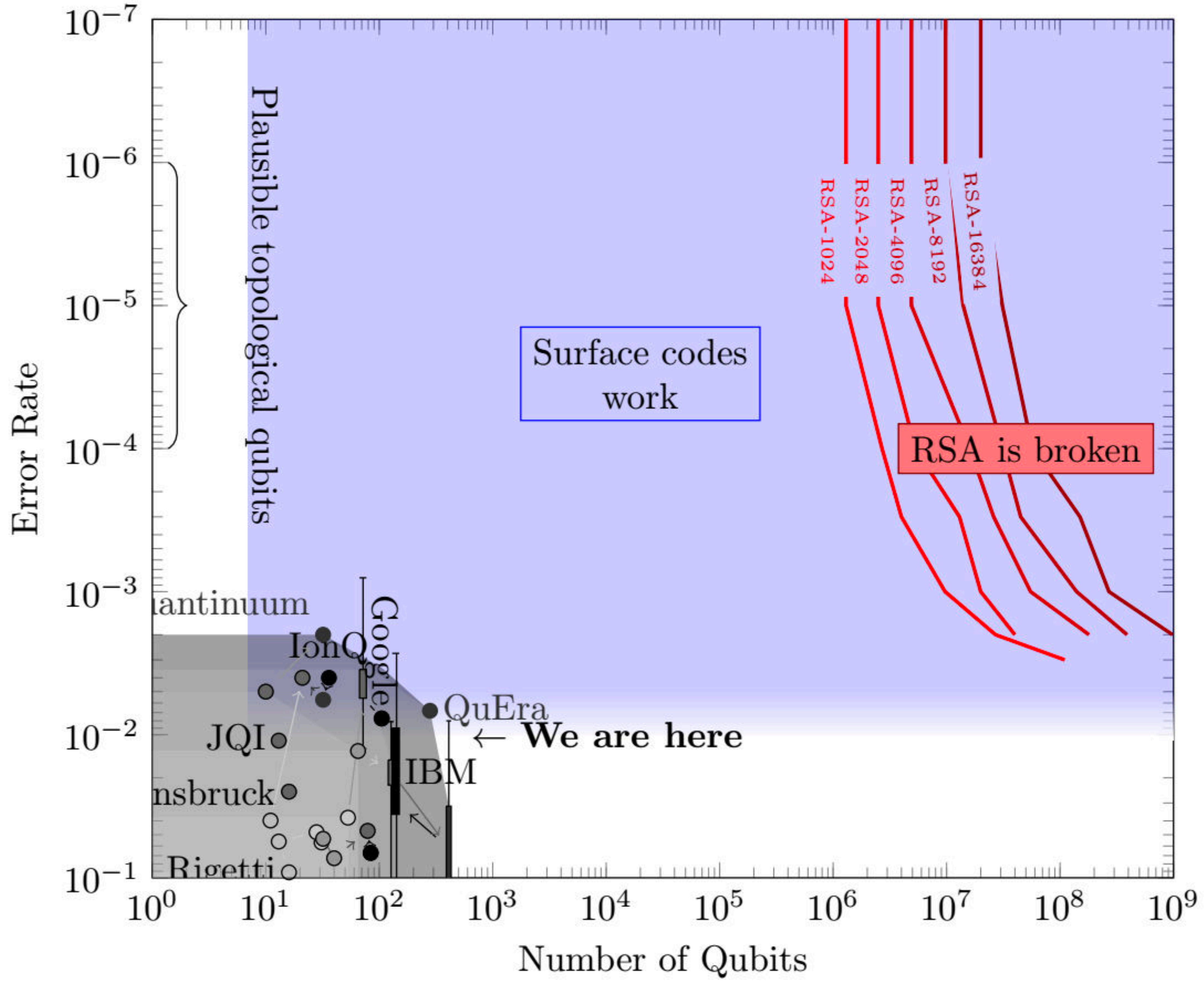
nature portfolio

Peer Review File

In my opinion, these experiments are very interesting and certainly relevant for the condensed matter community working on topological superconductors and Majorana states. What I do NOT like is the way the article is written which, sometimes subtly and sometimes more crudely, uses a language and wording that at all times leads the reader to think that we are dealing with a measurement that demonstrates parity in a topological qubit based on Majorana states. The examples are many and here I highlight only a few:

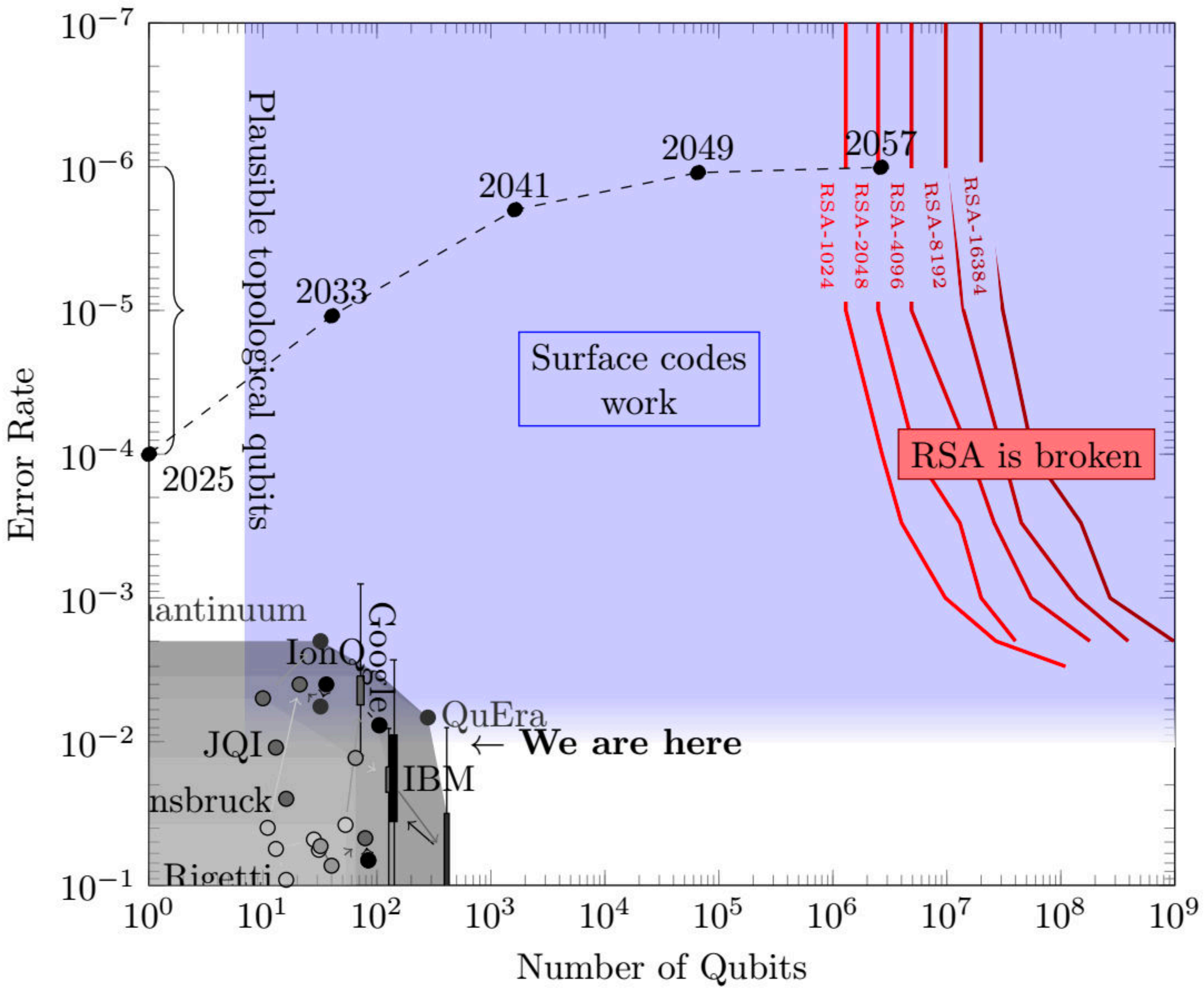
…maybe?

If Microsoft made a topological qubit:



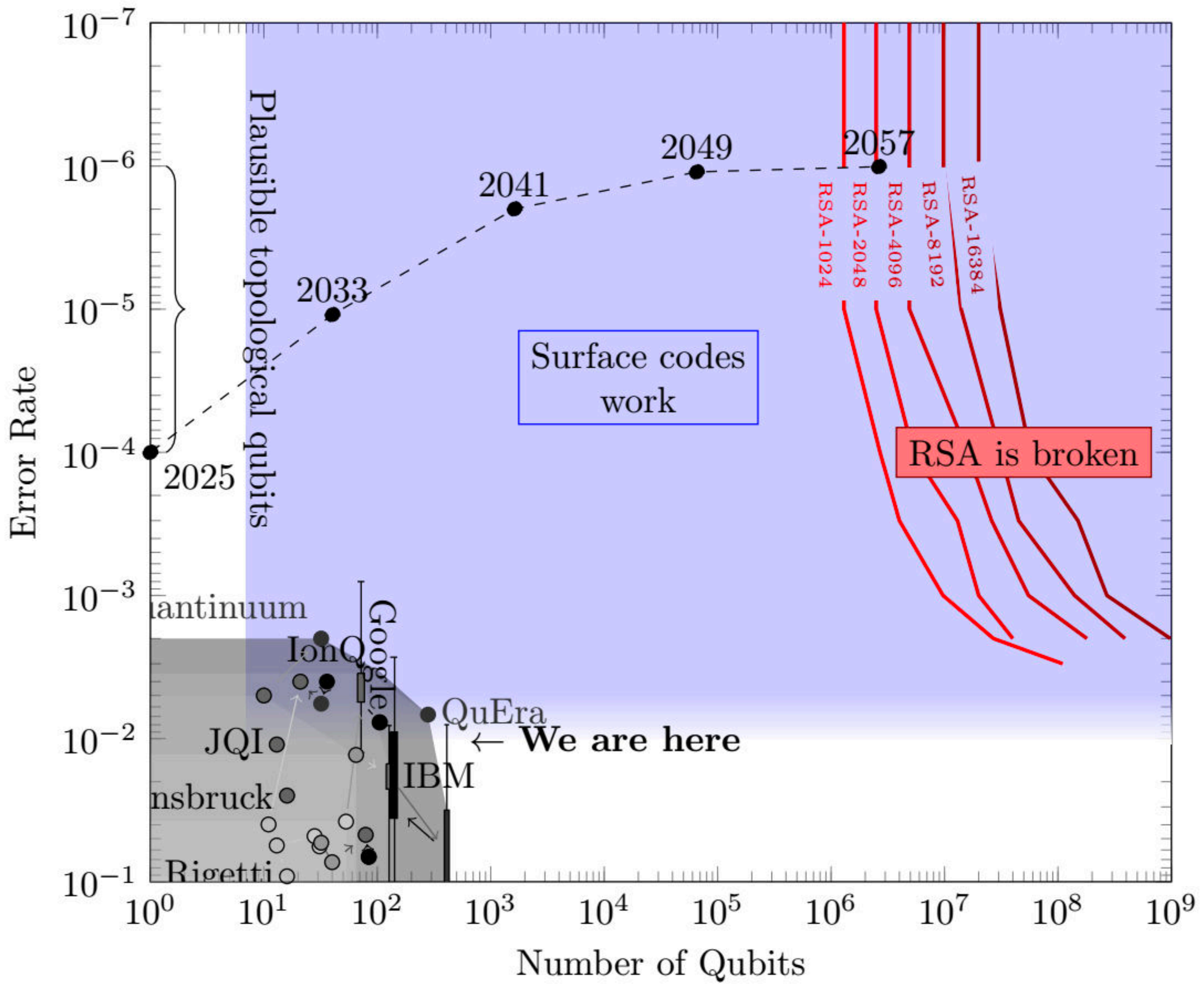
Even Microsoft (arxiv:2211.07629) expects topological qubits to need error correction

If Microsoft made a topological qubit:



Even Microsoft (arxiv:2211.07629) expects topological qubits to need error correction

If Microsoft made a topological qubit:



Even Microsoft (arxiv:2211.07629) expects topological qubits to need error correction

With 18-month doubling it's still a long ways from factoring

Surface codes have a high minimum overhead

Cat Qubits

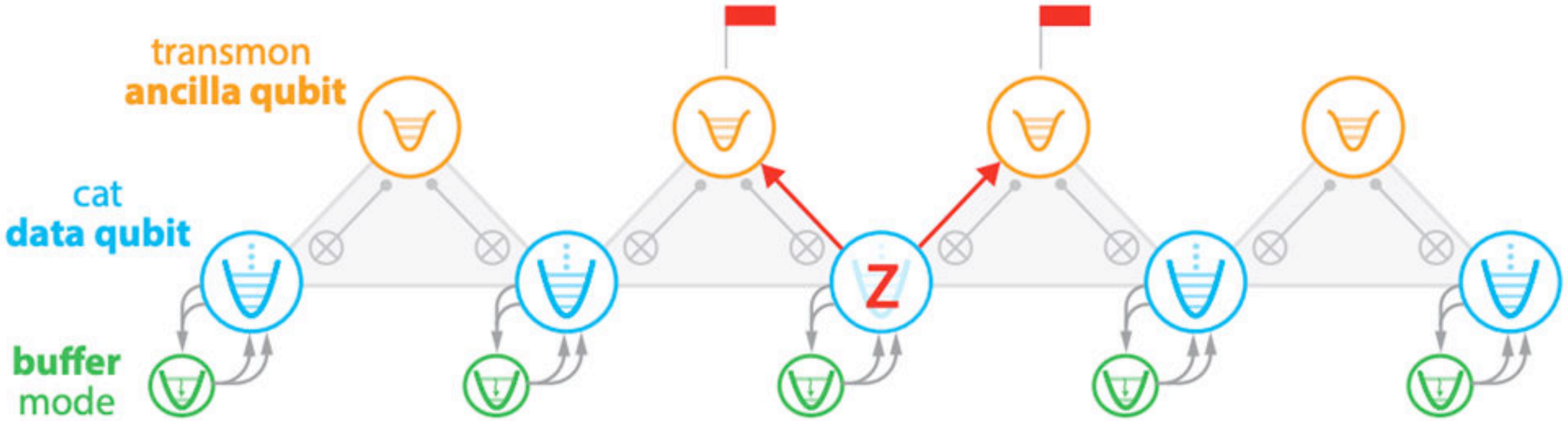


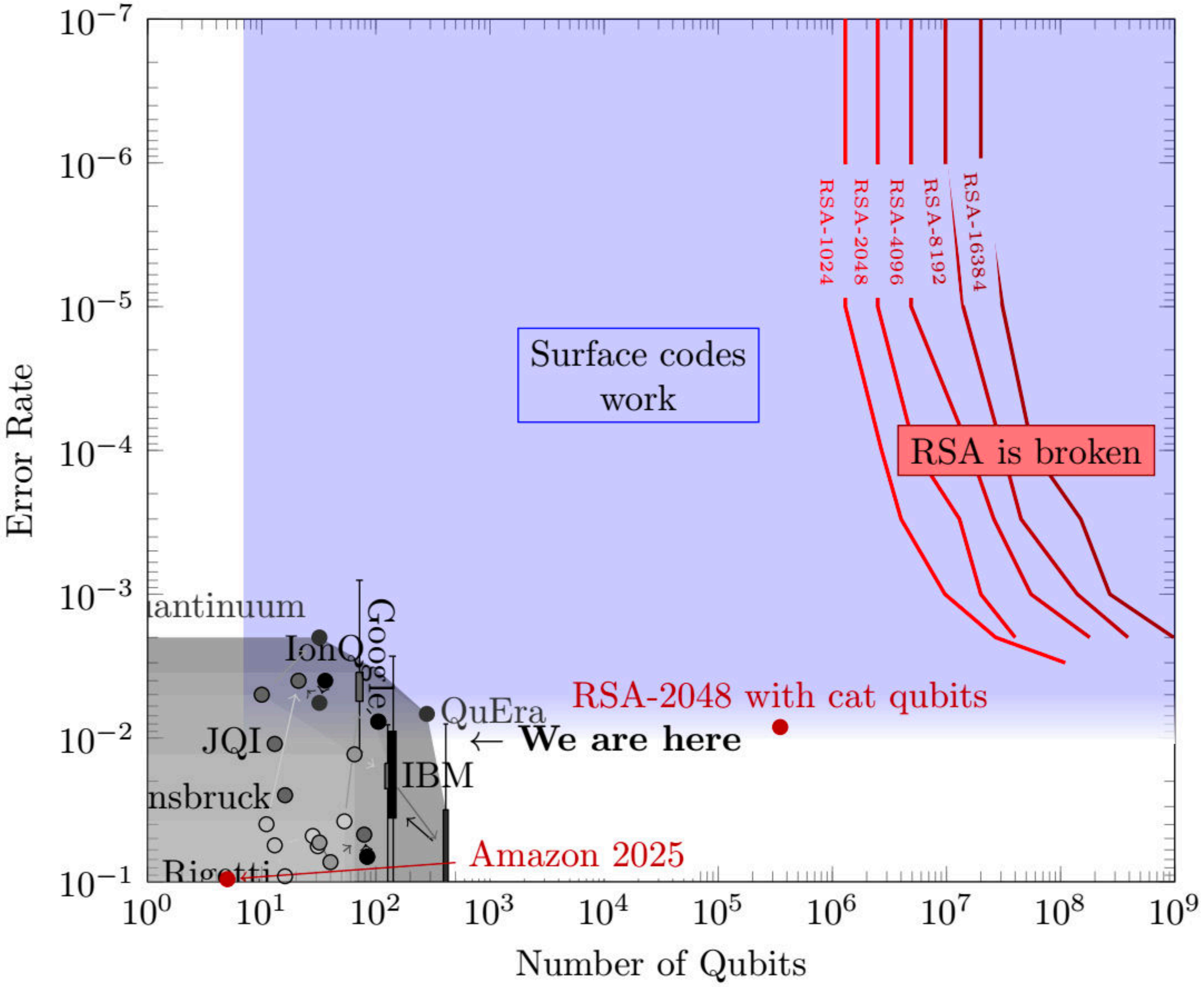
Diagram from Amazon's recent Nature paper

Quantum computing has two dimension of error: bit flips and phase flips

Cat qubit: each physical qubit is a coherent mixture of many photons, making bit flip errors **exponentially harder** but phase flips **linearly easier**

Benefit: can use an unbalanced surface code

Cat Qubits



- "Only" 15 doublings from here (2047 with Moore's law scaling)
  - (18 doublings with superconductors)
- Lots of uncertainties in hardware development

(Resource estimate from Gouzien et al. arxiv:2302.06639)

My opinions on hardware advances:

Google: "slow and steady" approach: use a more mature technology but which will require large overheads

Microsoft and Amazon: aiming for a riskier technology that might leap ahead

- What to look for:
  - Will Microsoft irrefutably demonstrate a topological qubit?
  - Will anyone demonstrate surface code error correction with something besides superconductors?

2. Better codes?

- The surface code is a (cohomological) product of two repetition codes: one for bit flip errors, one for phase flips
  - Nearly the simplest code you can construct
- Its asymptotic rate is zero
- Isn't there something better?

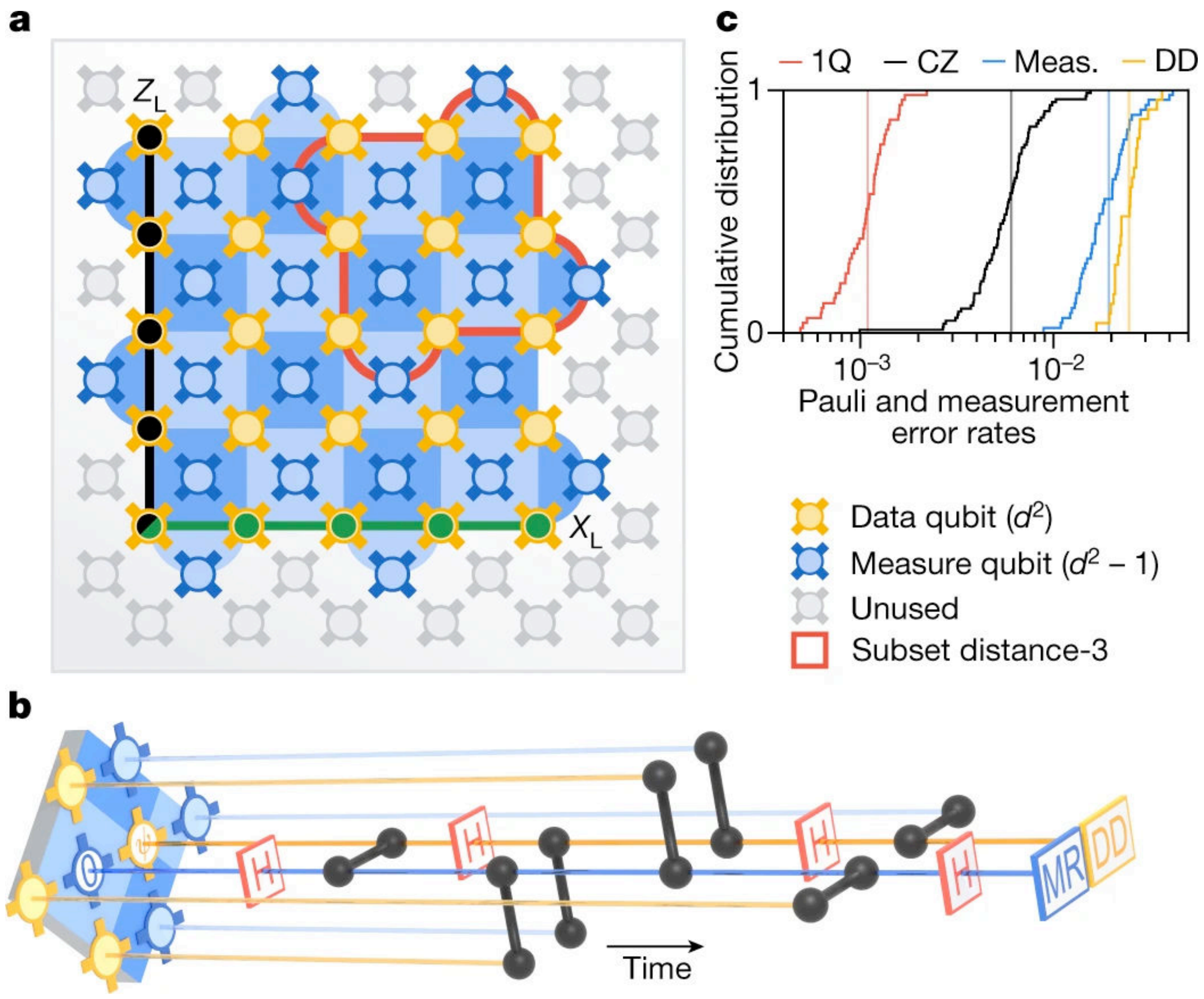
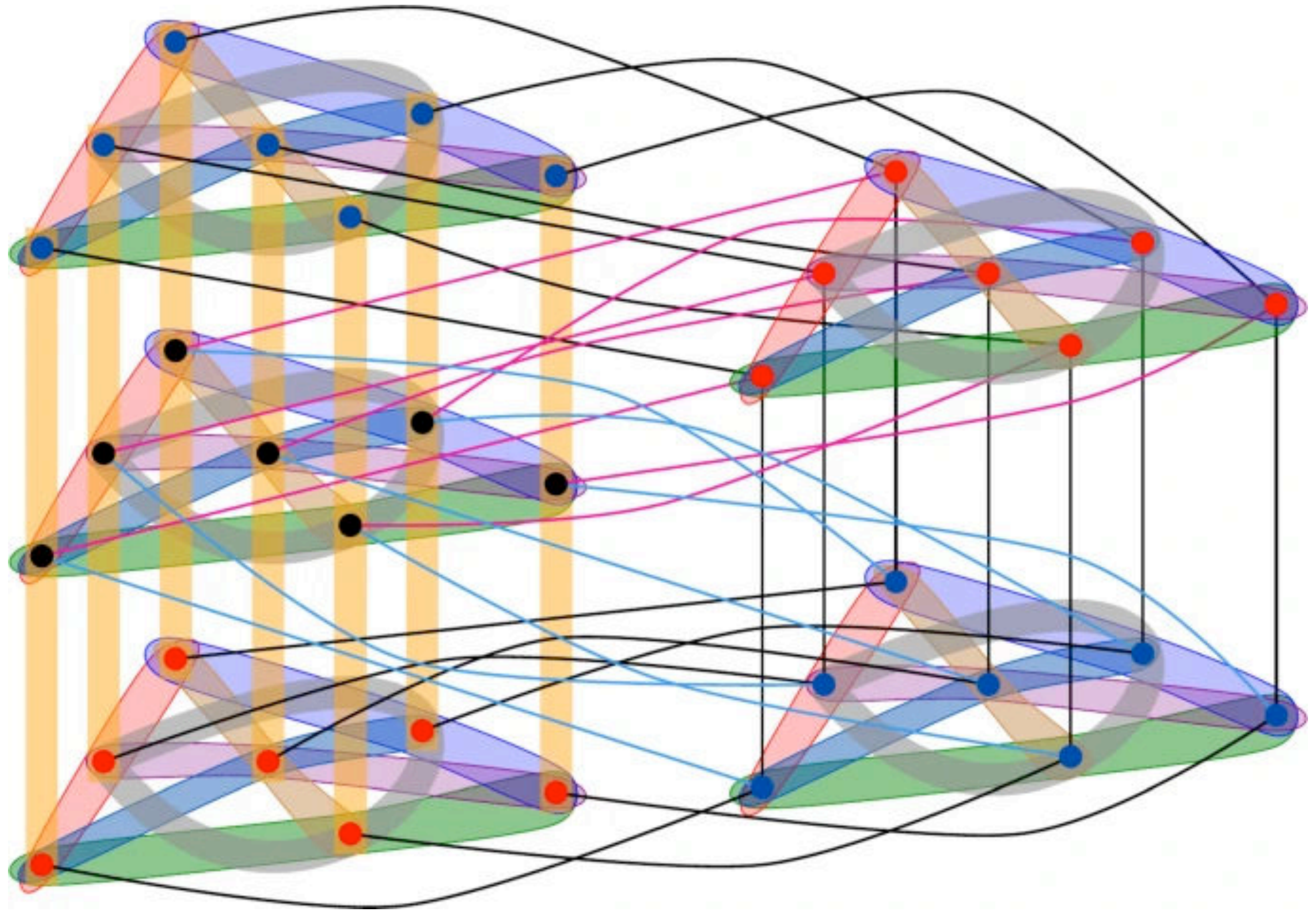


Diagram: Google Quantum AI

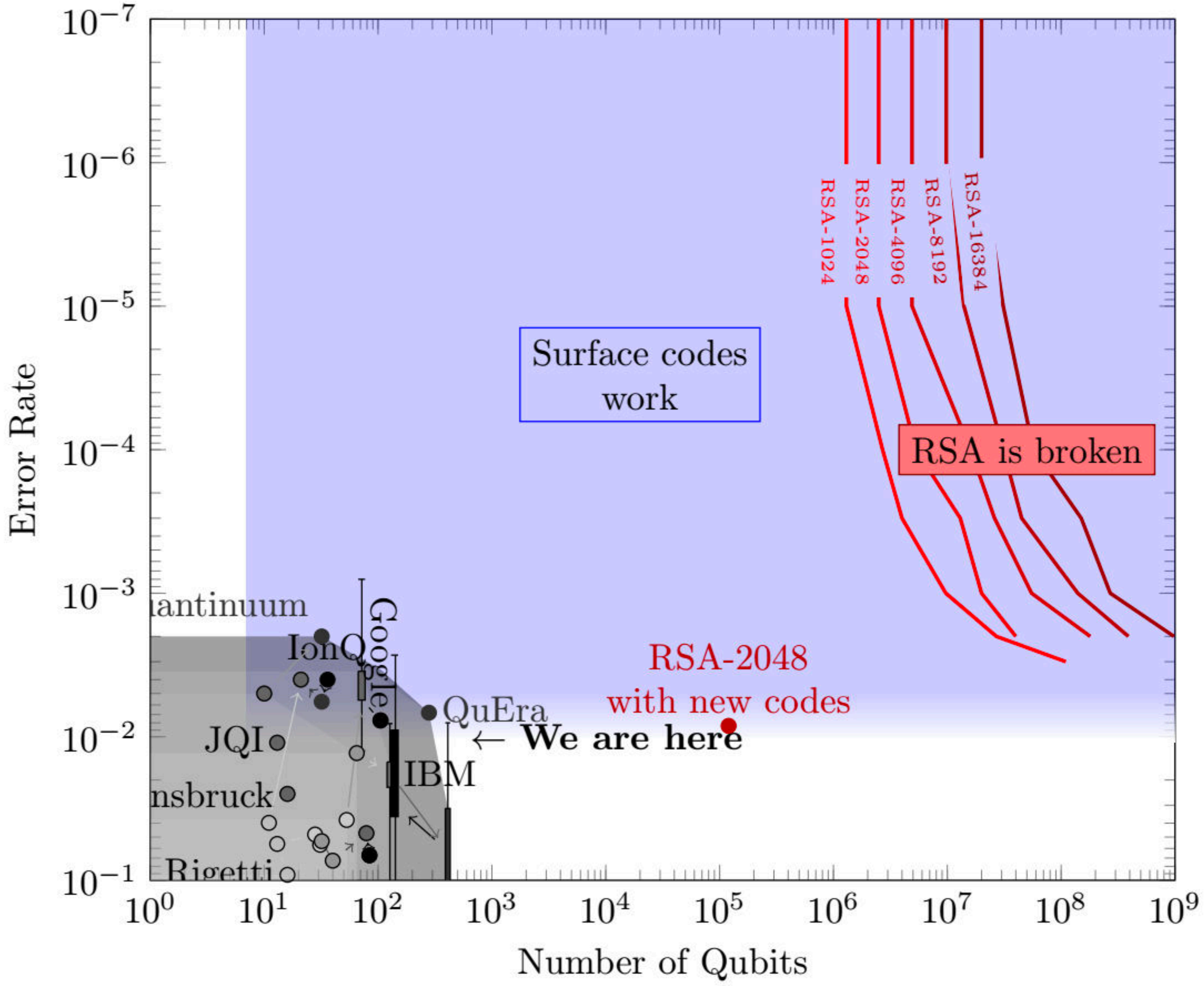
Asymptotically Good Codes

- In 2021 Pantaleev and Kalachev found an LDPC code with a constant ratio of physical:logical qubits
- LDPC = low density parity check, meaning errors can be detected with small circuits
- Physical:logic qubits maybe 14:1
  - Surface code is 881:1



From Akhtar and Marty, 2024. This is just a hypergraph product, a core mathematical building block of these new codes

Asymptotically good codes



- Only 10 doublings from here (**2039** with Moore's law scaling)
- **What's the catch?**

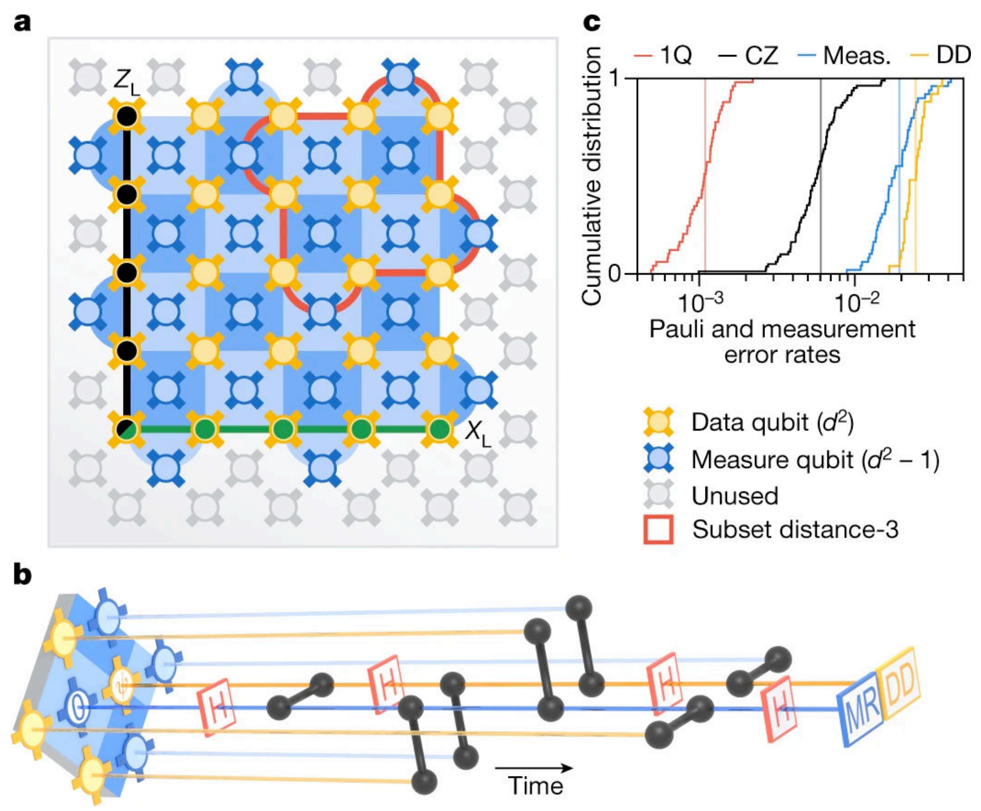
Unsolved Issues with new codes

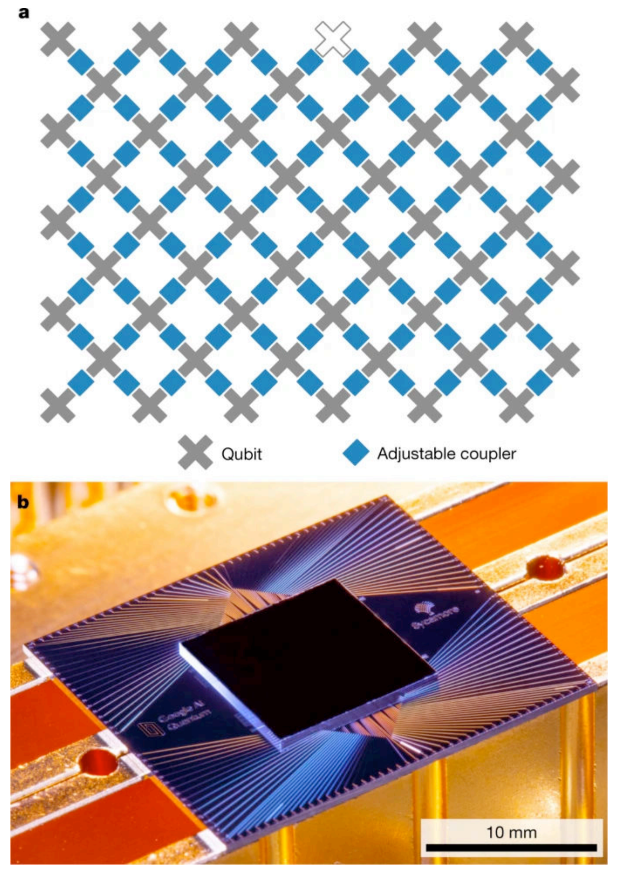
1. Long-range interactions between qubits

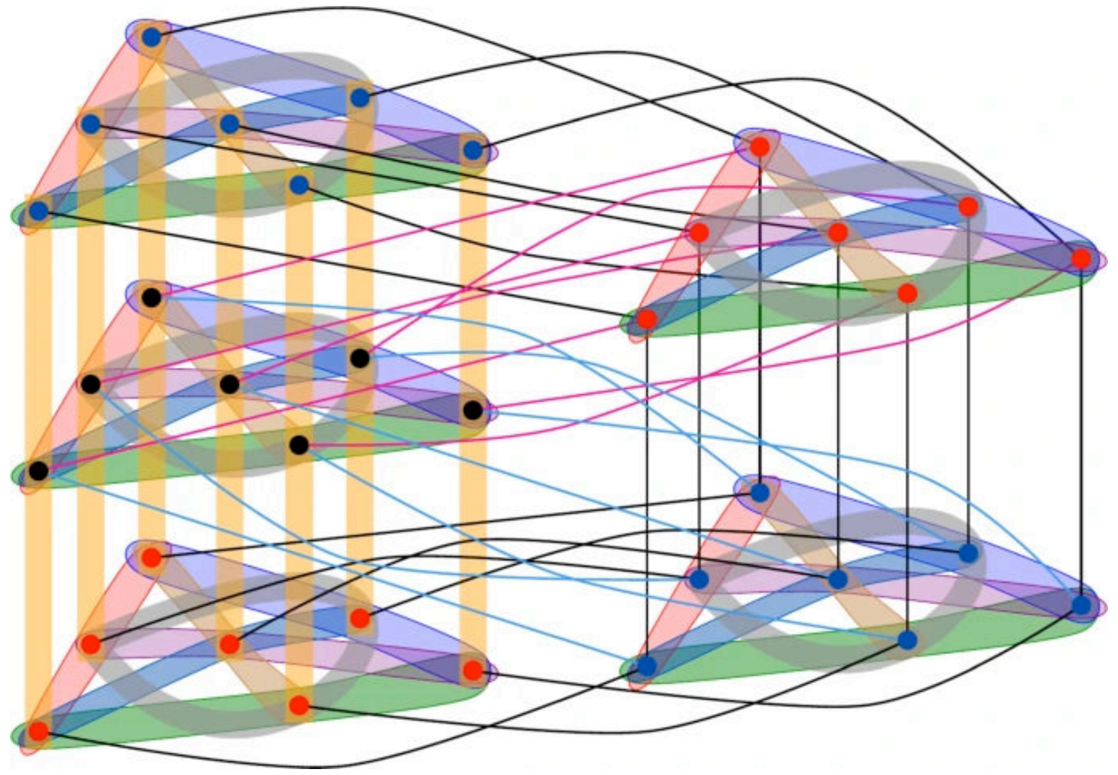
2. Uncertain how to compute with them

Unsolved Issues with new codes

1. Long-range interactions between qubits





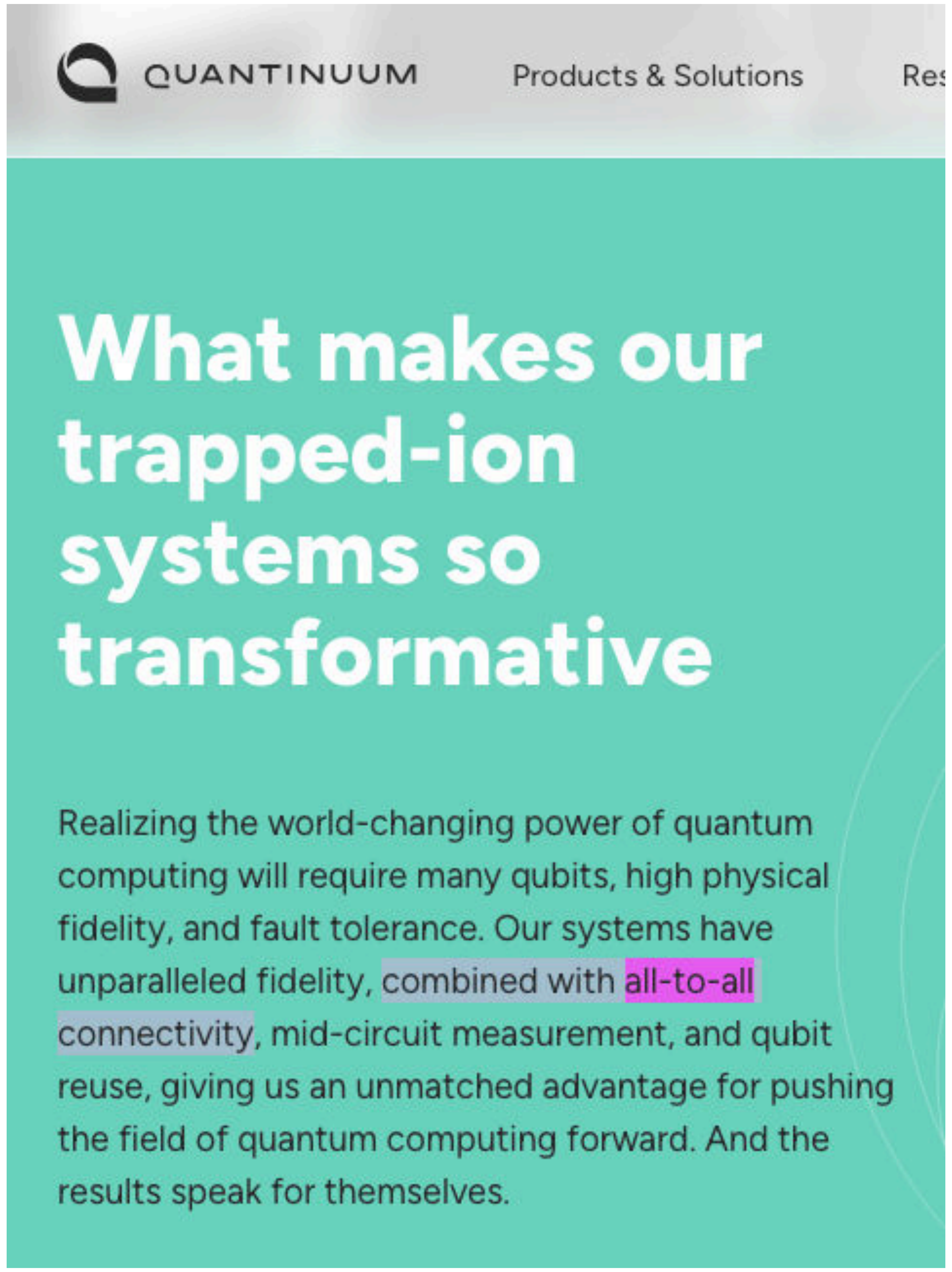


???????

Unsolved Issues with new codes

1. Long-range interactions between qubits

Baspin and Krishna (arXiv:2109.10982) show that long-range interactions **cannot be avoided** for high-rate codes.
In fact the surface code is optimal for codes in that layout!



Can any hardware handle long-range interactions?
Ion trappers will tell you that ion traps can!

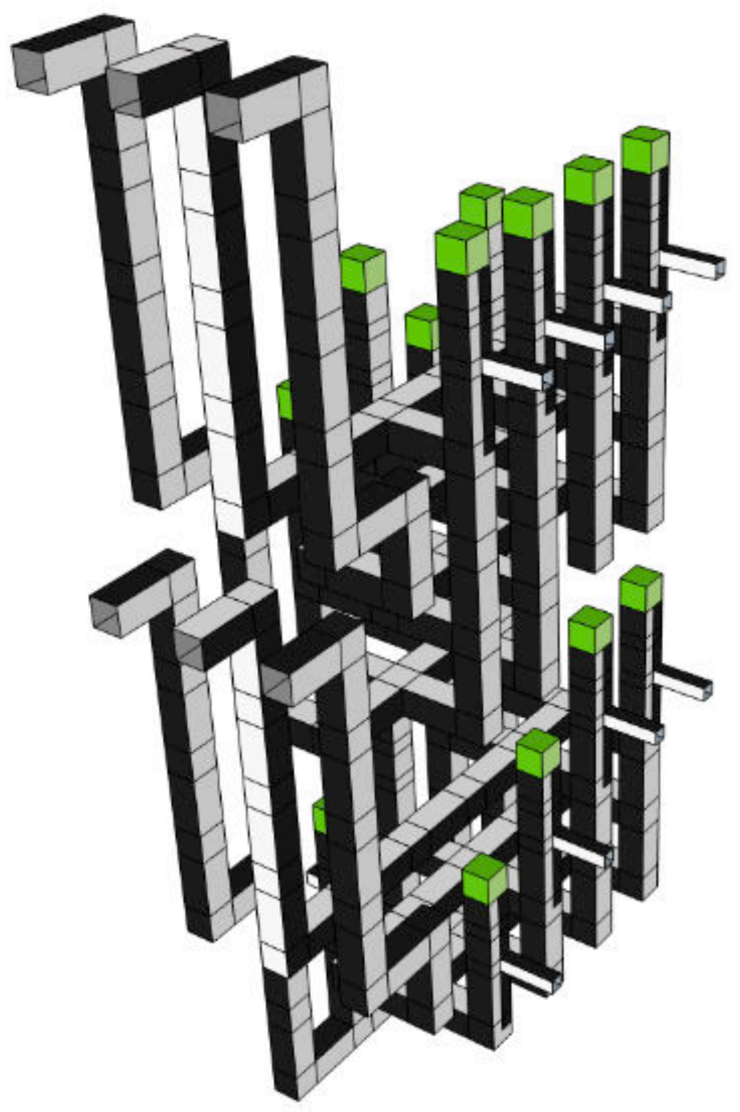
I'm skeptical about scalability

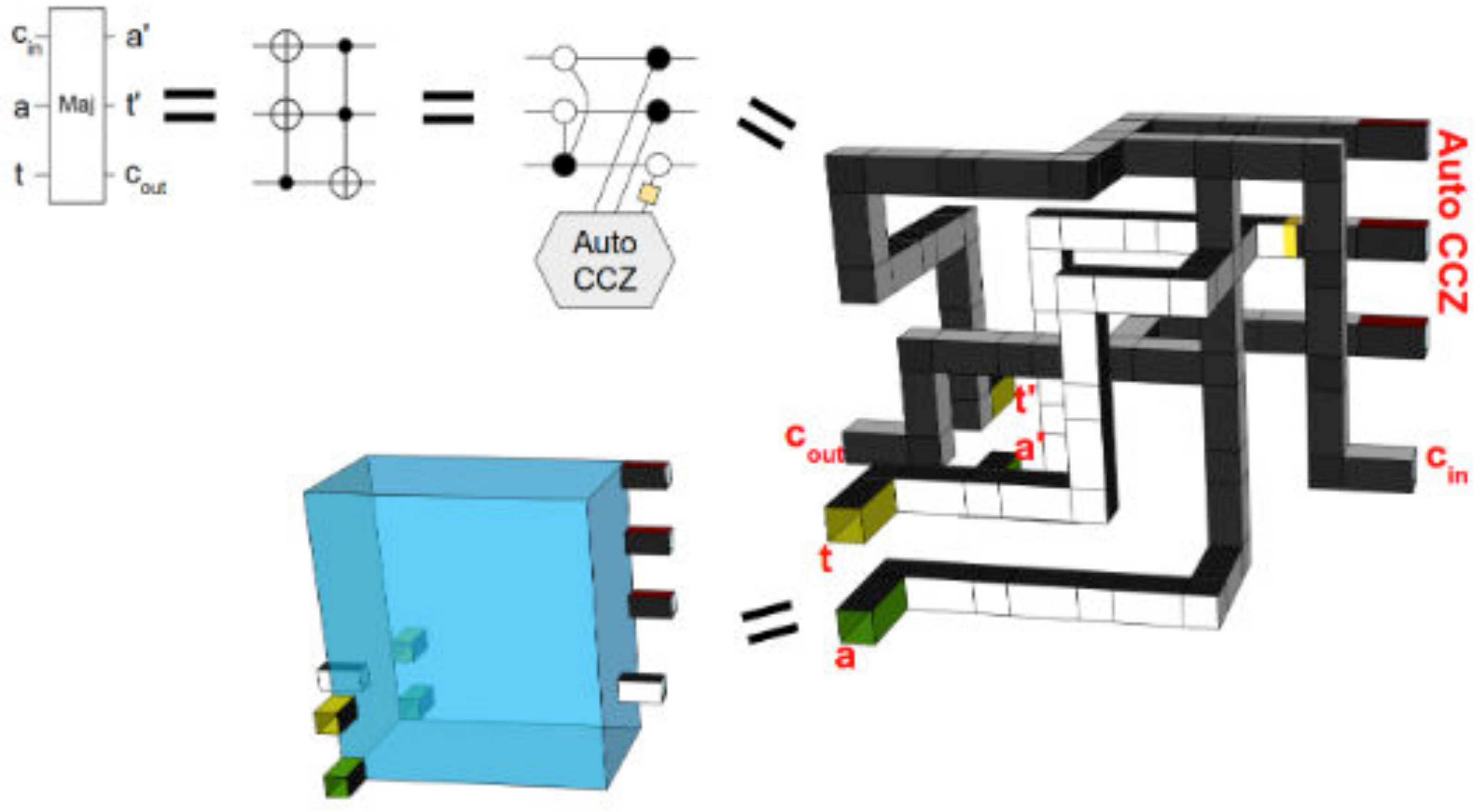
Unsolved Issues with new codes

2. Uncertain how to compute with them

Qubits are so noisy they must **stay** encoded during computations

Computing on encoded data is non-trivial! Look at the surface code:



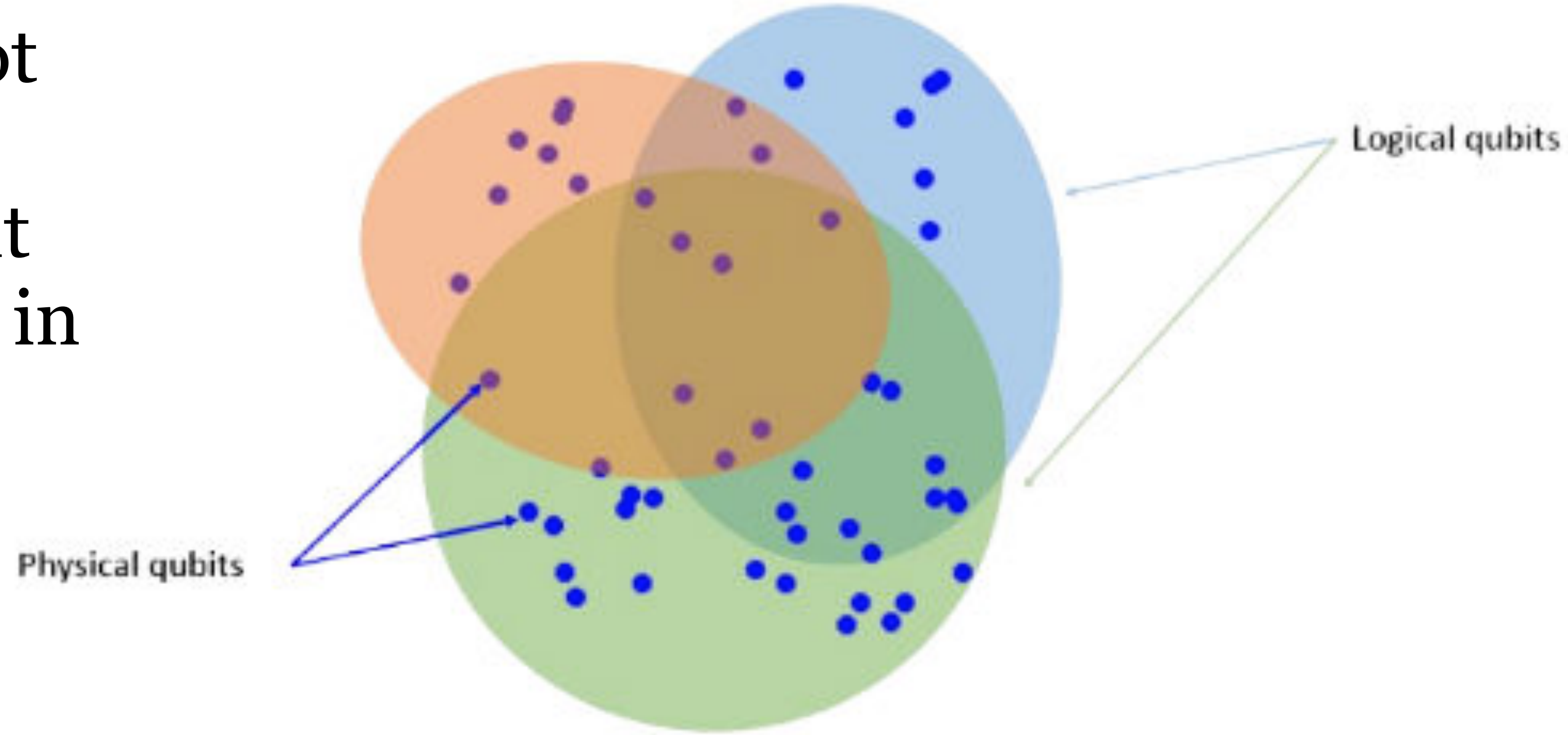


Gidney and Fowler, arxiv:1905.08916

Unsolved Issues with new codes

2. Uncertain how to compute with them

Recent results with Jérôme Guyot (arxiv:2502.13889) proved some impossibility results; other recent papers show constructive results in worse codes



UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

3. Better algorithms?

- In 2021 I wrote:

> …Shor's algorithm is mainly just modular exponentiation, meaning that it's about as hard for a quantum computer to *use* RSA as it is to *break* RSA. An **asymptotic improvement is highly unlikely**

3. Better algorithms?

- In 2021 I wrote:

…Shor's algorithm is mainly just modular exponentiation, meaning that it's about as hard for a quantum computer to *use* RSA as it is to *break* RSA. An **asymptotic improvement is highly unlikely**

[Submitted on 12 Aug 2023 (v1), last revised 7 Jan 2024 (this version, v3)]

An Efficient Quantum Factoring Algorithm

Oded Regev

We show that n-bit integers can be factorized by independently running a quantum circuit with $\tilde{O}(n^{3/2})$ gates for $\sqrt{n}+4$ times, and then using polynomial-time classical post-processing. The correctness of the algorithm relies on a number-theoretic heuristic assumption reminiscent of those used in subexponential classical factorization algorithms. It is currently not clear if the algorithm can lead to improved physical implementations in practice.

Regev’s New Factoring Algorithm

From Ekerå and Gärtner (arxiv:2405.14381)

A.1 RSA IFP

A.1.1 A basic baseline comparison

	IFP via Regev [30] with [28, 29]							RSA IFP via Ekerå–Håstad [8, 9, 12]							
						per run	overall					per run		overall	
$\lceil \log N \rceil$	d	m	C	$\log D$	K	#ops	#ops	m	s	ℓ	n	#ops	adv	#ops	adv
2048	46	50	2.03	96	138	2760	138000	1023	–	993	1	6018	0.46	6018	22.9
									17	61	20	2290	1.20	45800	3.01

- Total gate complexity is still $O(n^3)$ (like Shor’s) but split into $O(n^{1/2})$ runs
  - Ekerå and Gärtner (arxiv:2311.05545) show that it tolerates runs with errors
  - Overall error correction might be lower, but it remains to be seen

Reducing the Number of Qubits in Quantum Factoring

Chevignard, Fouque, Schrottenloher (eprint: 2024/222)

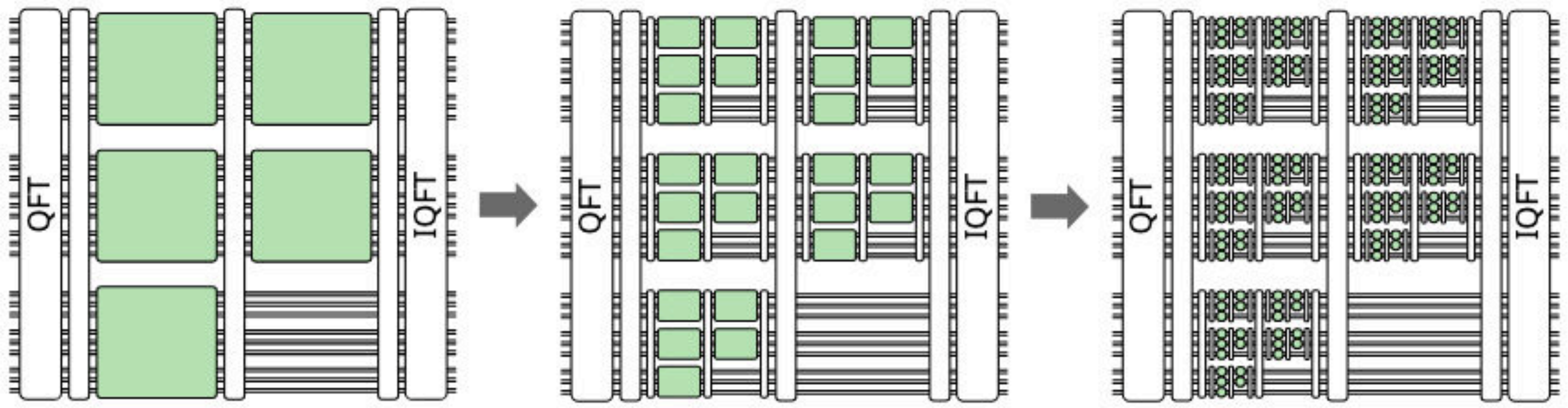
Reduces logical qubit count by using the residue number system

At least 1.6 million physical qubits (likely more for "state factories" and routing)

Fast quantum integer multiplication with zero ancillas

Kahanamoku-Meyer and Yao (arxiv: 2403.18006)

Uses QFT arithmetic; likely improves in practice but not with the paper above



Reducing the Number of Qubits in Quantum Factoring

Chevignard, Fouque, Schrottenloher (eprint: 2024/222)

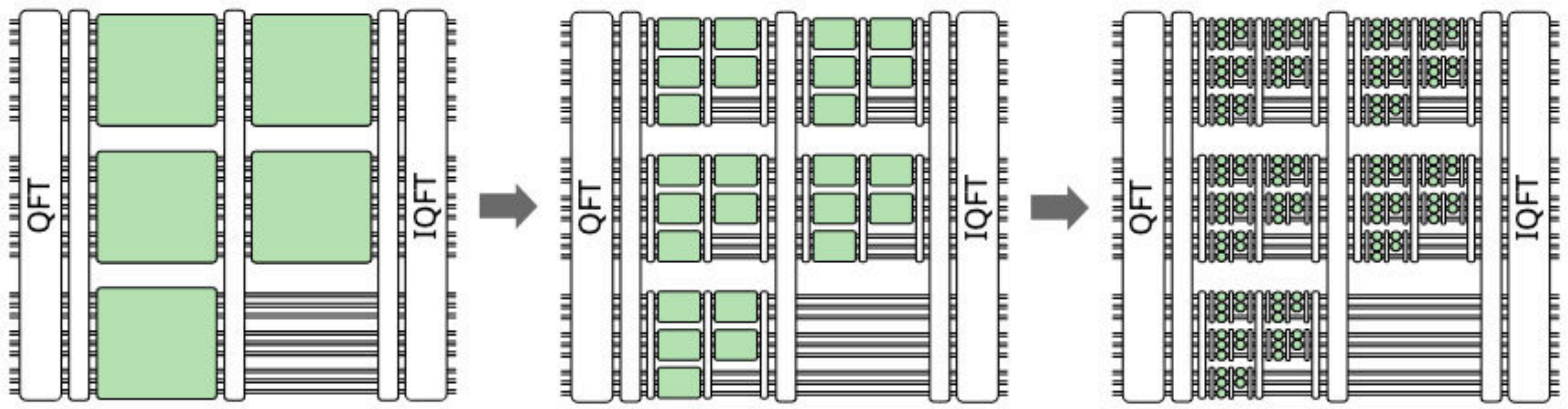
Reduces logical qubit count by using the residue number system

At least 1.6 million physical qubits (likely more for “state factories” and routing)

Fast quantum integer multiplication with zero ancillas

Kahanamoku-Meyer and Yao (arxiv: 2403.18006)

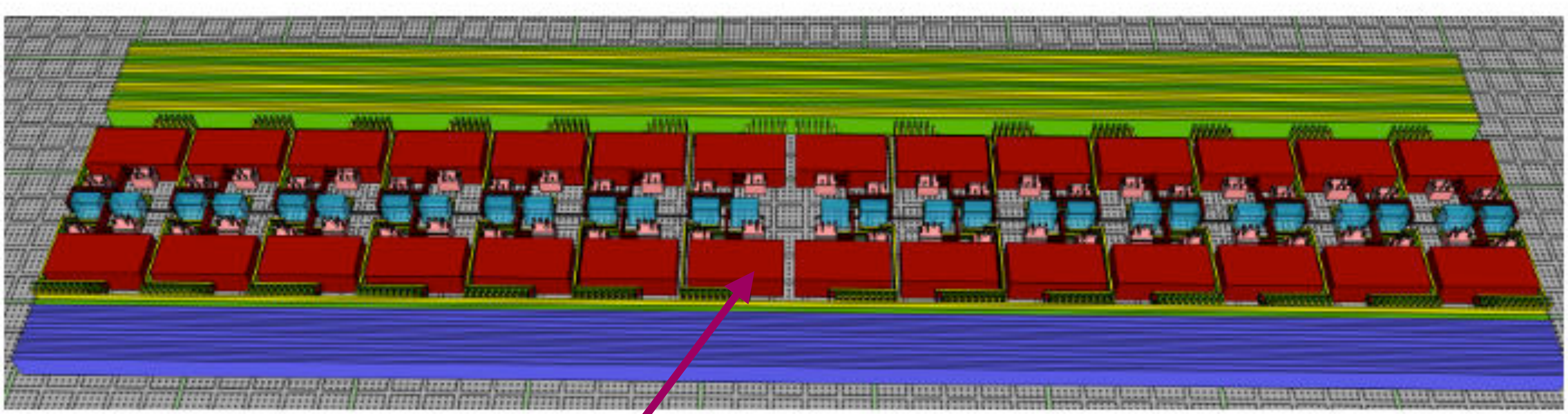
Uses QFT arithmetic; likely improves in practice but not with the paper above



Overall: great work but I don’t expect more than 10x cost reduction, if any

4. Better Implementations

Surface code layout for Shor's algorithm from Gidney and Ekerå 2019. Time is vertical axis

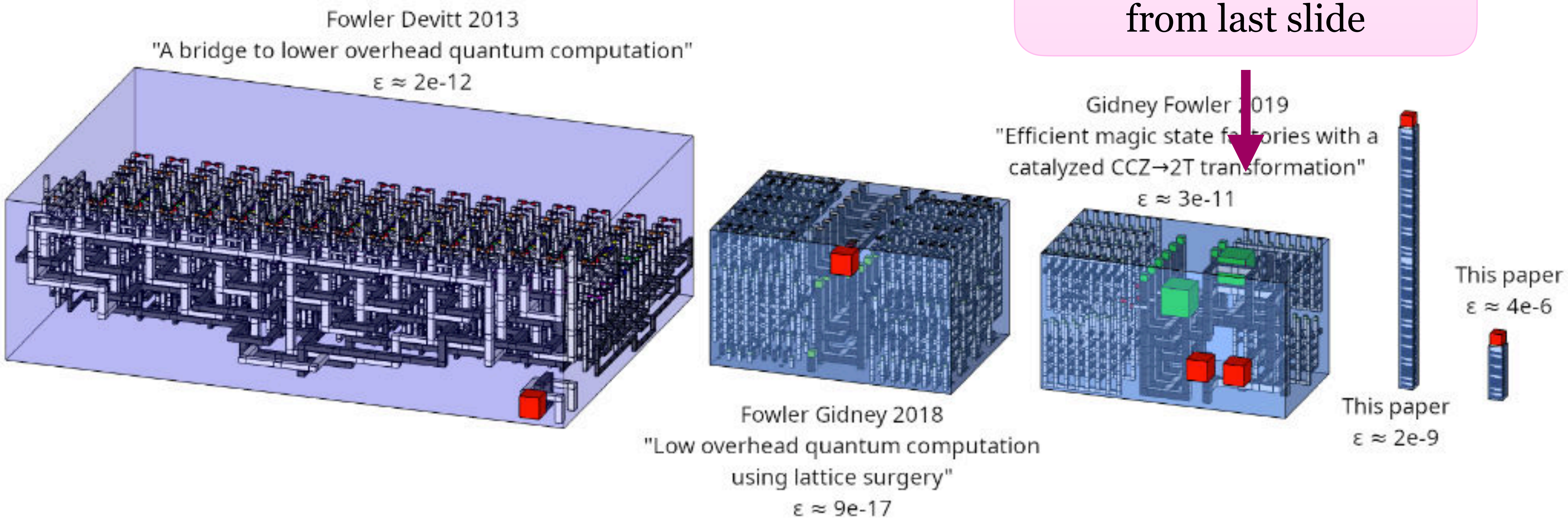


Each of these red and pink pairs of boxes does 1 AND gate

Magic state *cultivation*

- Gidney, Shutty, and Jones (arxiv: 2409.17595) Figure 3 speaks for itself

About half of the red box from last slide

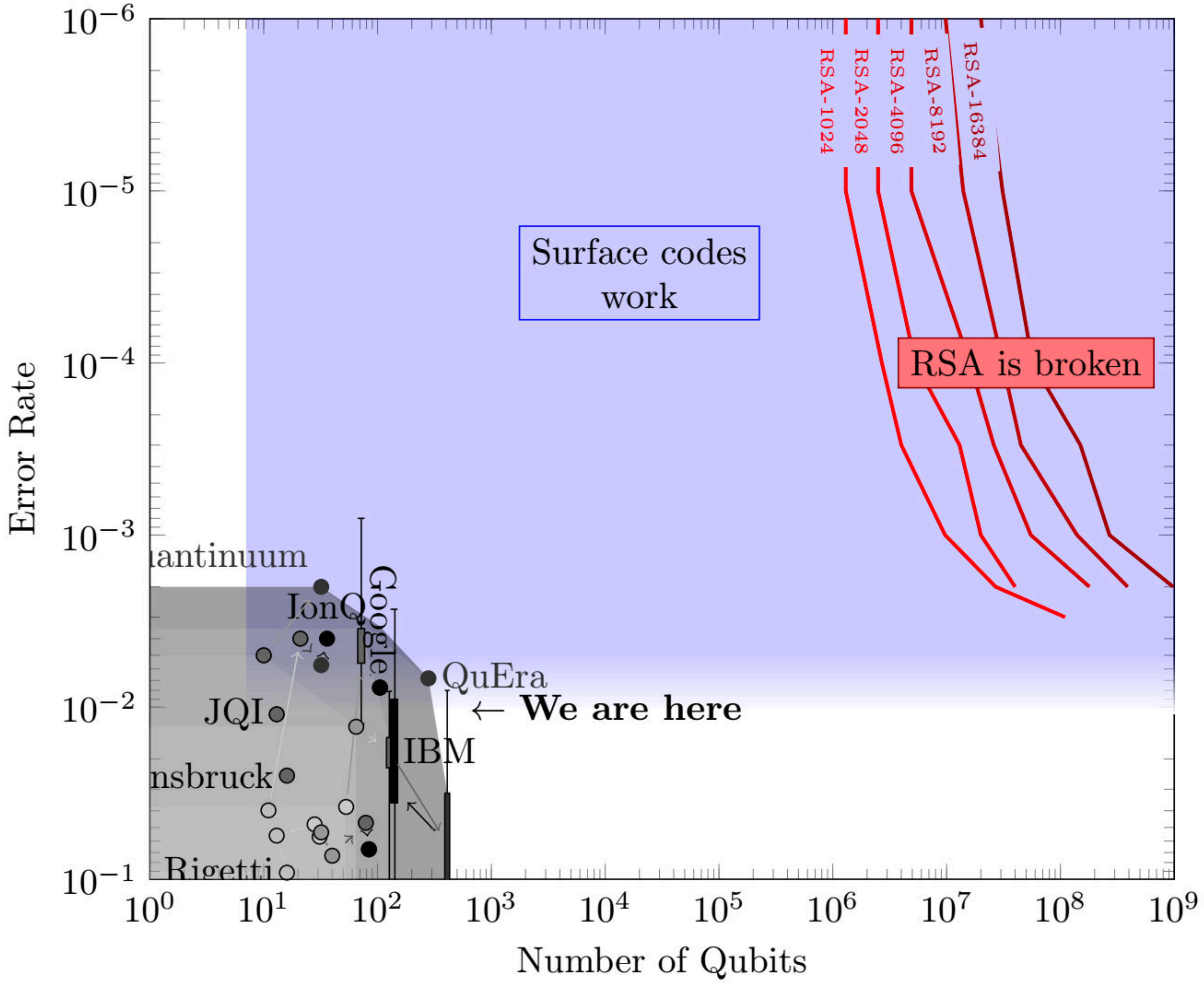


Not only could this **drastically** reduce resources of previous circuits, it could up use of new classes of circuits

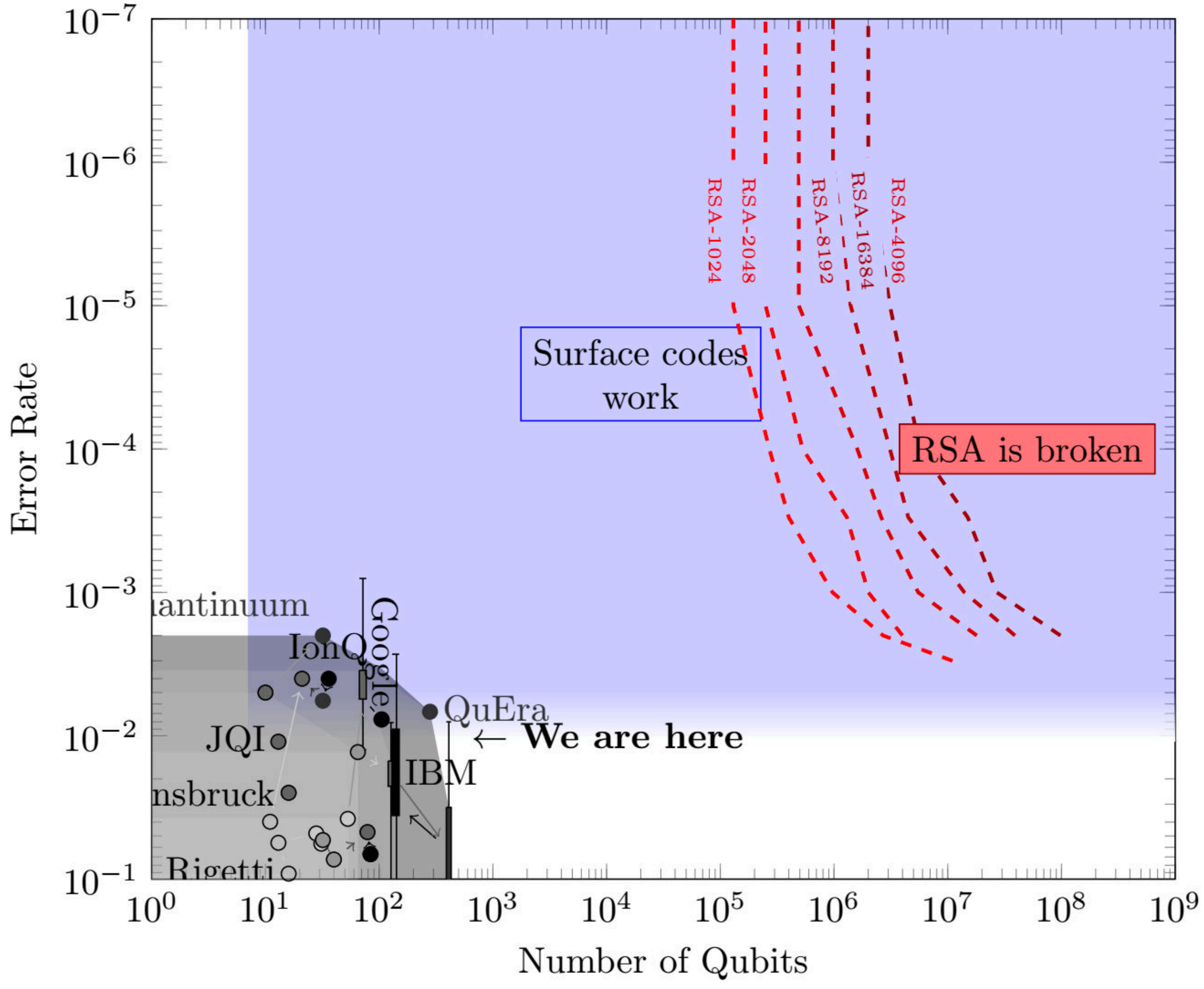
Quantum Resource Estimation Stack

	Full-Stack Estimation	
	Gidney and Ekerå (2019)	Current State-of-the-art
Factoring Algorithm	Ekerå-Håstad (2017)	Regev (2023)? Chevignard-Fouqe-Schrottenloher (2024)?
Arithmetic Circuits	Gidney (2018-2019)	Kahanamoku-Meyer and Yao (2024)?
Error-corrected layout	Gidney and Ekerå (2019)	??????
Fault-Tolerant Gates	Gidney and Fowler (2019)	Gidney, Shutty, and Jones (2024)

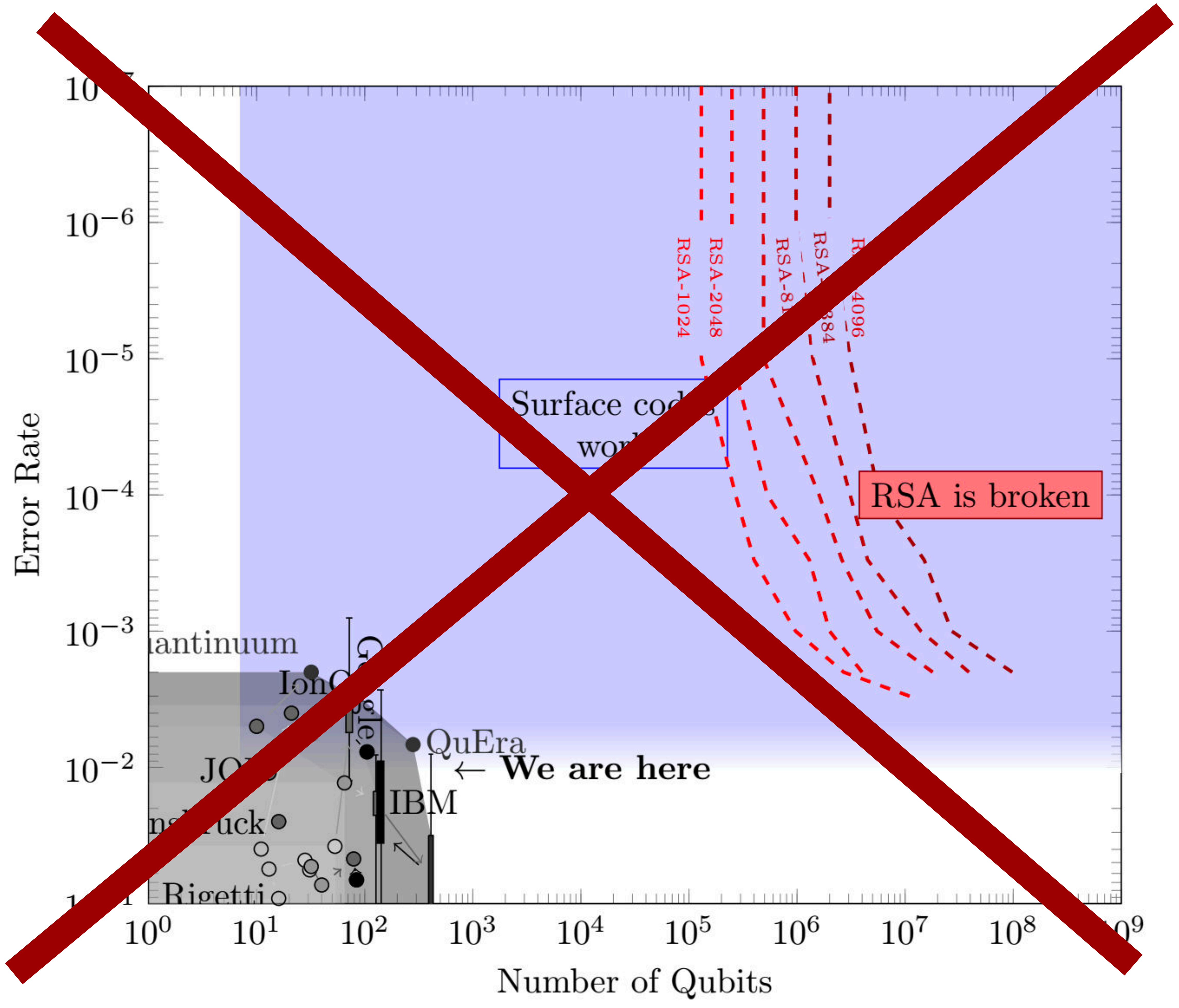
The chart I would like to show you



The chart I would like to show you



The chart I would like to show you



- The red lines came from a **full stack** estimate of resources in a surface code, including physical layout, “magic state distillation”, etc.
- Updating the full stack is a big project no one has done yet

UNIVERSITY OF WATERLOO | FACULTY OF MATHEMATICS

CONCLUSIONS

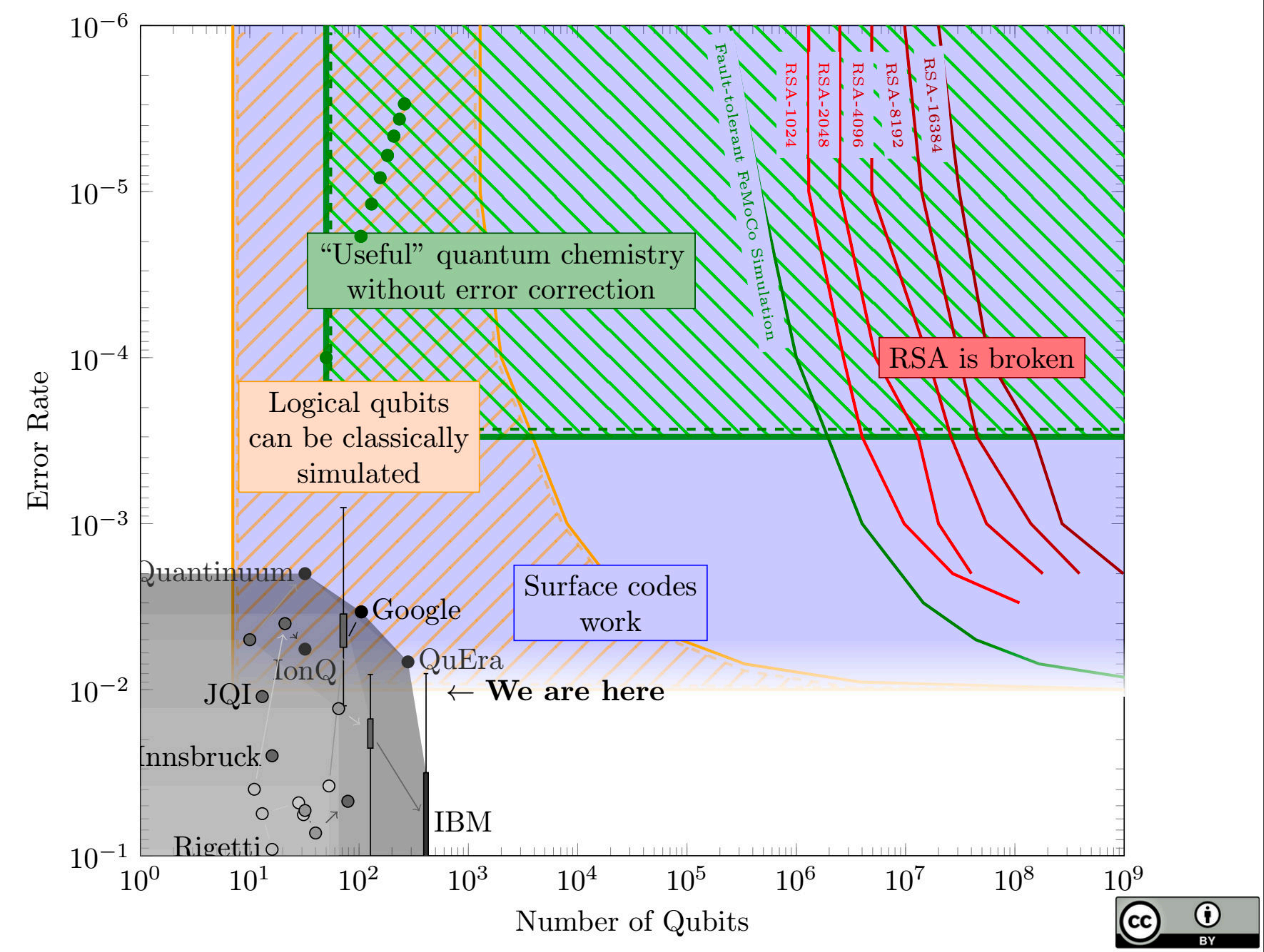
- Qubits will need error correction
- Today's best estimate to factor RSA-2048: 20 million qubits (200,000x beyond today)
- RSA is probably easier to factor than this estimate: stay tuned
- Quantum computing is still an immature technology; expect unexpected developments

CONCLUSIONS

- Qubits will need error correction
- Today's best estimate to factor RSA-2048: 20 million qubits (200,000x beyond today)
- RSA is probably easier to factor than this estimate: stay tuned
- Quantum computing is still an immature technology; expect unexpected developments

Thank you, I'm done talking now

Samuel Jaques



10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
Error Rate
10^0 10^1 10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9
Number of Qubits
Fault-tolerant FeMoCo Simulation
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
"Useful" quantum chemistry without error correction
RSA is broken
Logical qubits can be classically simulated
Surface codes work
Quantinuum
Google
IonQ
QuEra
JQI
← We are here
Innsbruck
IBM
Rigetti