Quantum Computers: Should we worry?

Dr. Morton Swimmer

Forward-looking Threat Research, Trend Micro

2025 TF-CSIRT Meeting & FIRST Regional Symposium Europe, Monaco, January 14-16, 2025

What is the threat?

TREND MICRO

ACCESSWIRE

Why We Can't Afford to Ignore Quantum Computing, Even if We Don't Completely Understand It

TAG Infosphere
Wed, December 4, 2024 at 3:00 PM GMT+1 • 3 min read

Available For Free Download

NEW YORK, NY / ACCESSWIRE / the fear that the Y2K bug provoke
even panic-that when the calenda
and systems that could only acco
would come crashing down, wreak
many deaths.

If that sounds like a distant memo
about Y2Q, the shorthand cyber ex
Though quantum computing is sti
about it can come across as geeky
danger it poses to the global inter

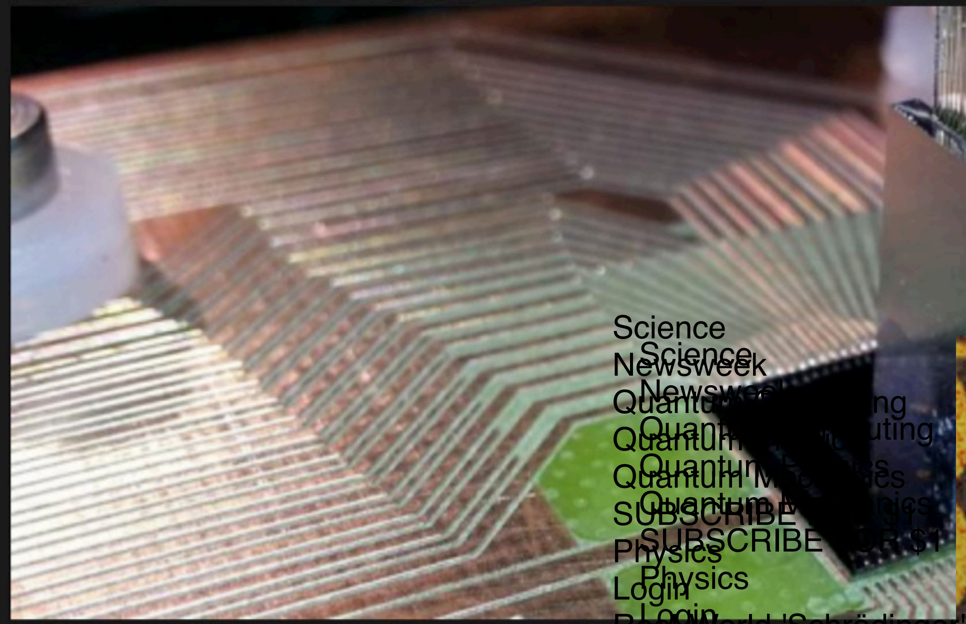
Experts agree that it's only a matte
technology will be able to crack th
secrets that keep the internet secu
current safeguards with post-quan
potential catastrophe seems years
the quantum technology being dev
advancing.

The new issue of the Security Ann
has four articles and a short story
interview with Peter Shor, the mat
quantum algorithm that now bears
will likely be another decade befor
capable of cracking the code. But
to hurry.

QUANTUM COMPUTING KILLS ENCRYPTION

by: Elliot Williams — 79 Comments

September 29, 2015



Imagine a world where the most widely used cryptogra
computers allow encrypted Internet data transactions to
listening. No more HTTPS, no more PGP. It sounds a litt
cryptographers interested in post-quantum crypto are w
threat of quantum computing to cryptography is already
activity in the field, so we felt it was time for a recap.

HOW BAD IS IT?

If you take the development of serious quantum compu
based on factoring primes or doing modular exponentia
and Diffie-Hellman are all in trouble. Specifically, Shor's
will render the previously difficult math problems that u
irrespective of chosen key length. That covers most cu
that's used in negotiating an SSL connection. That is (o
nearly every important encrypted transaction that touch

All is not doom and gloom, however. There are families of public-key algorithms that aren't solved by Shor's algorithm or any of the other known quantum algorithms, although they haven't been subjected to as much (classical) cryptanalysis and the algorithms and protocols aren't as polished yet. (More on this topic below.)

Newsweek — SUBSCRIBE FOR $1 — Login

Science | Quantum Computing | Quantum Physics | Quantum Mechanics | Physics

Real-World 'Schrödinger's Cat' Brings Quantum Computing Breakthrough

Published Jan 14, 2025 at 2:50 PM EST | **Updated** Jan 14, 2025 at 2:51 PM EST

COULD ADVANCED QUANTUM COMPUTING POSE A RISK TO BITCOIN SECURITY?

Rapid progress in quantum computing could pose a risk to certain types of bitcoin transactions. So how can we combat this risk?

DEBANJAN CHATTERJEE • OCT 16, 2021

HOME > TECHNICAL

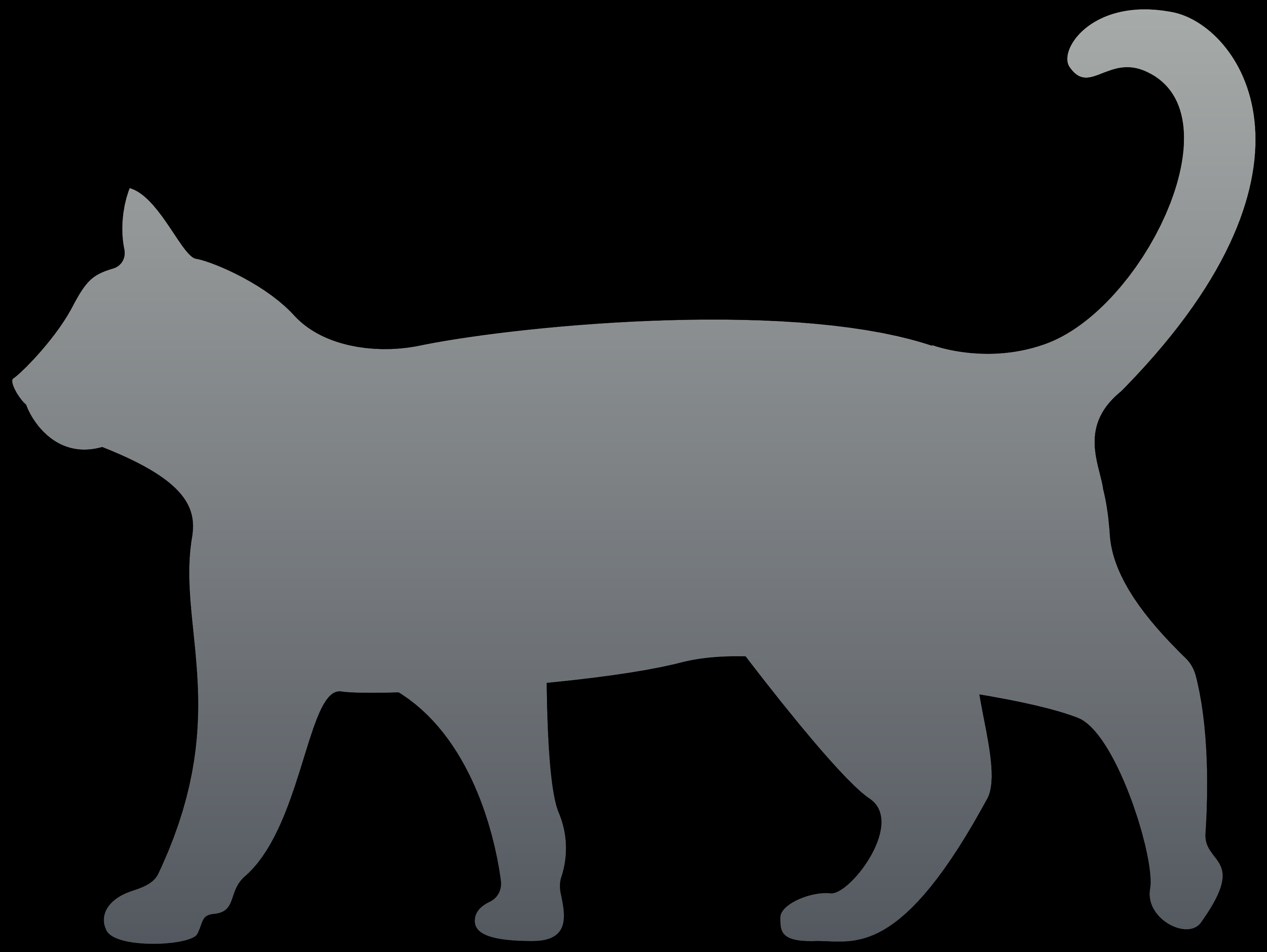
Rapid progress in quantum computing is predicted by some to have crucial ramifications in domains using public-key cryptography, such as the Bitcoin ecosystem.

Bitcoin's "asymmetric cryptography" is based on the principle of "one-way function," implying that a public key can be easily derived from its corresponding private key but not vice versa. This is because classical algorithms require an astronomical amount of time to perform such computations and consequently are impractical. However, Peter Shor's polynomial-time quantum algorithm run on a sufficiently-advanced quantum

Three questions

- What is the threat?
- How real is the threat?
- What can we do about it?

?



Quantum Computing

Quantum Computers

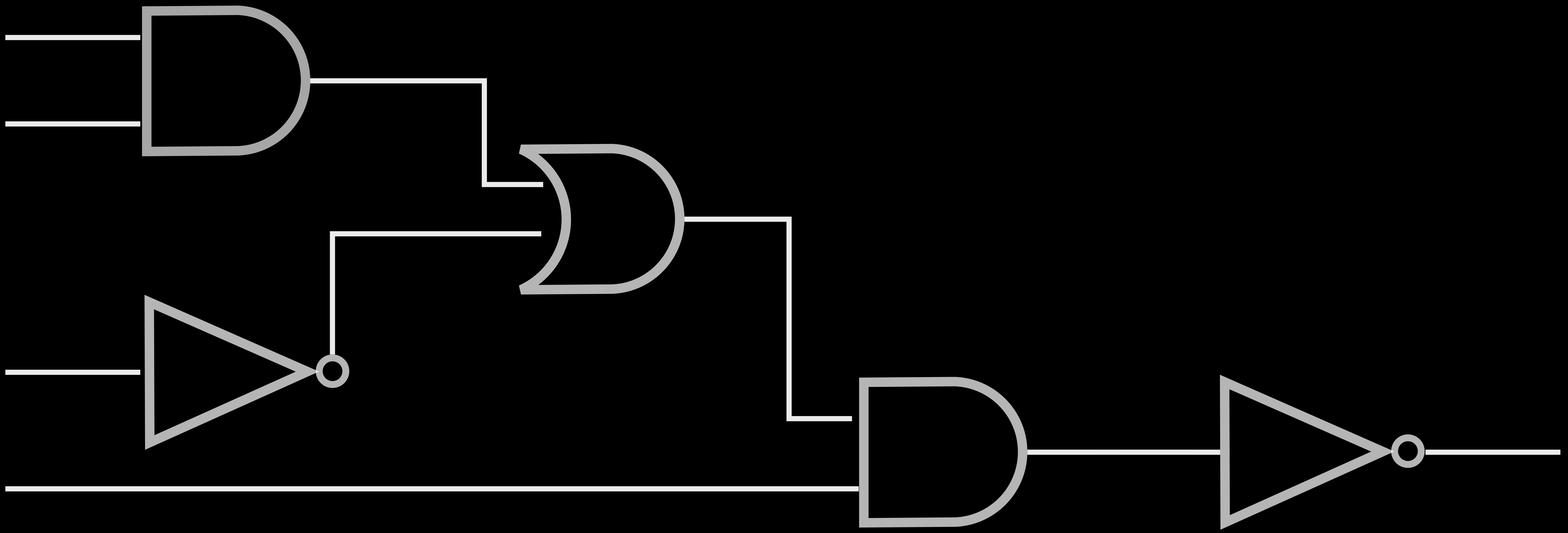
No physicists were permanently damaged in the creation of these following slides!

But it was a close thing!

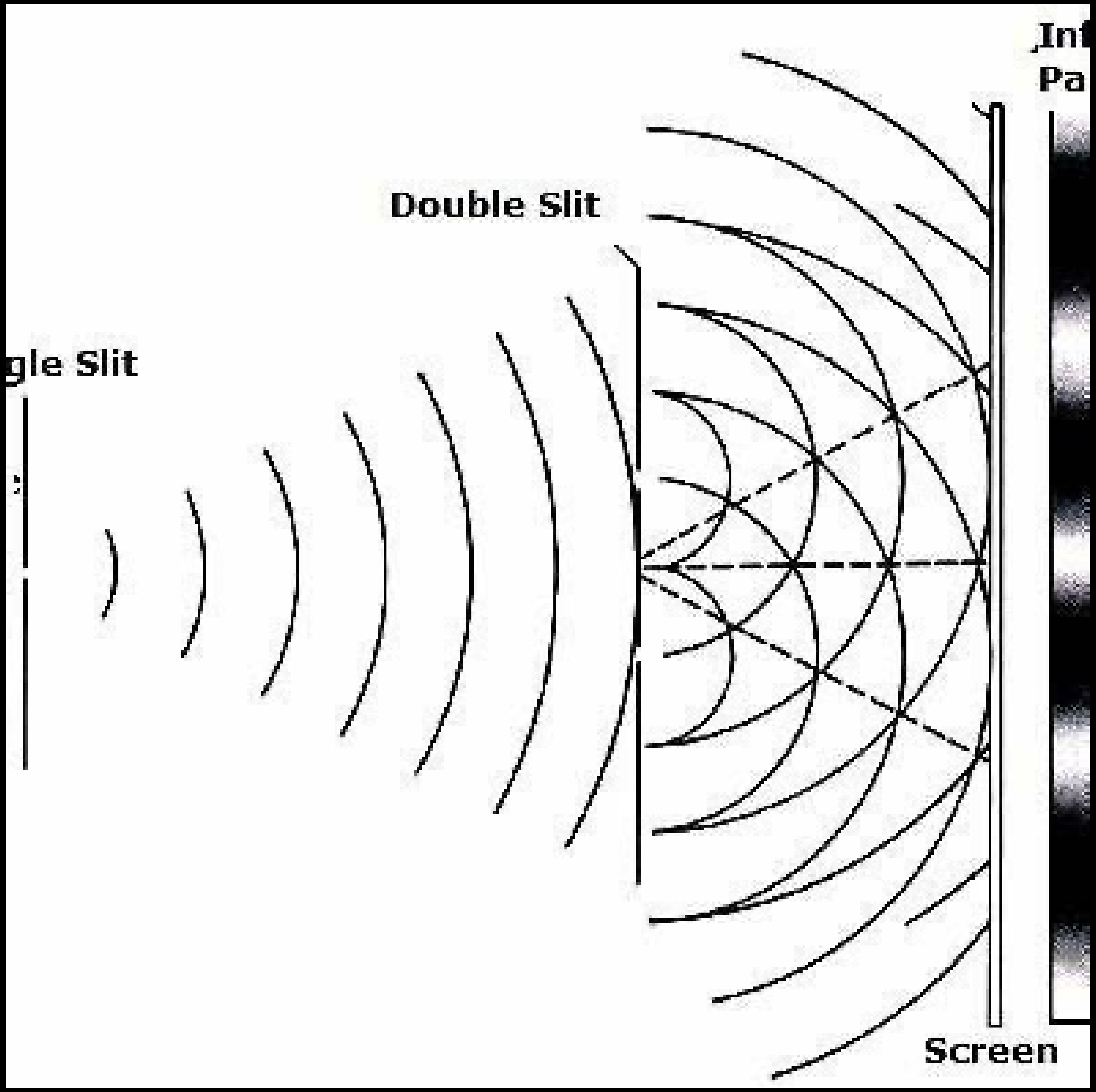
- Not an evolution of classical computers
- Based on the quantum properties of Superposition and Entanglement
- Built with Qubits and Gates
- I will be talking about Universal Quantum Computers, not other variants like Adiabatic Quantum Computers

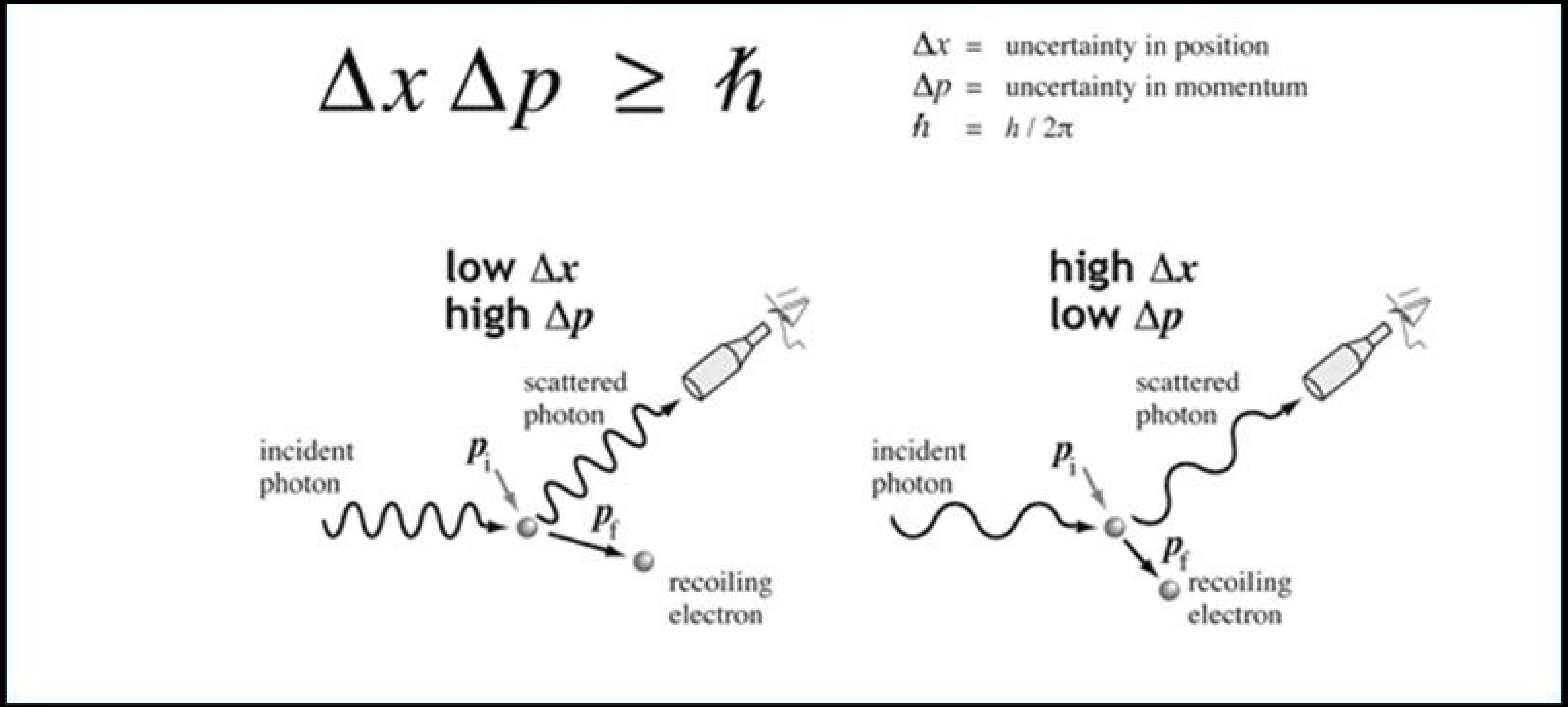
Classical Computing: the bit

Classical Computing: the circuit



Enter quantum mechanics

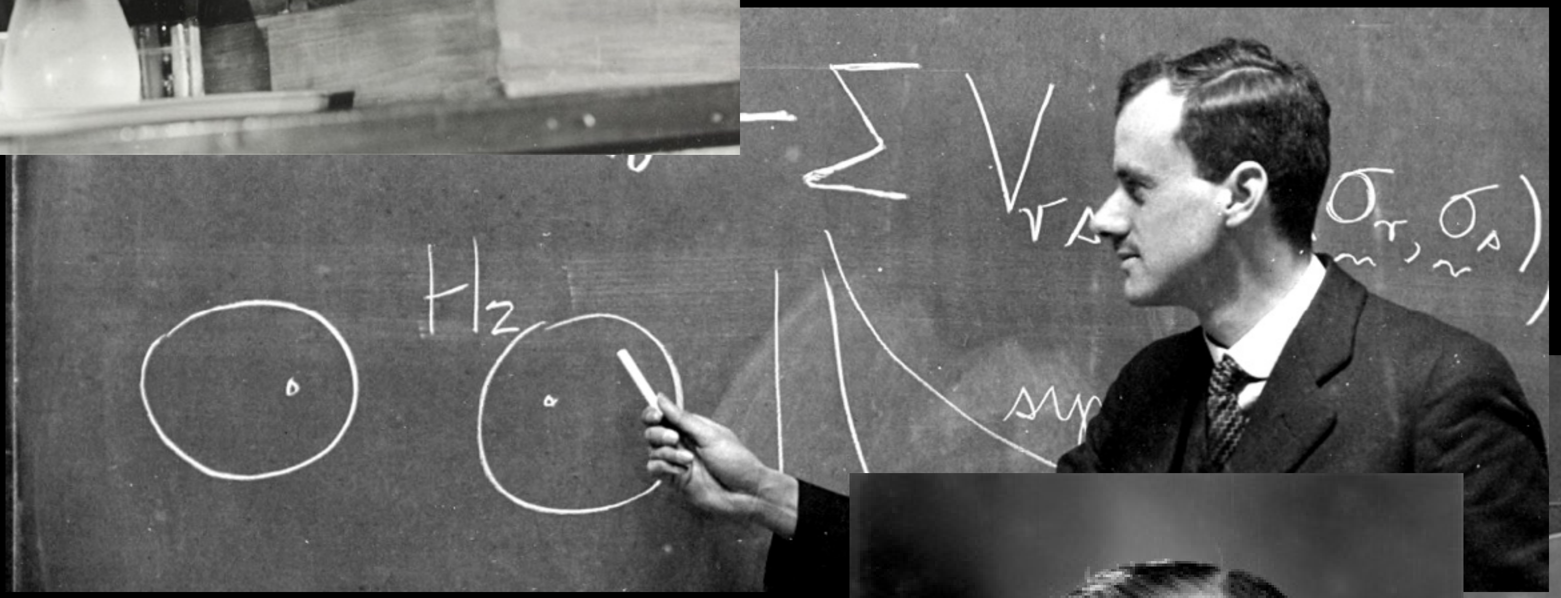




Hall of fame (incomplete)

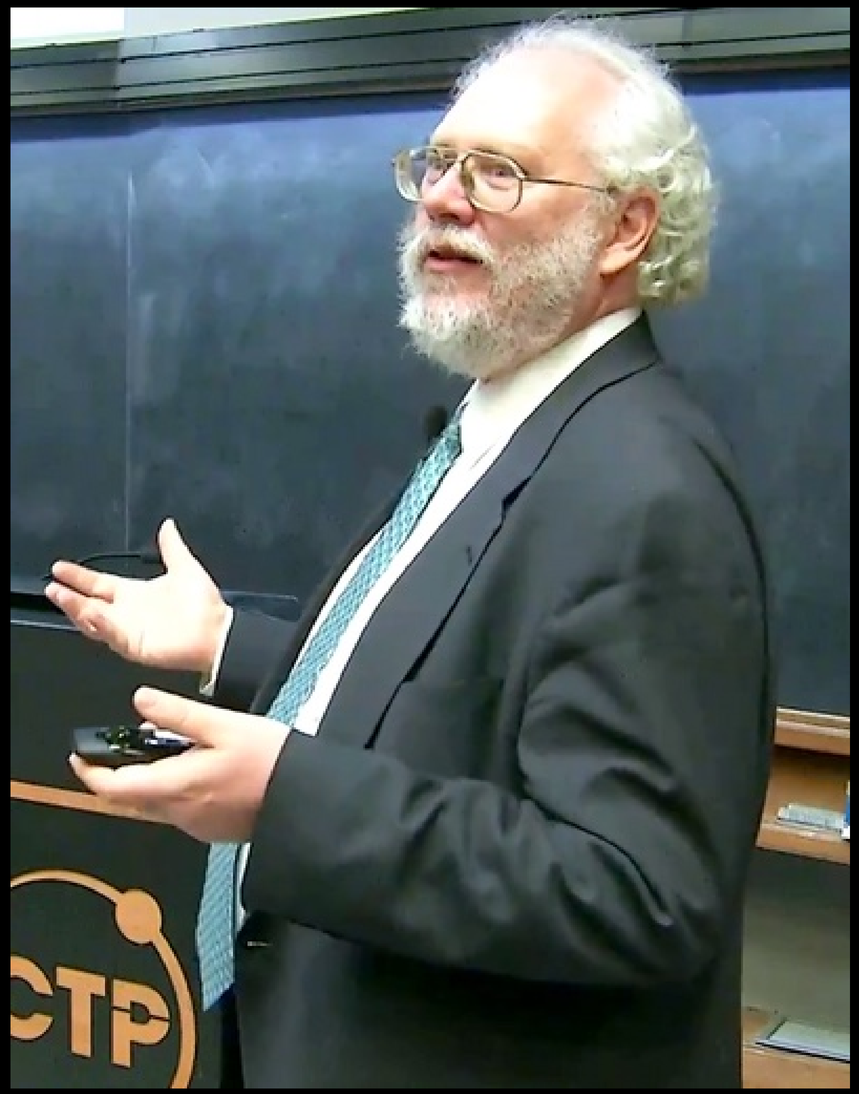
Erwin Schrödinger

Paul Dirac



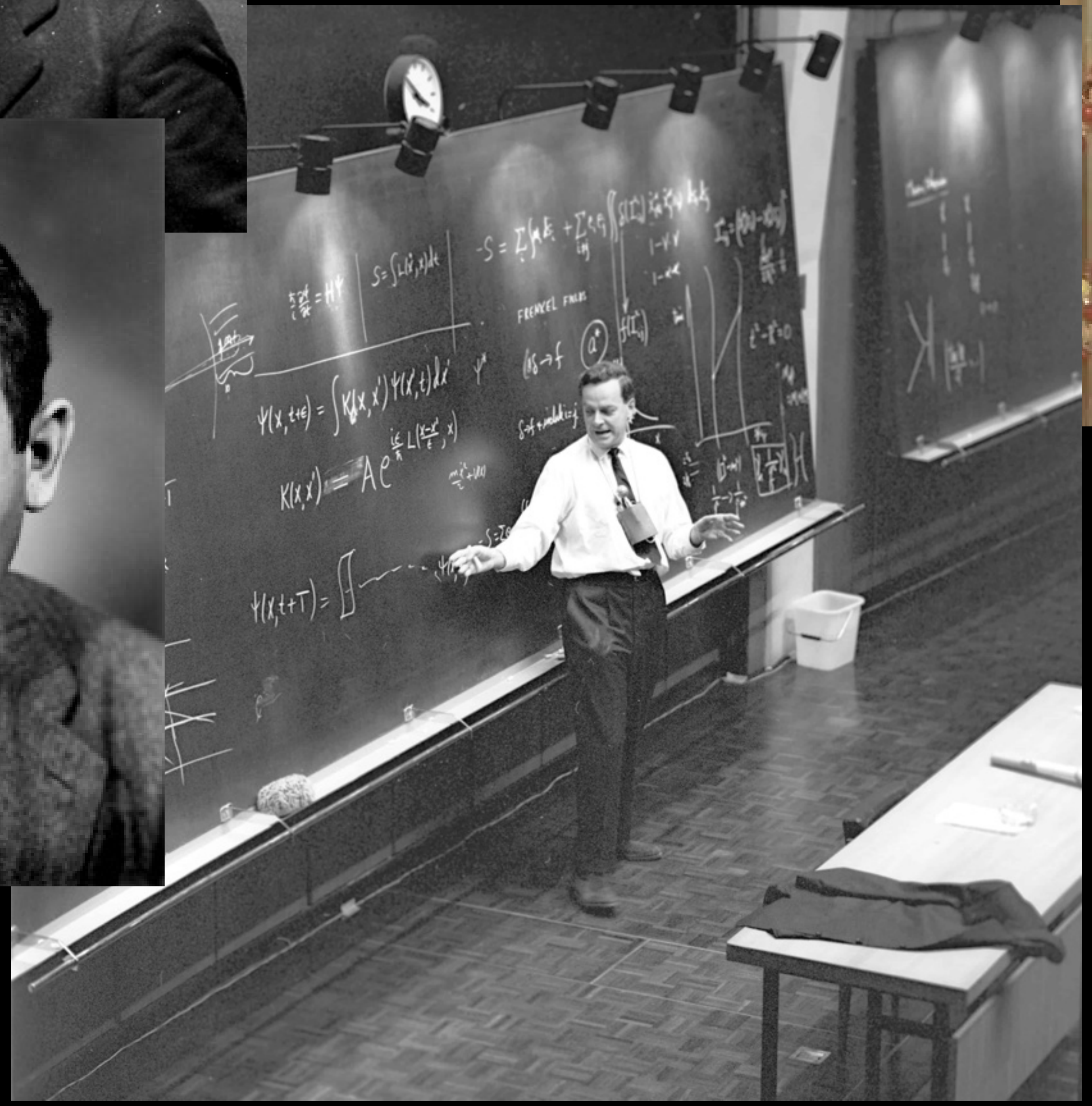
Paul Benioff

Peter Shor



David Deutsch

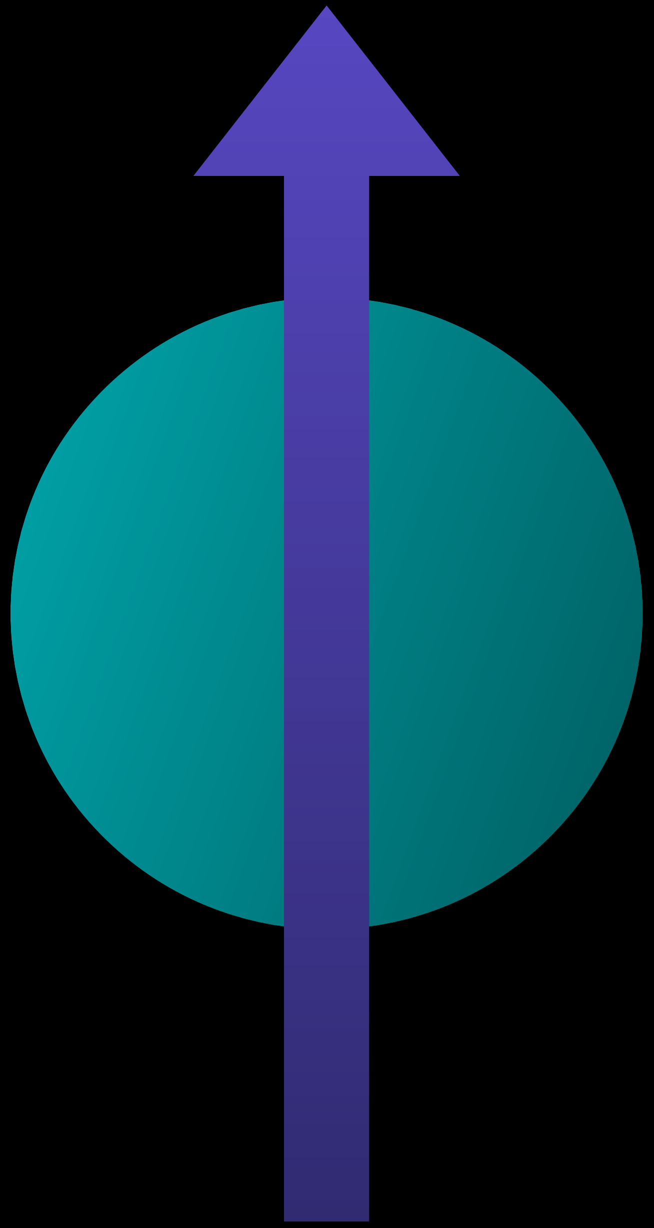
John von Neumann



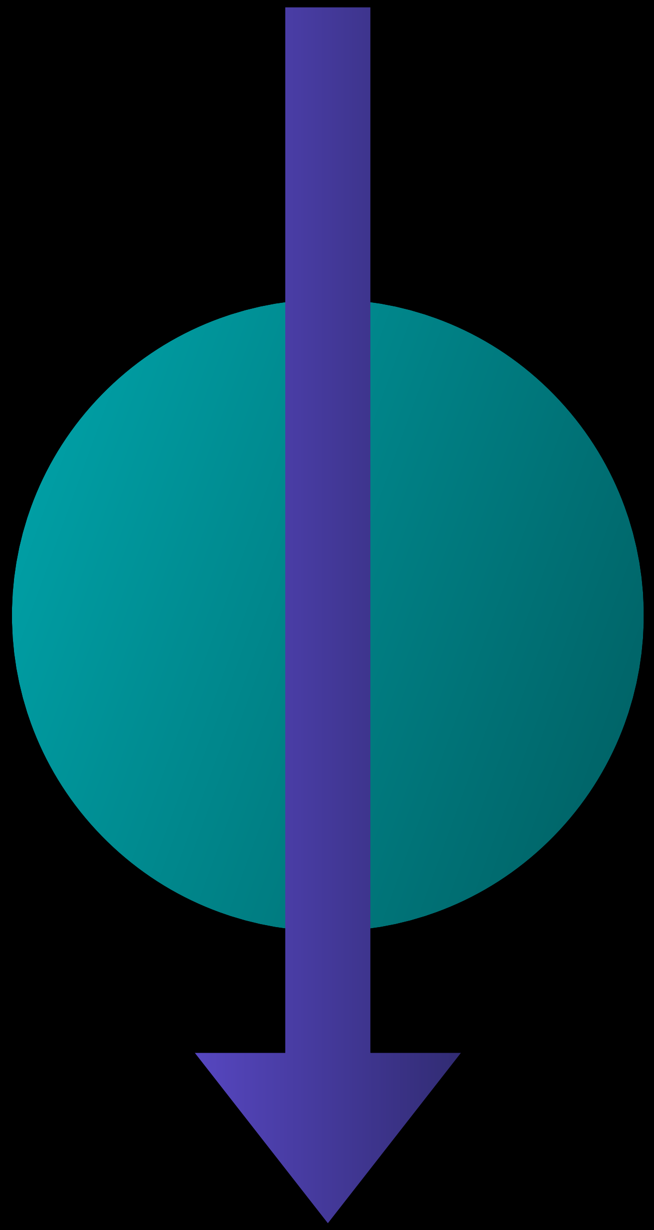
Richard Feynman

Charles Bennet

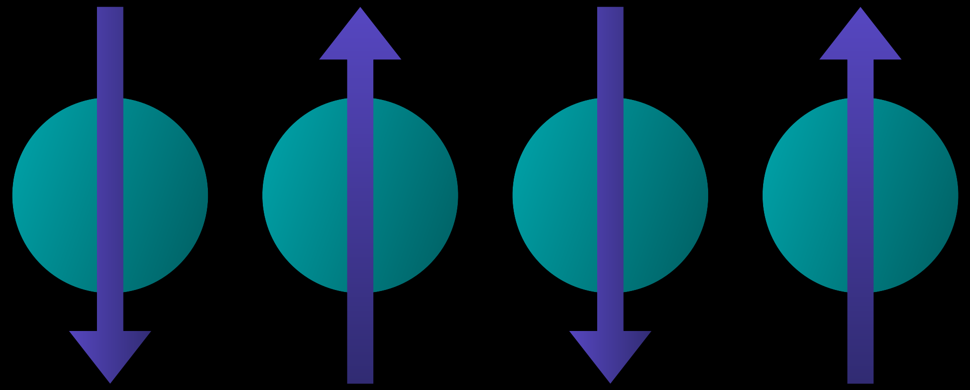
Quantum Computing: Qubits



$$\Longleftrightarrow |1\rangle$$



$$\Longleftrightarrow |0\rangle$$

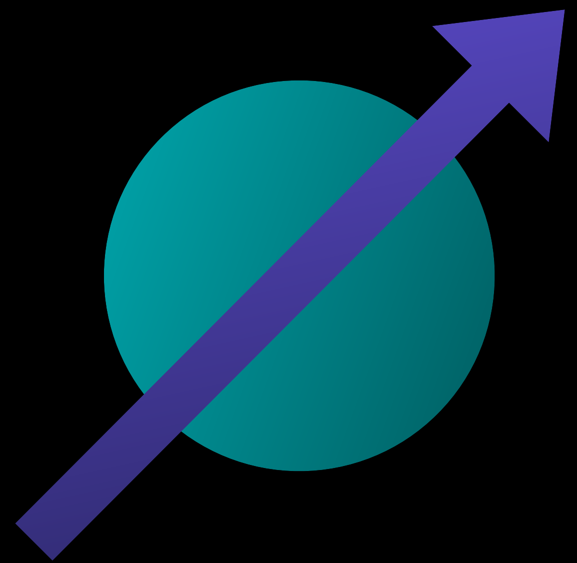


$$\Longleftrightarrow |0101\rangle \Longleftrightarrow |5\rangle$$

Question

Is this coin
heads or tails?

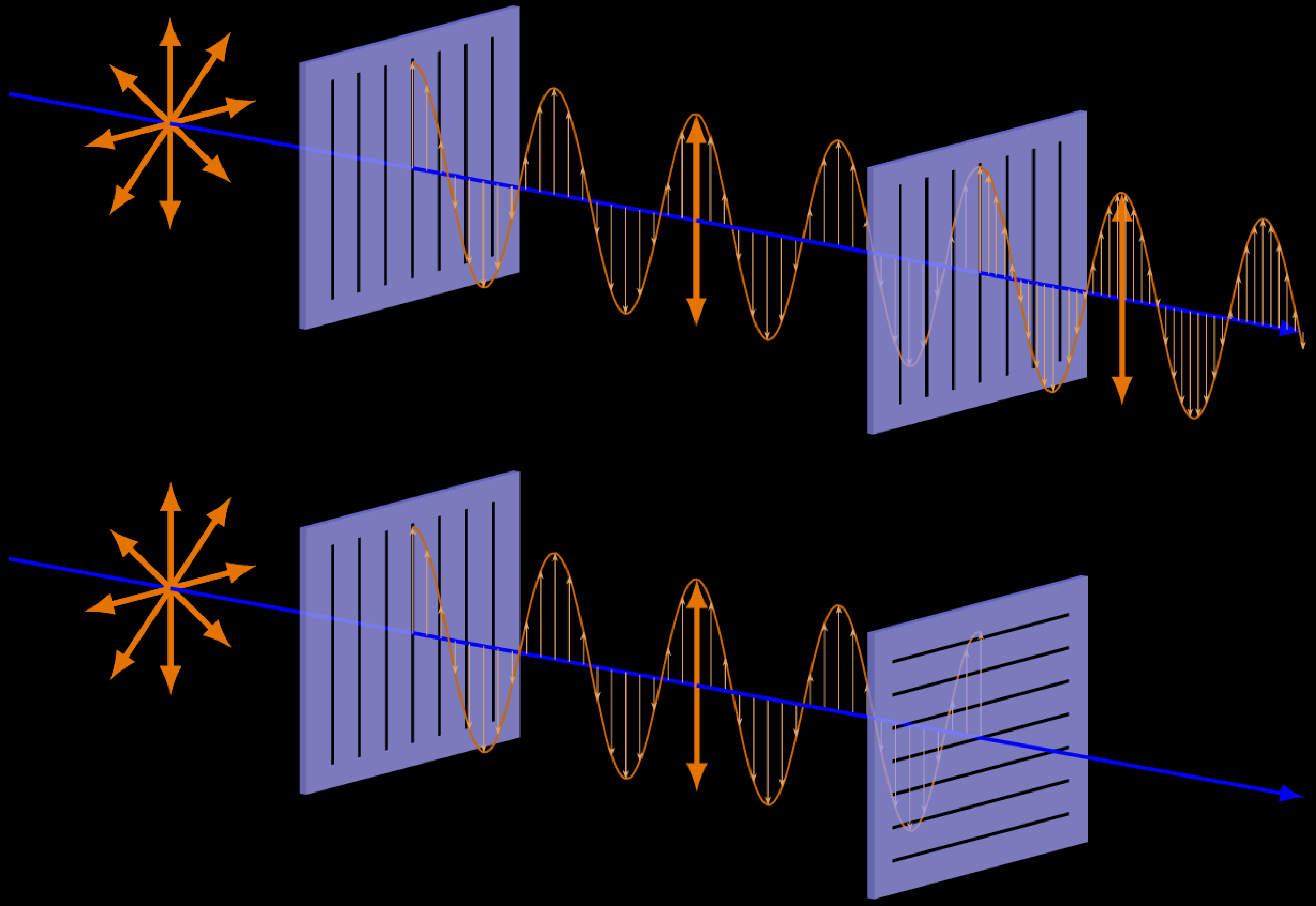
Superposition



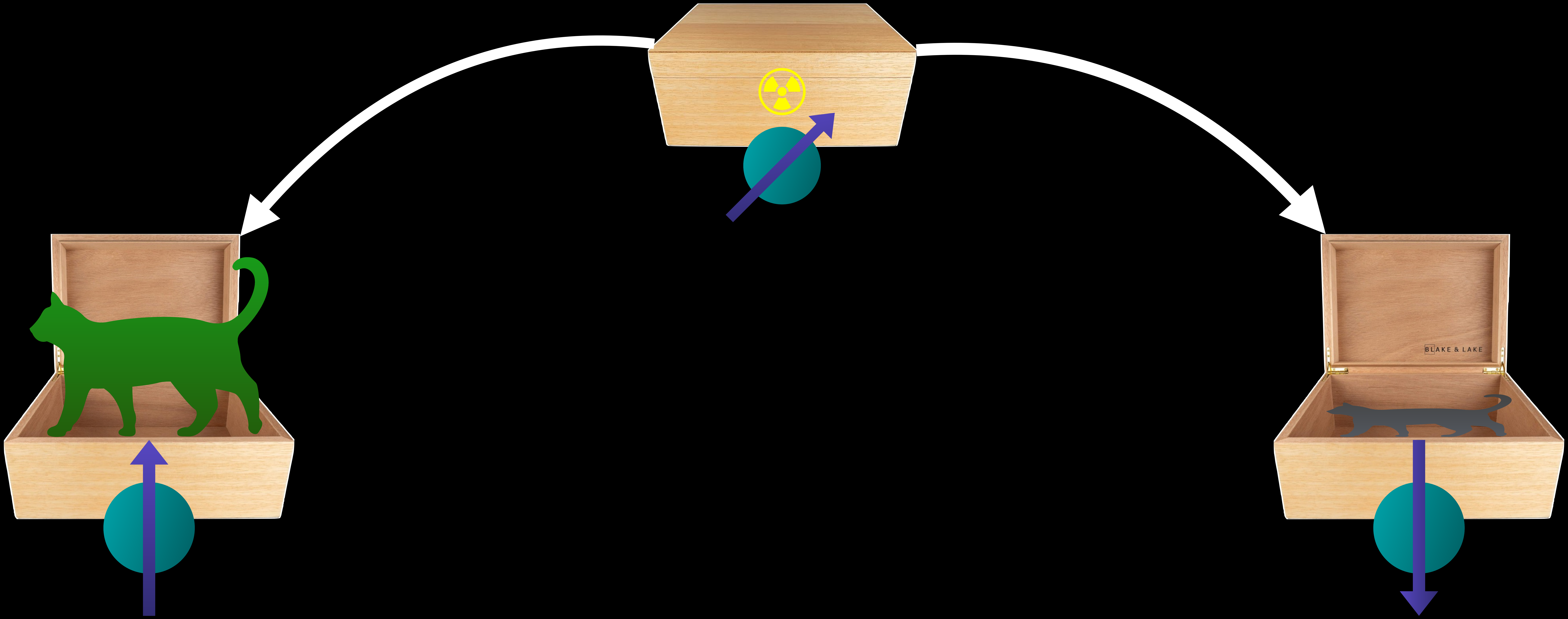
$$\Longleftrightarrow a\,|0\rangle + b\,|1\rangle$$

each qubit, in superposition, can be in infinite states

Measurement



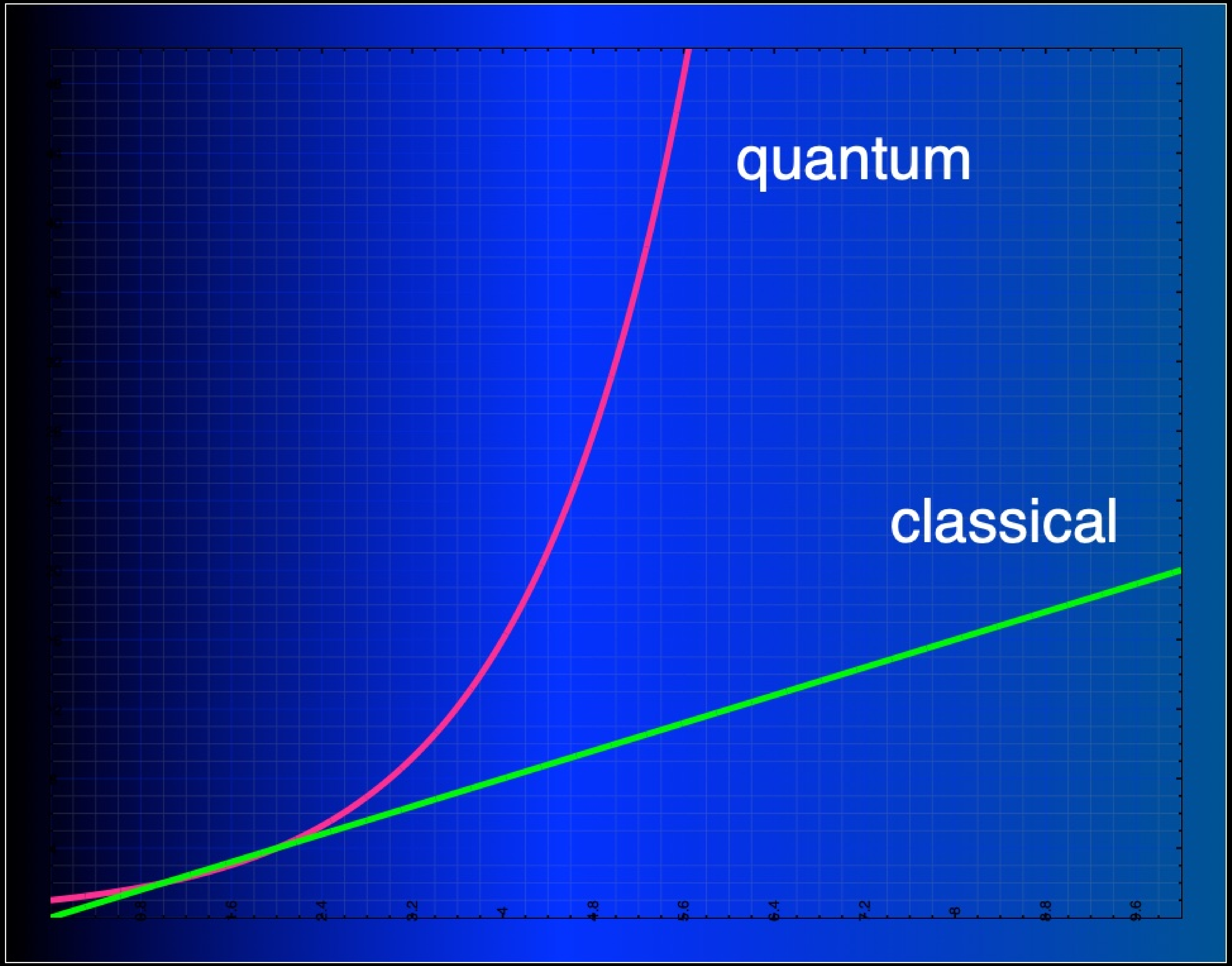
Superposition



States for (qu)bits

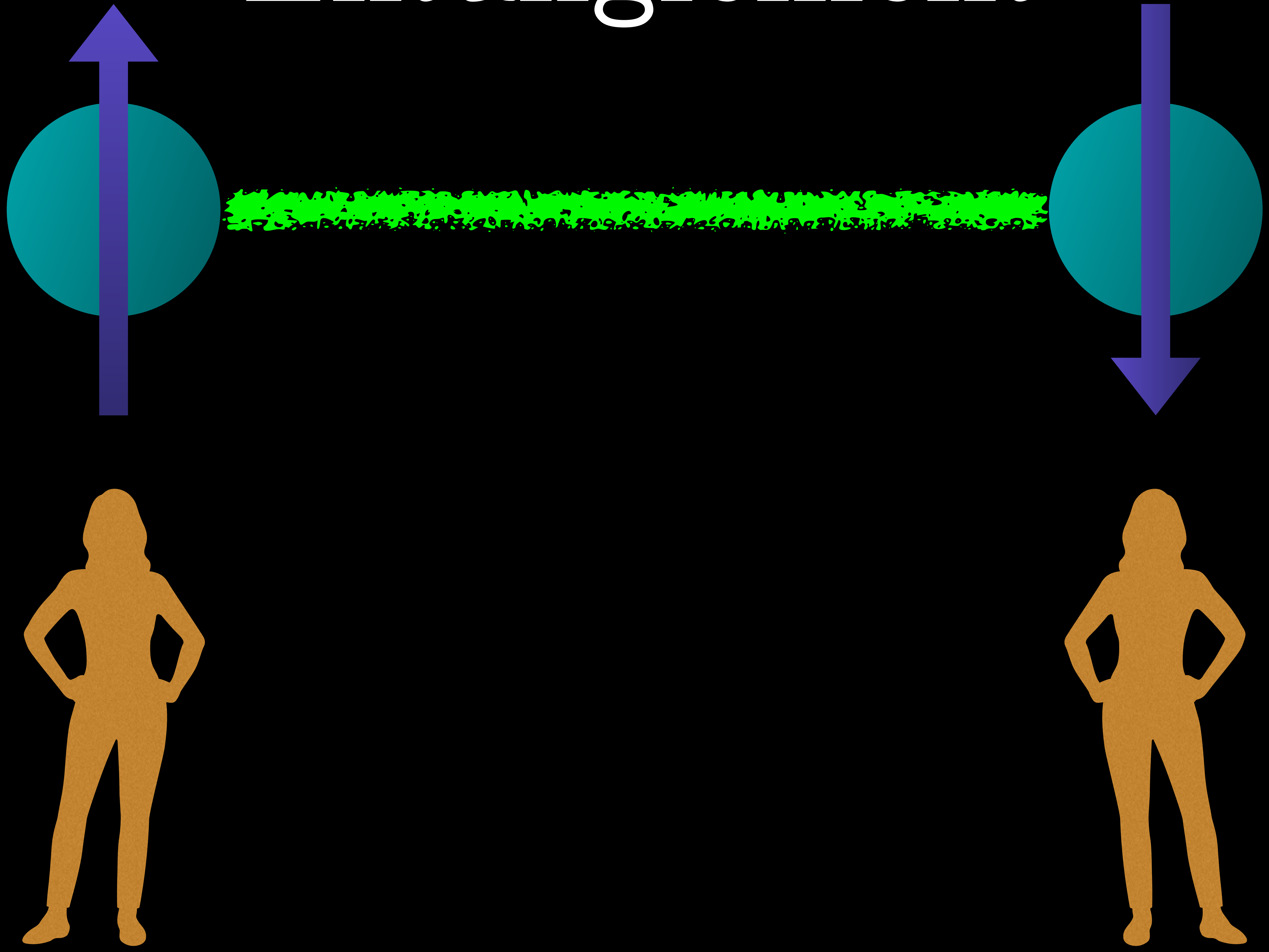
n bits → $2n$ states

n qubits → 2^n states



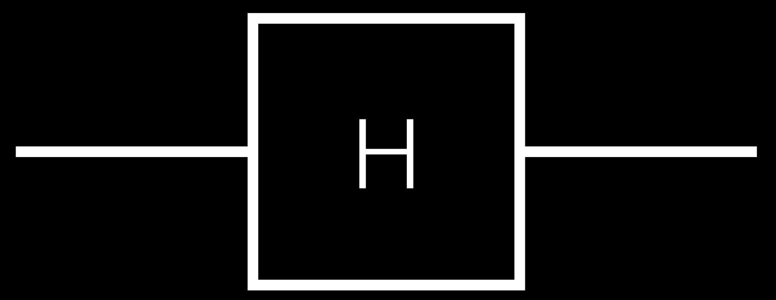
"Verschränkung"

Entanglement

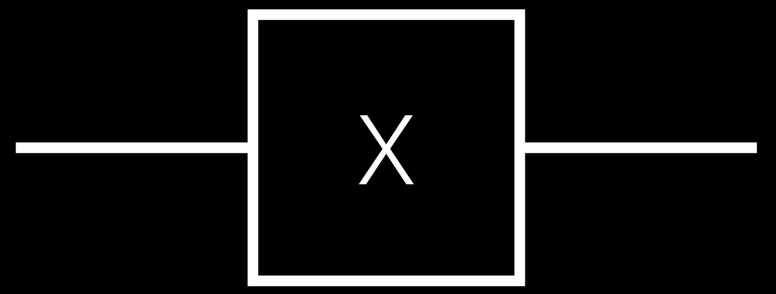


linkedin.com/in/mswimmer

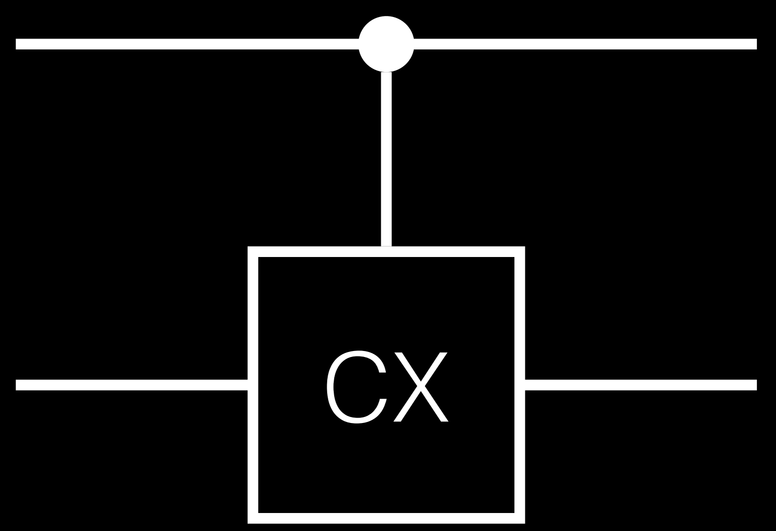
Quantum gates



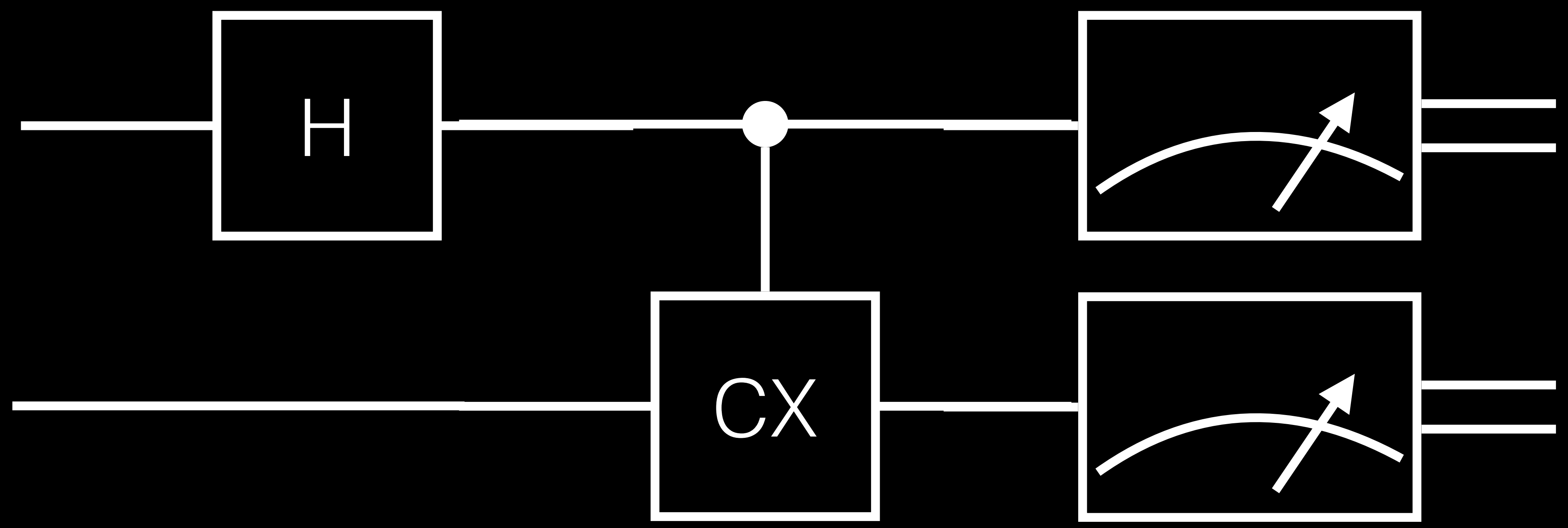
Hadamard



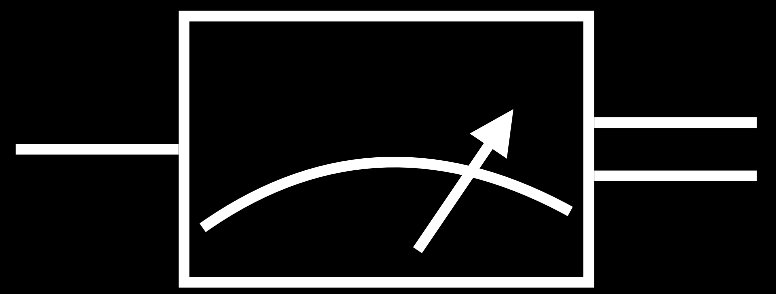
NOT



Controlled NOT

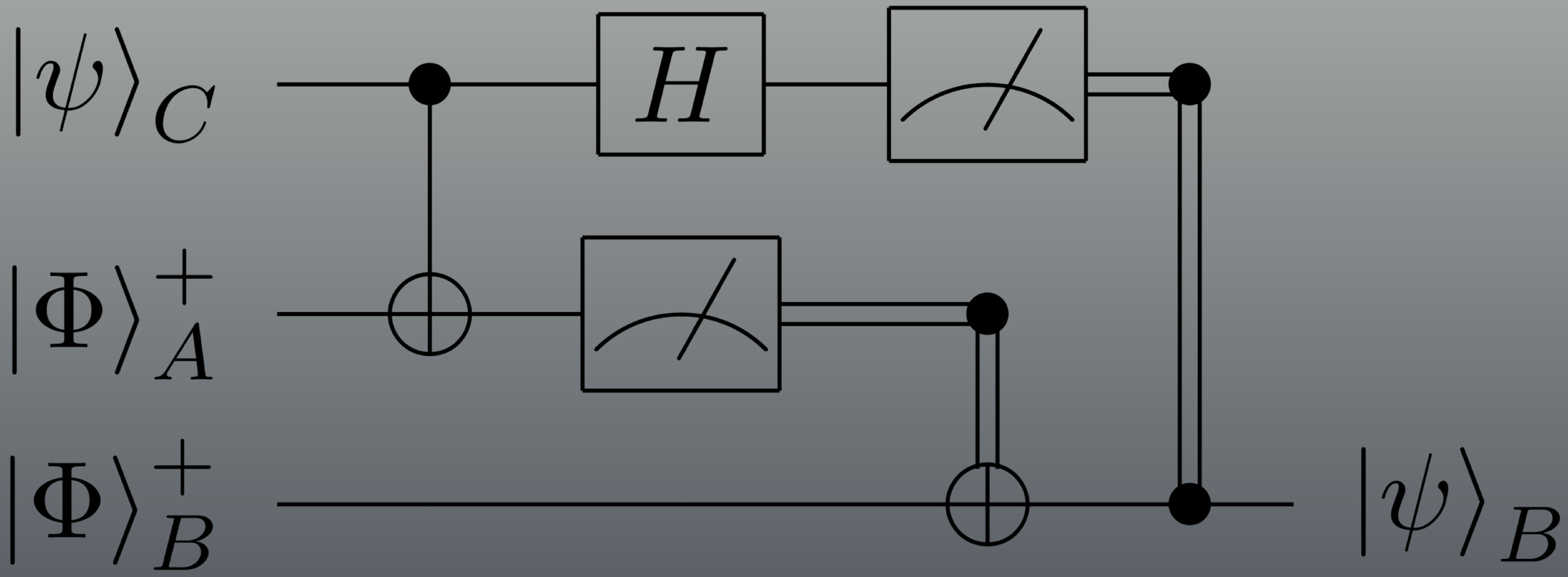


and many more



Measurement
resulting in a classical bit

Quantum Programming



Breaking RSA

Disclaimer

No cryptographers were permanently damaged in the production of the following slides

BUT, there will be math

Breaking RSA

This means factoring large integers

$$s \times t = N$$

N is shared, s and t are secret

The attacker's goal: find s or t

Factoring is hard: Naive approach

```python
def calculate_primes_up_to(n):
    primes = set()
    for a in range(2, int(n/2)+1):
        if not any(a % b == 0 for b in primes):
            primes.add(a)
    return sorted(primes)
```

```python
def naive_factor(N, primes):
    for i in primes:
        for j in [p for p in primes if p < i]:
            if i * j == N:
                return i, j
```

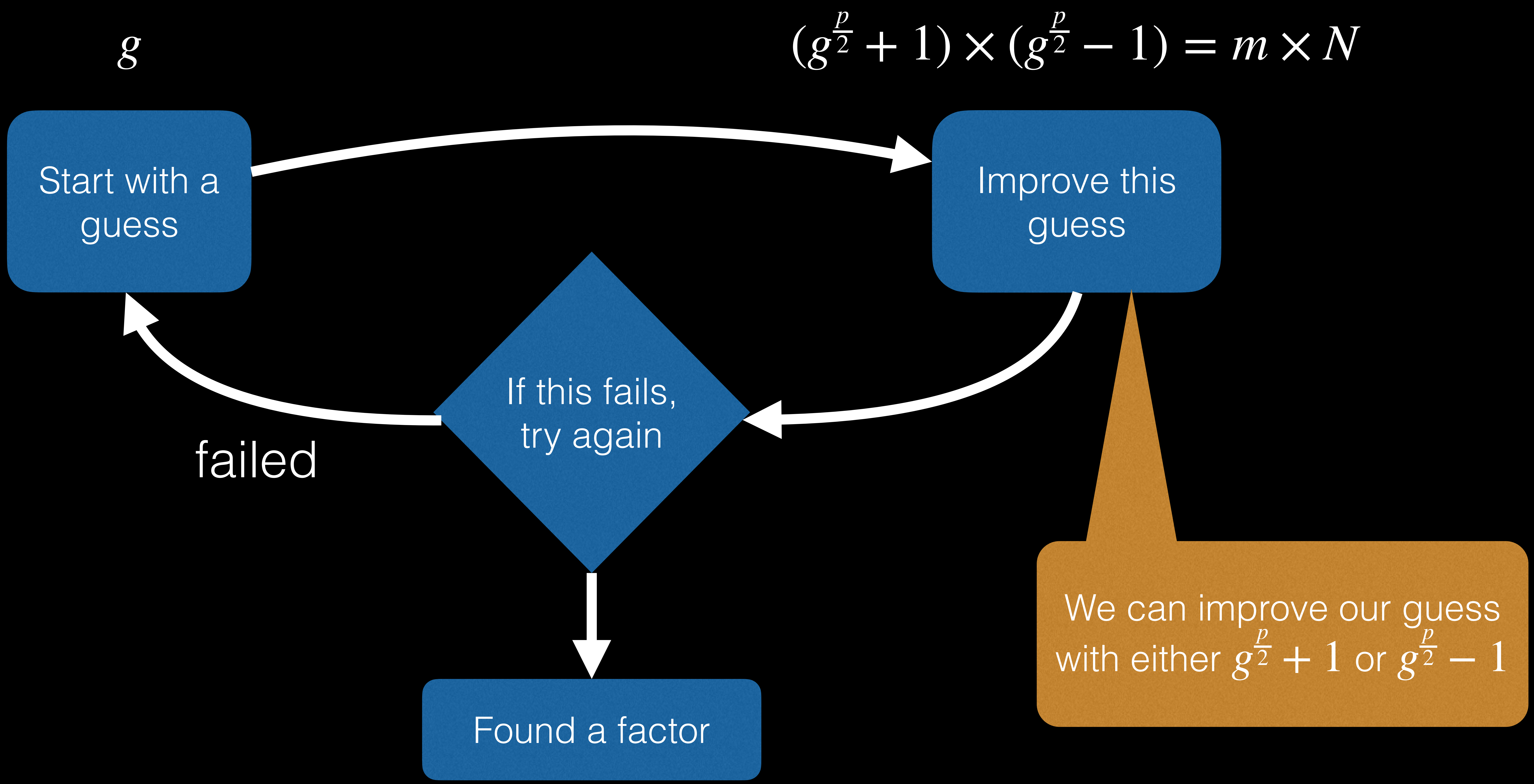
Factor a 38 bit integer: 249976000567

```python
N = 249976000567
primes = calculate_primes_up_to(N)
s, t = naive_factor(N, primes)
print(s, t, s * t)
```

Never completed on my machine. A 25 bit key solved in over 5 hours.

RSA challenges solved up to 829 bits

Guess and check



N=15

1. Guess g = 3
2. gcd(15, 3) == 3
3. Found factors: 3, 5

N=15

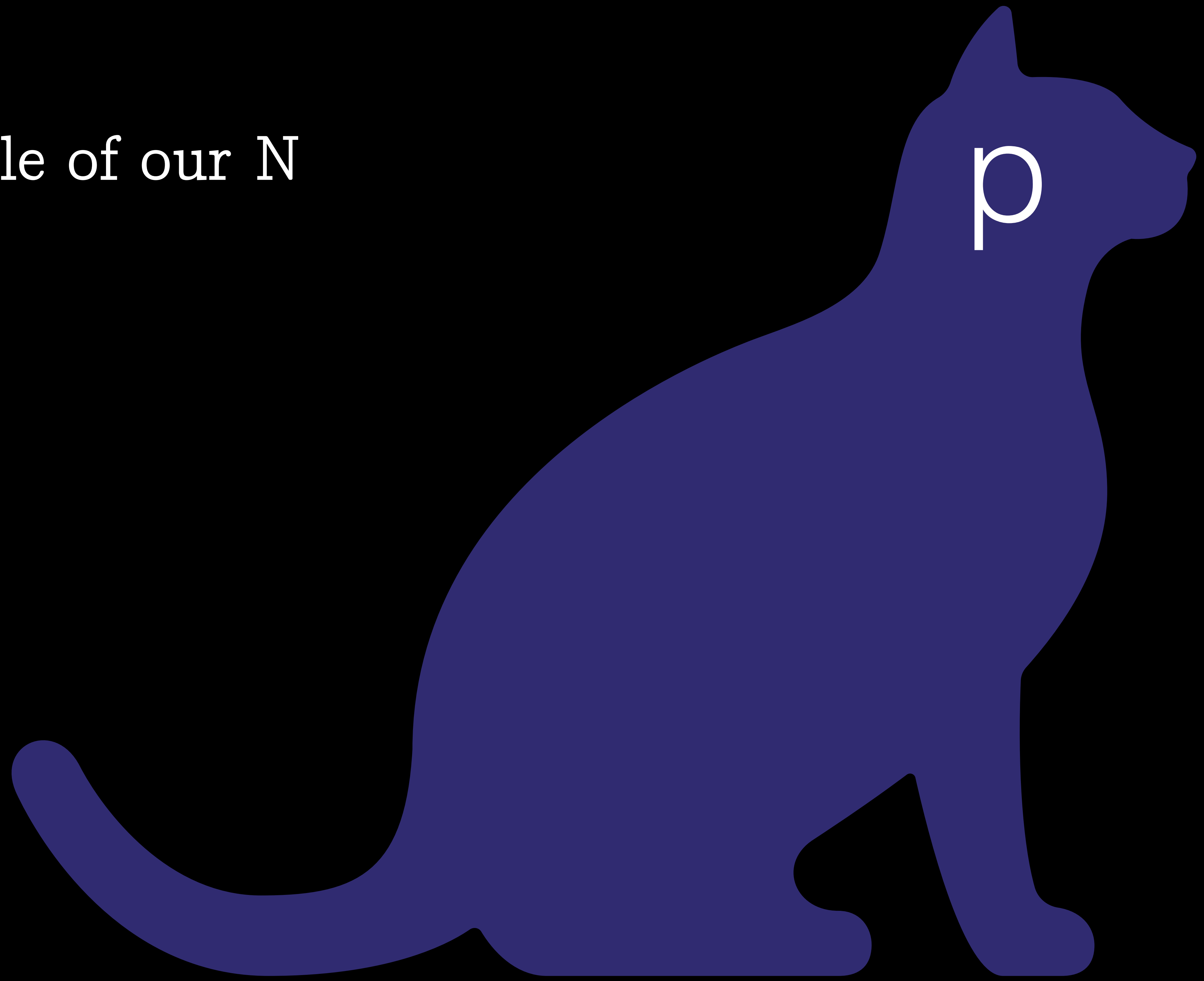
1. Guess g = 7
2. No common divisor
3. Let's improve our guess with $g^{\frac{p}{2}} - 1$
4. Trying p=2
5. New guess $7^{\frac{2}{2}} - 1 = 7 - 1 = 6$
6. gcd(15, 6) == 3
7. Found factors: 3, 5

N=15

1. Guess g = 2
2. No common divisor
3. Let's improve our guess with $g^{\frac{p}{2}} - 1$
4. Trying p=2
5. new guess: $2^{\frac{2}{2}} - 1 = 2 - 1 = 1$
6. 1 is a trivial divisor and is rejected
7. Let's use $g^{\frac{p}{2}} + 1$ instead
8. new guess: $2^{\frac{2}{2}} + 1 = 2 + 1 = 3$
9. gcd(15, 3) == 3
10. Found factors: 5, 3

p is the problem

- For large values of N, it becomes hard to find the right p
- Reflecting on this method
  - We have $(g^{\frac{p}{2}} + 1) \times (g^{\frac{p}{2}} - 1) = m \times N$
  - Multiplying our two guess candidates we get some multiple of our N
- Multiply this out
  - $g^p = m \times N + 1$
  - Special case of $g^p = m \times N + r$
  - Meaning g^p is some multiple of N plus a remainder



$N = 15, g = 7$

$$g^x = m \times N + r$$

$$7^0 = 1 = 0 \times 15 + 1$$
$$7^1 = 7 = 0 \times 15 + 7$$
$$7^2 = 49 = 3 \times 15 + 4$$
$$7^3 = 343 = 22 \times 15 + 13$$
$$7^4 = 2401 = 160 \times 15 + 1$$
$$7^5 = 16807 = 1120 \times 15 + 7$$
$$7^6 = 117649 = 7843 \times 15 + 4$$
$$7^7 = 823543 = 54902 \times 15 + 13$$
$$7^8 = 5764801 = 384320 \times 15 + 1$$
$$7^9 = 40353607 = 2690240 \times 15 + 7$$

N = 15, g = 7

$g^x = m \times N + r$

$7^0 = 1 = 0 \times 15 + 1$
$7^1 = 7 = 0 \times 15 + 7$
$7^2 = 49 = 3 \times 15 + 4$
$7^3 = 343 = 22 \times 15 + 13$
$7^4 = 2401 = 160 \times 15 + 1$
$7^5 = 16807 = 1120 \times 15 + 7$
$7^6 = 117649 = 7843 \times 15 + 4$
$7^7 = 823543 = 54902 \times 15 + 13$
$7^8 = 5764801 = 384320 \times 15 + 1$
$7^9 = 40353607 = 2690240 \times 15 + 7$

We need to find p so that

$$g^{1+0} \cong g^{p+x} \cong g^{2p+x} \cong \cdots \pmod{N}$$

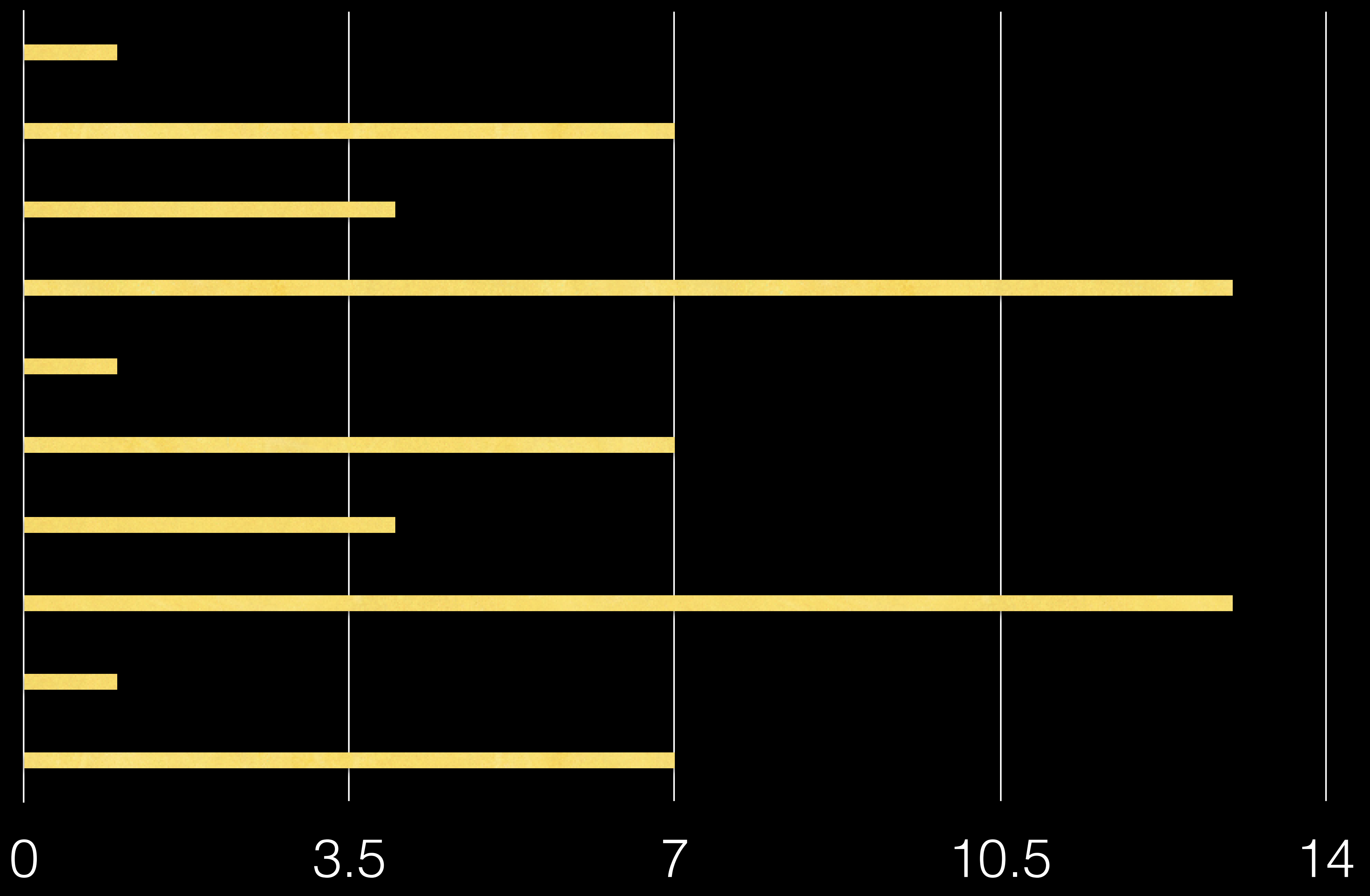
$N = 15, g = 7$

$$
\begin{aligned}
7^0 &= 1 = 0 \times 15 + 1 \\
7^1 &= 7 = 0 \times 15 + 7 \\
7^2 &= 49 = 3 \times 15 + 4 \\
7^3 &= 343 = 22 \times 15 + 13 \\
7^4 &= 2401 = 160 \times 15 + 1 \\
7^5 &= 16807 = 1120 \times 15 + 7 \\
7^6 &= 117649 = 7843 \times 15 + 4 \\
7^7 &= 823543 = 54902 \times 15 + 13 \\
7^8 &= 5764801 = 384320 \times 15 + 1 \\
7^9 &= 40353607 = 2690240 \times 15 + 7
\end{aligned}
$$

There is a pattern to the remainders

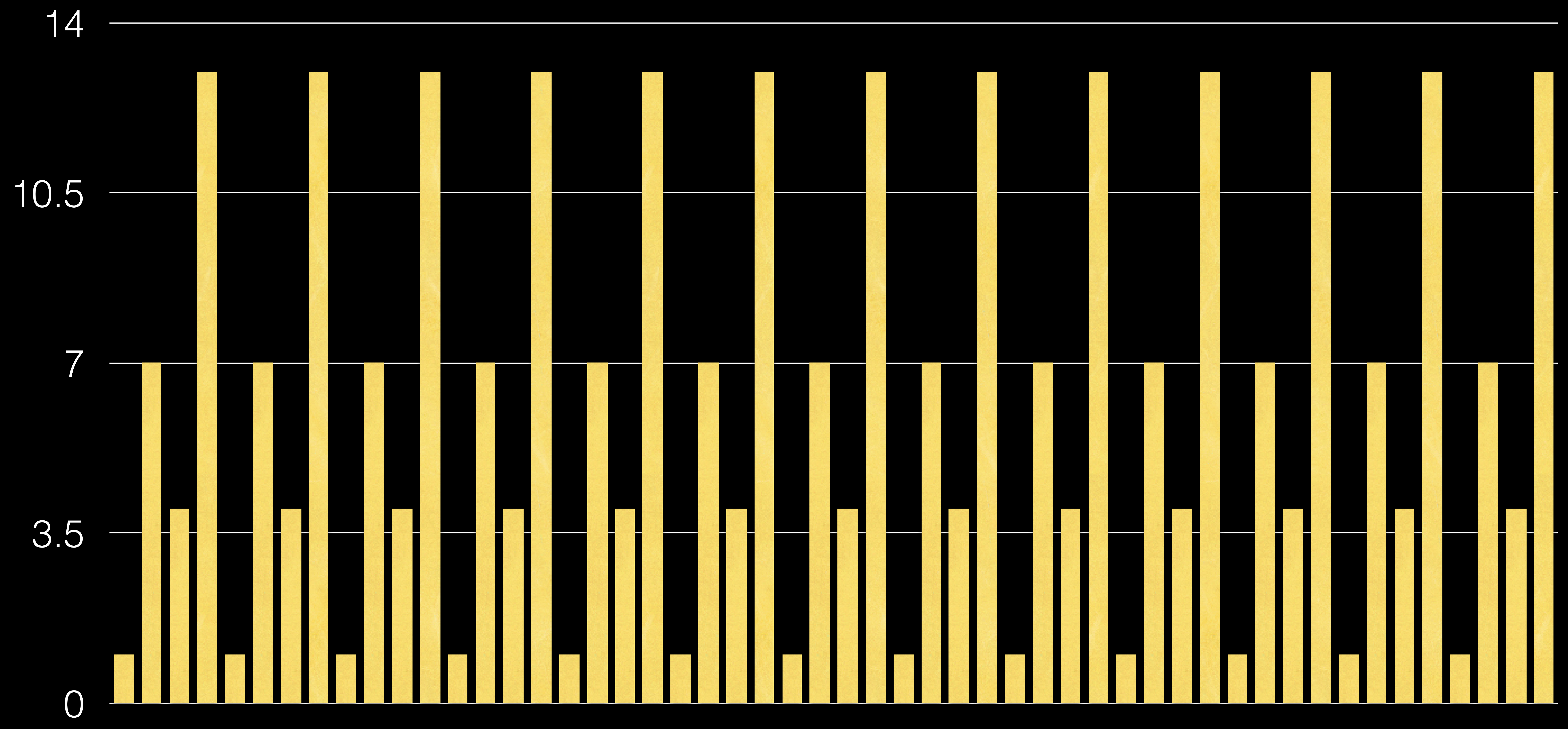
$N = 15, g = 7$

$$7^0 = 1 = 0 \times 15 + 1$$
$$7^1 = 7 = 0 \times 15 + 7$$
$$7^2 = 49 = 3 \times 15 + 4$$
$$7^3 = 343 = 22 \times 15 + 13$$
$$7^4 = 2401 = 160 \times 15 + 1$$
$$7^5 = 16807 = 1120 \times 15 + 7$$
$$7^6 = 117649 = 7843 \times 15 + 4$$
$$7^7 = 823543 = 54902 \times 15 + 13$$
$$7^8 = 5764801 = 384320 \times 15 + 1$$
$$7^9 = 40353607 = 2690240 \times 15 + 7$$



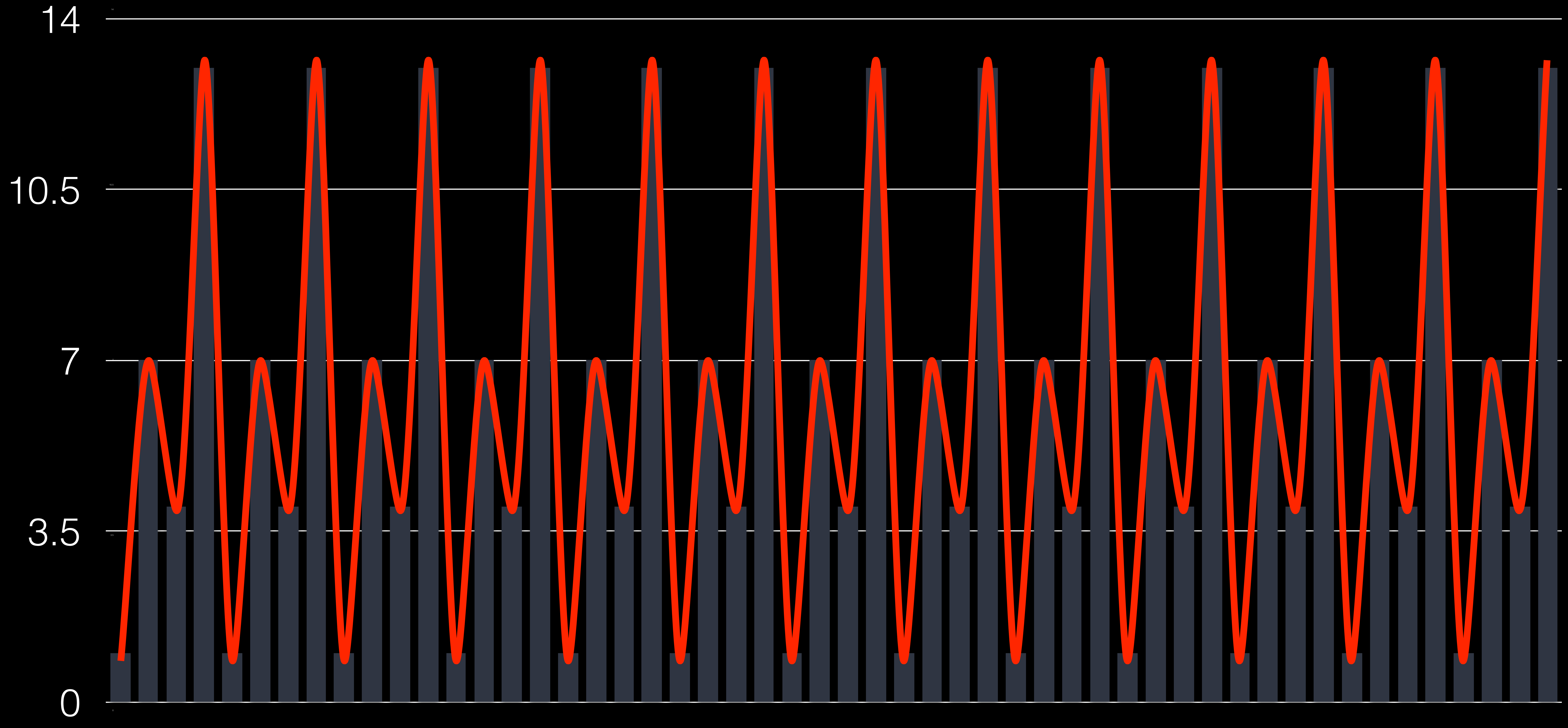
linkedin.com/in/mswimmer

$N = 15, g = 7$



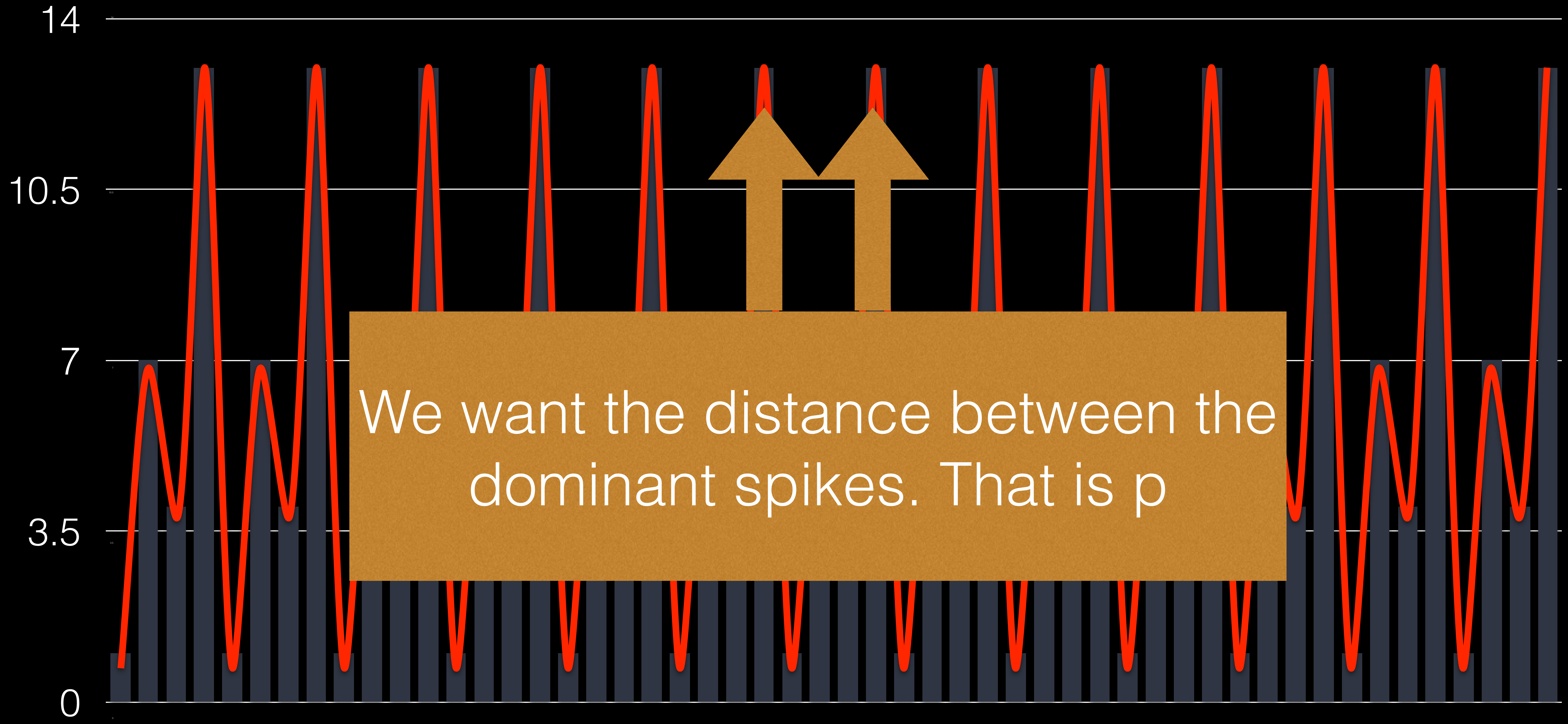
linkedin.com/in/mswimmer

$N = 15, g = 7$



The remainders look like a signal

$N = 15, g = 7$

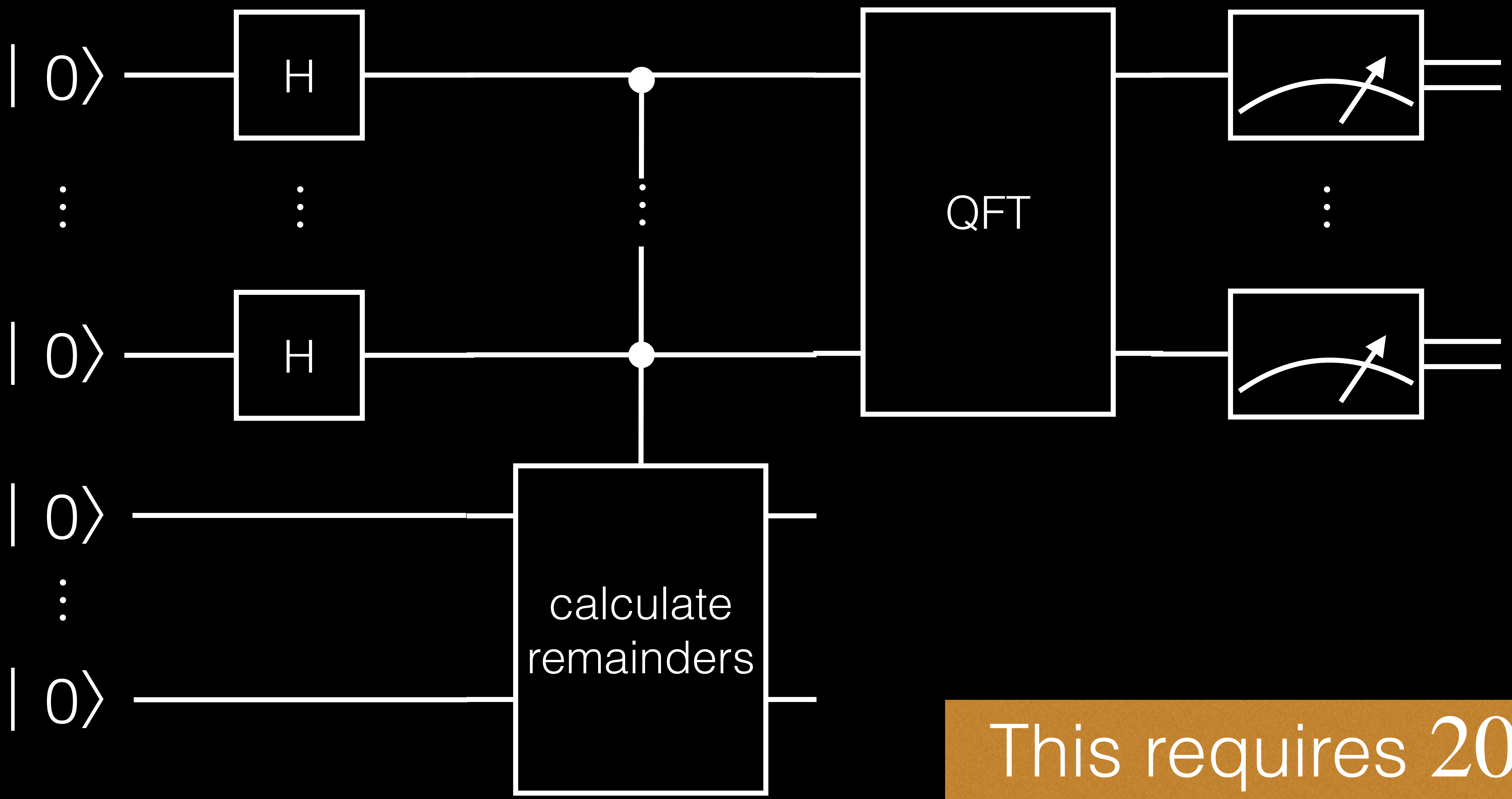


Can we use a Fourier Transform?

Not so fast Fourier Transforms

- Fourier Transforms can help us find the composite wave functions
- And therefore the dominant wave
- BUT, 'Fast' Fourier Transforms are not fast enough for large N
- Enter the Quantum Fourier Transform

By Lucas V. Barbosa - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=24830373

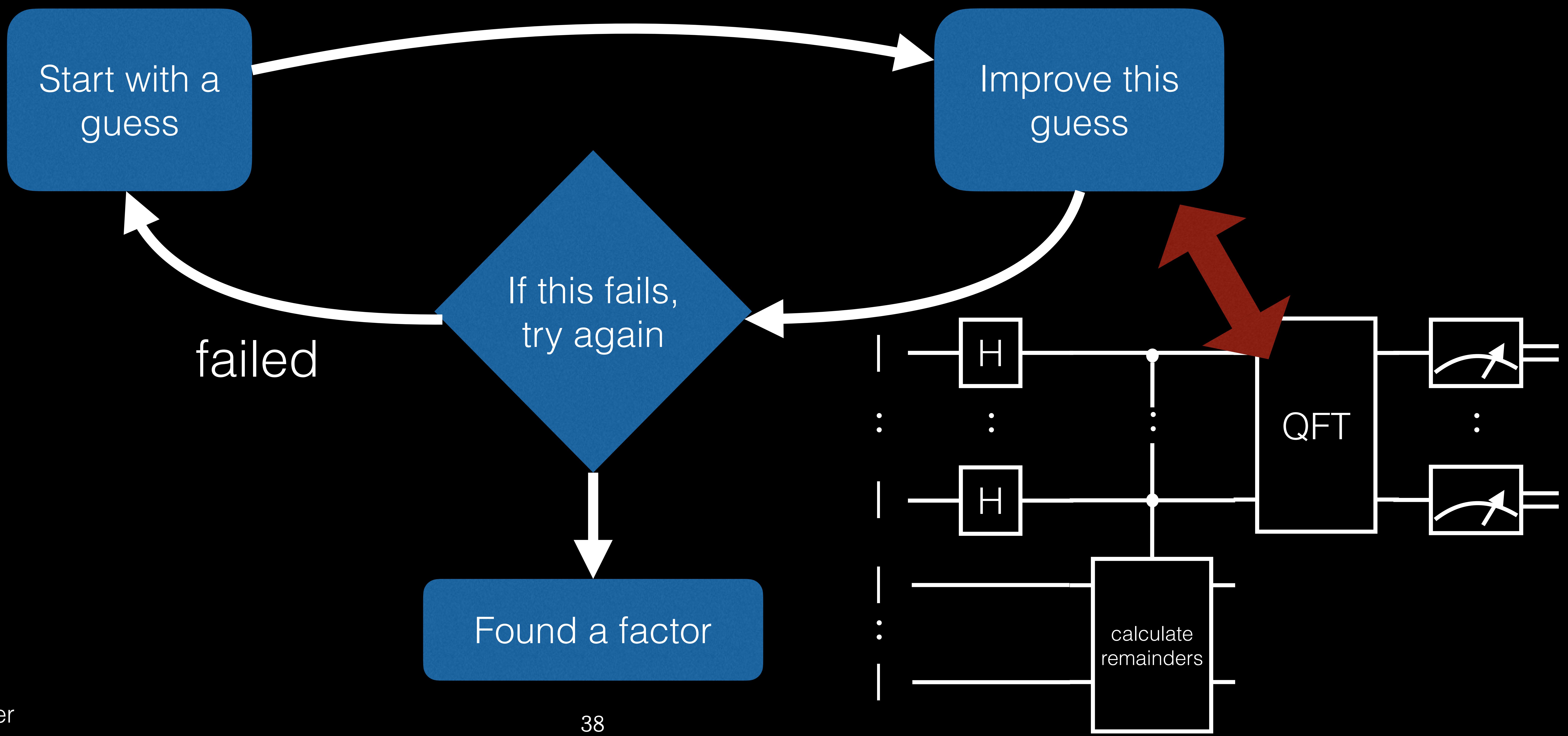


This requires 2050 completely noise-free qubits and $4.81 \cdot 10^{12}$ gates for RSA-1024

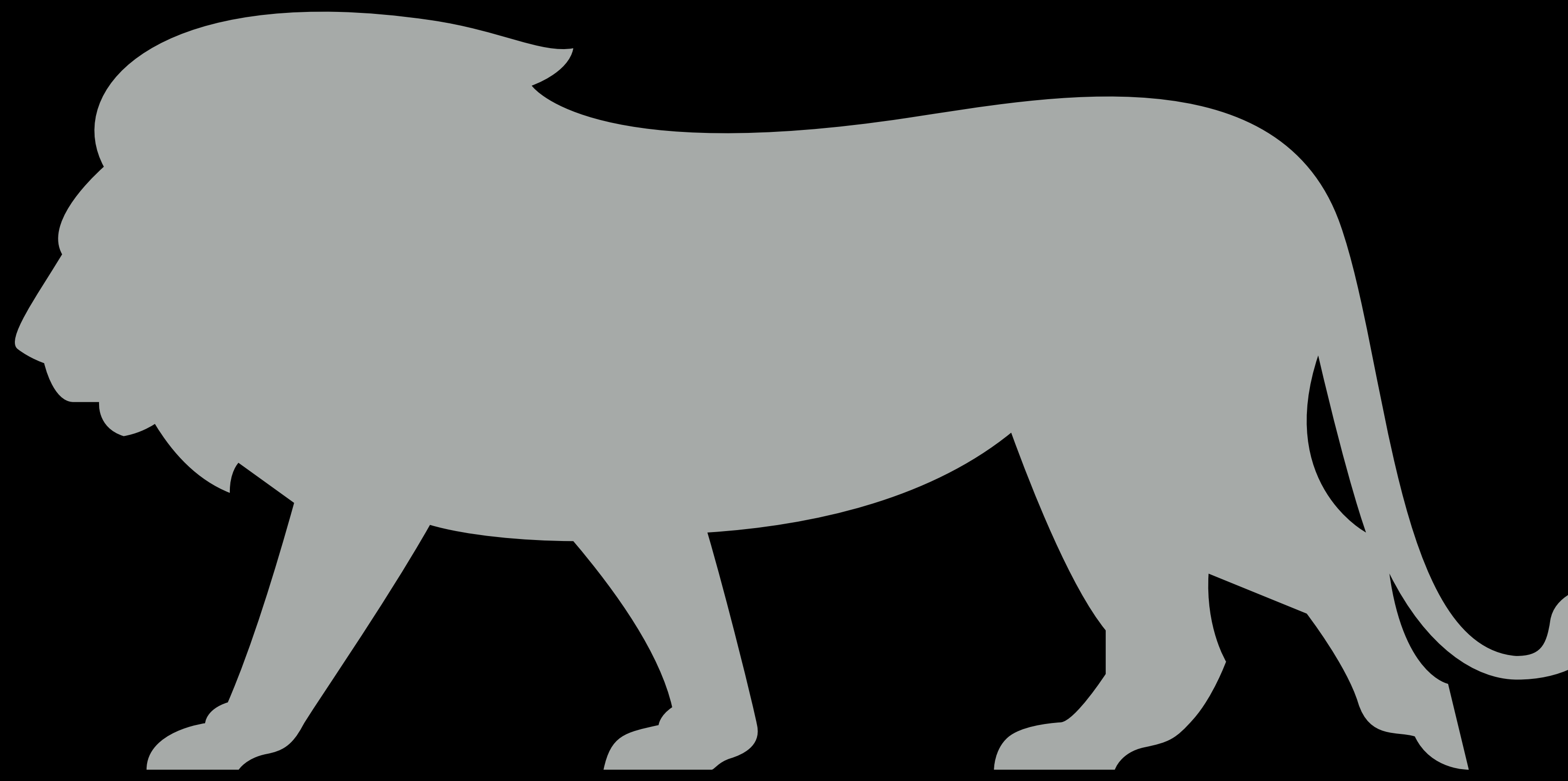
Guess and check with QFT

g

$$(g^{\frac{p}{2}} + 1) \times (g^{\frac{p}{2}} - 1) = m \times N$$



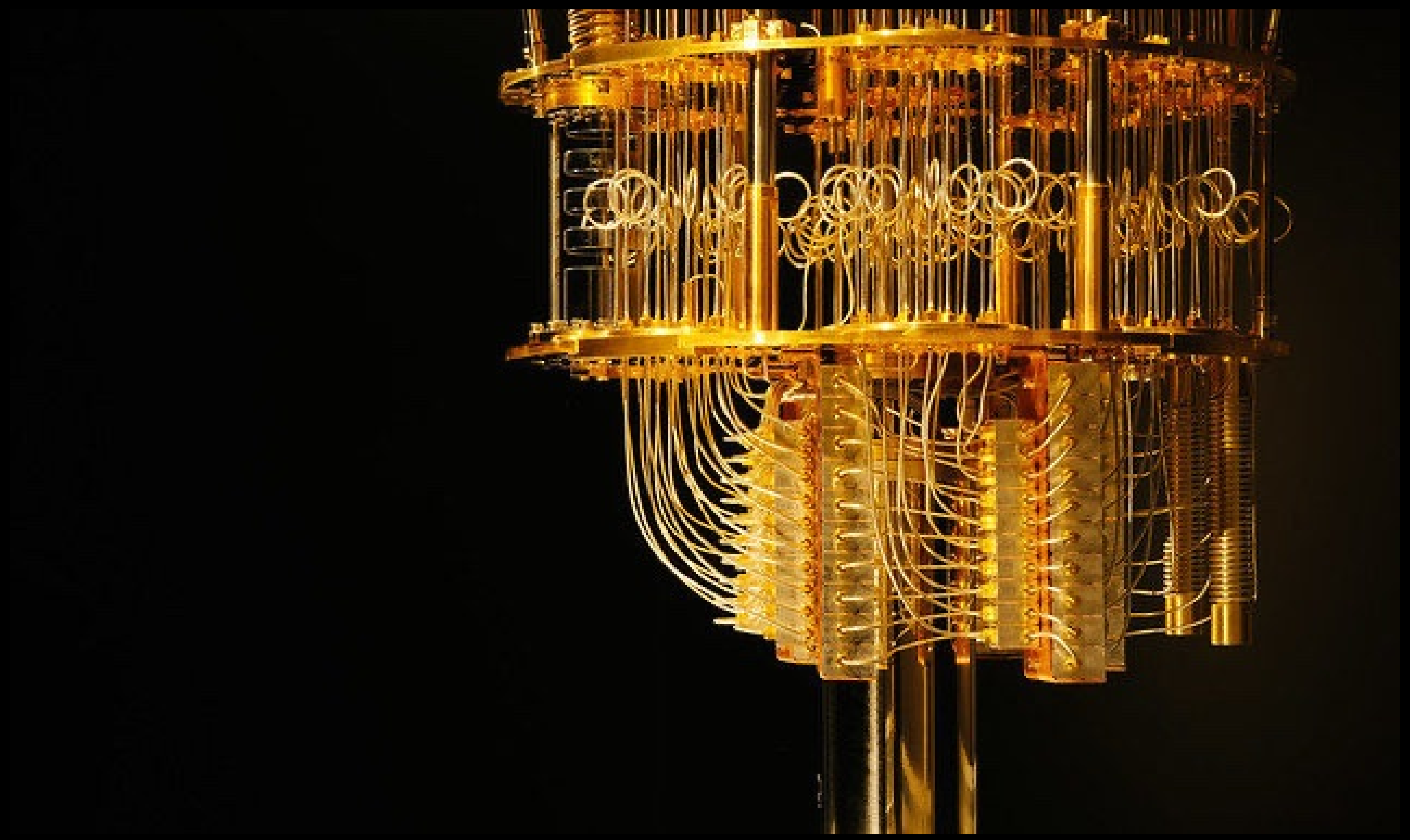
Conclusions



- We can break RSA
  - By reducing the problem to period finding
  - Which we can do quickly with a quantum computer
- This allows for the Harvesting Attack
- Discrete logarithmic problems 'reducible' to integer factorization
  - so, DHE and ECDHE are also be broken
- But it needs a sh*t-ton of qubits and gates

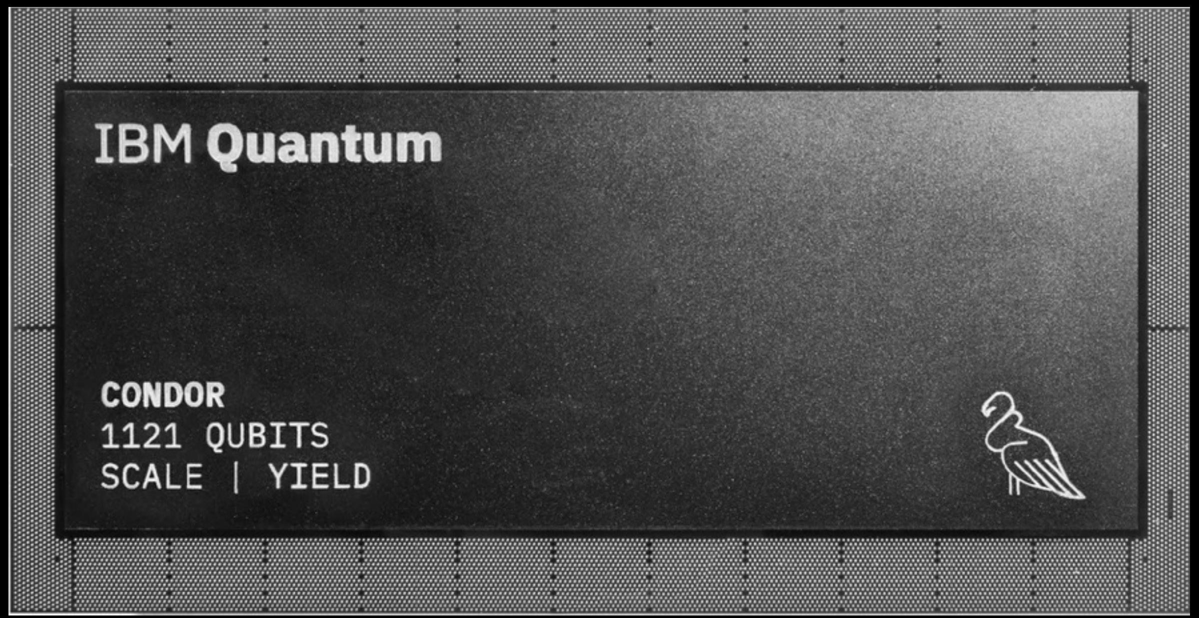
Interlude: Symmetric cryptography and hashing

- AES
  - Normally, search space of AES-128 is 2^{127}
  - Grover's algorithm speeds this up to 2^{64}
  - Therefore, why worry? Use AES-256 and be happy! For now
- Hashing
  - Also attackable by Grover's
  - But doubling the hash size will protect you for a generation

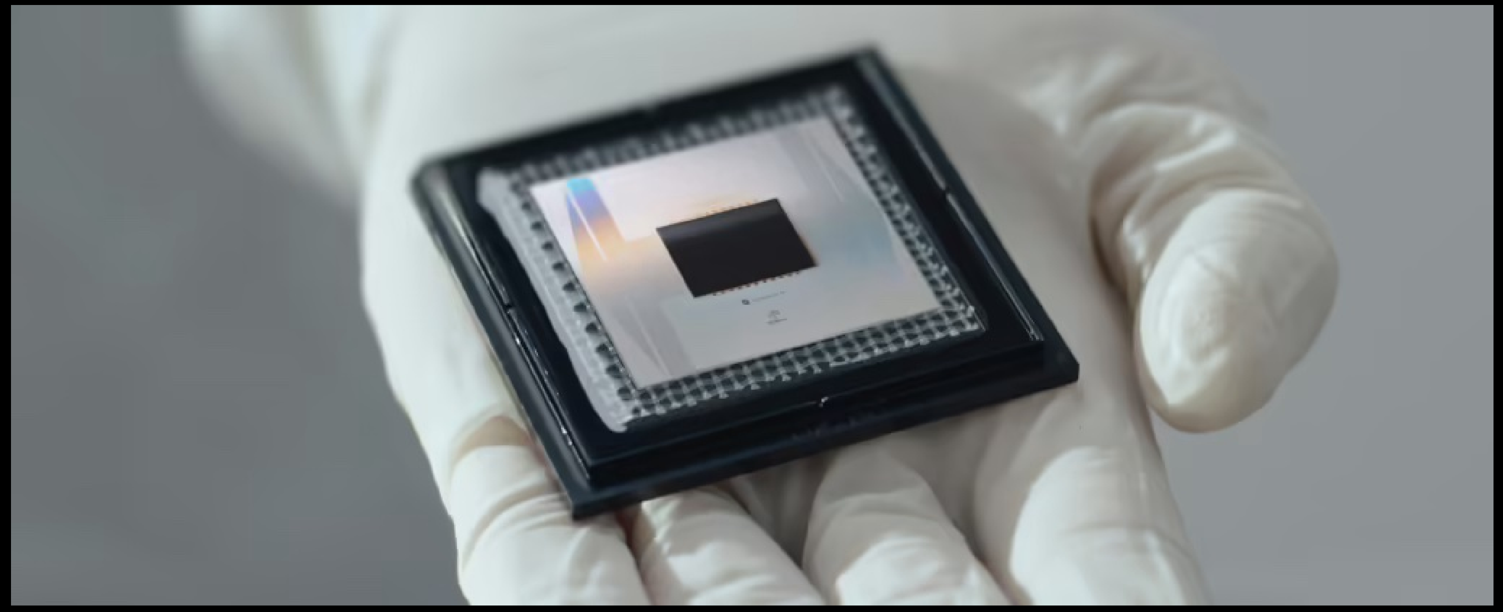


How real is the threat?

Quantum Computers are not there yet



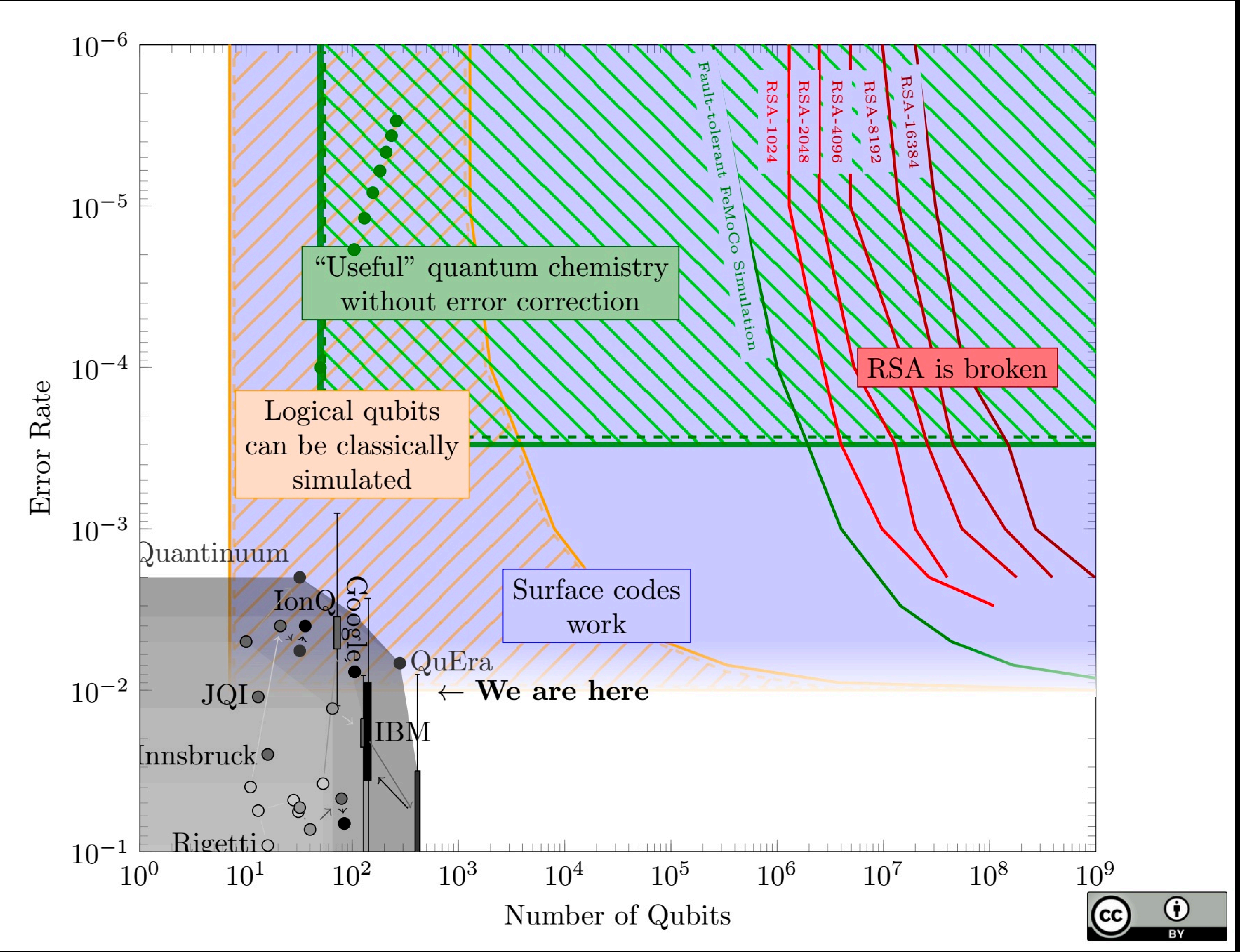
- Three criteria: Qubit count, gate count, gate performance
- IBM's Condor QPU is 1121 qubits with the maybe >1000 gates
  - IBM Heron has better gate performance but only 133 qubits



- These are noisy qubits
  - Noise mitigation requires 10-100x number of qubits!
  - Google's Willow showed that surface codes for error correction work
- Horizontal scaleout will need a rethink of algorithms

Remember what we said:
"This requires 2050 completely noise-free qubits and $4.81 \cdot 10^{12}$ gates for RSA-1024"

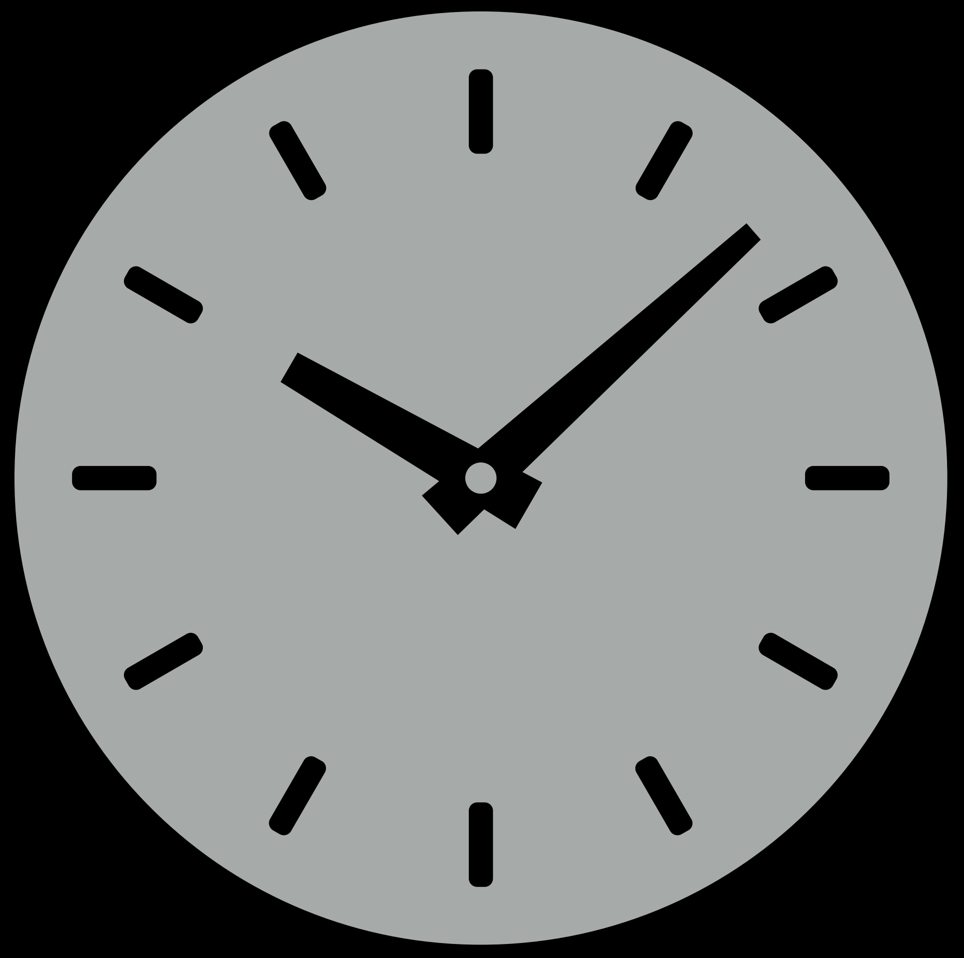
How close are we?



https://sam-jaques.appspot.com/quantum_landscape_2024

The 'if's

- 5 years from usable machines for special purposes
  - Specific algorithms on specific machines for specific problems
- 10-15 years away from breaking RSA with Shor's
- But there could be scientific and engineering breakthroughs



Death of Crypto?

Post-Quantum Cryptography

Meet the new crypto!

Algorithm	Standard	Former name	Intension	Approach
ML-KEM	FIPS 203	Crystals Kyber	KEM	Lattice, MLWE
ML-DSA	FIPS 204	Crystals Dilithium	DSA	Lattice, MLWE
SLH-DSA	FIPS 205	SPHINCS+	DSA	(Hash)
?	?	FALCON	DSA	FFT, NTRU Lattice
XMSS	RFC 8391		DSA	Hash
Leighton-Micali	RFC 8554		DSA	Hash

In the pipeline

Algorithm	Intension	Assumption	Status
Classic McEliece	KEM	Code	Round 4
BIKE	KEM	Code	Round 4
HQC	KEM	Code	Round 4
~~SIKE~~	~~KEM~~	~~Isogenies~~	Retracted

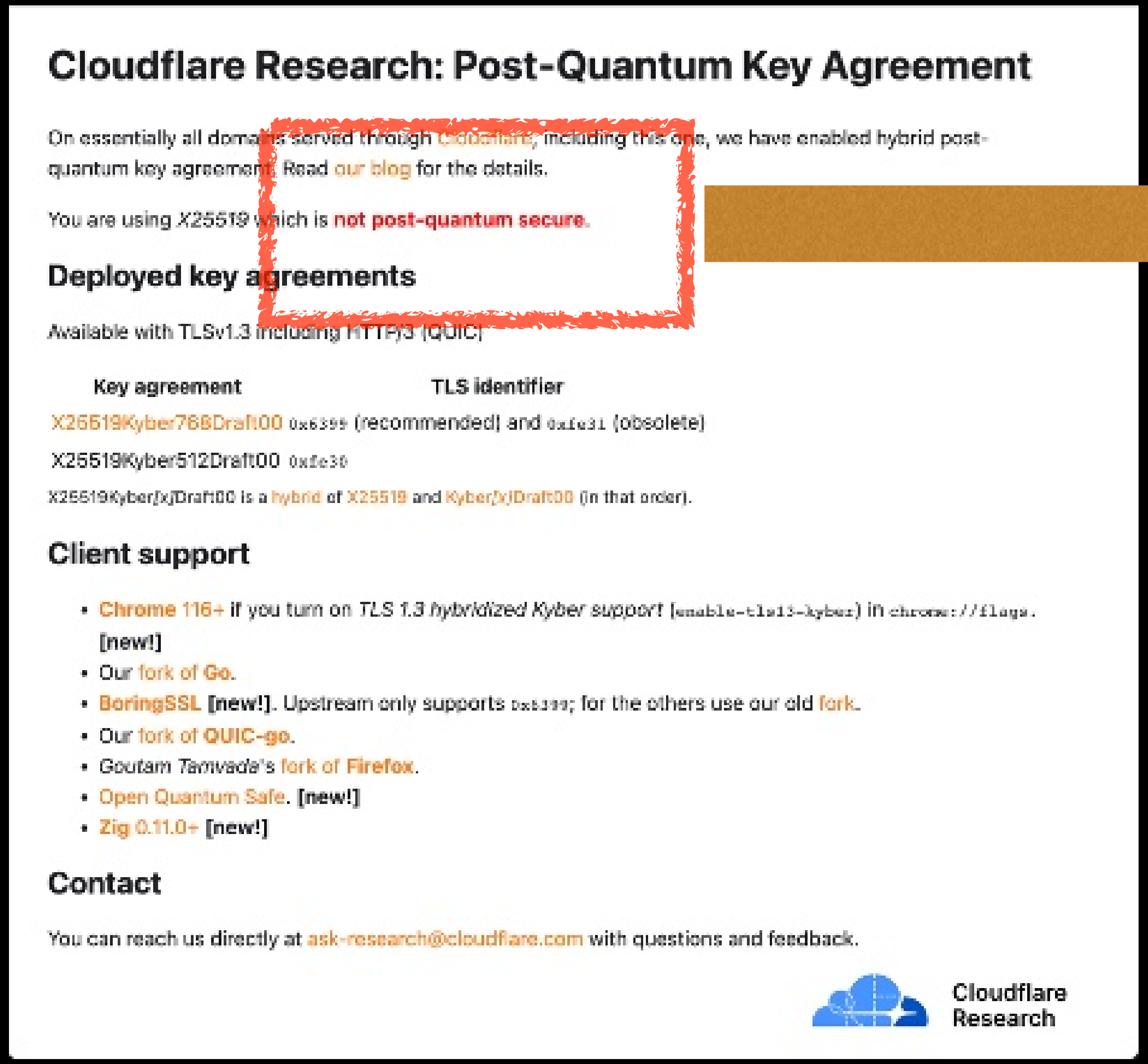
Others

- FALCON selected but not yet standardized
- SIKE vulnerability demonstrates risk
  - Follow German BSI advise: go hybrid
- What's up with FrodoKEM?
  - BSI and ANSSI recommend FrodoKEM-976 and FrodoKEM-1344
  - NIST probably objects to its high overhead

Support

- TLS 1.3 allows for PQC
  - Open Quantum Safe, BoringSSL, WolfSSL
  - But OpenSSL doesn't not implement any PQC
- OpenSSH from 9.9 onwards
  - uses the hybrid approach: ML-KEM and ECDH
- AWS, Cloudflare, Chrome, Signal, iMessage, …

Support


Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. Read our blog for the details.

You are using X25519 which is not post-quantum secure.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519Kyber768Draft00	0x6399 (recommended) and 0xfe31 (obsolete)
X25519Kyber512Draft00	0xfe30

X25519Kyber[x]Draft00 is a hybrid of X25519 and Kyber[x]Draft00 (in that order).

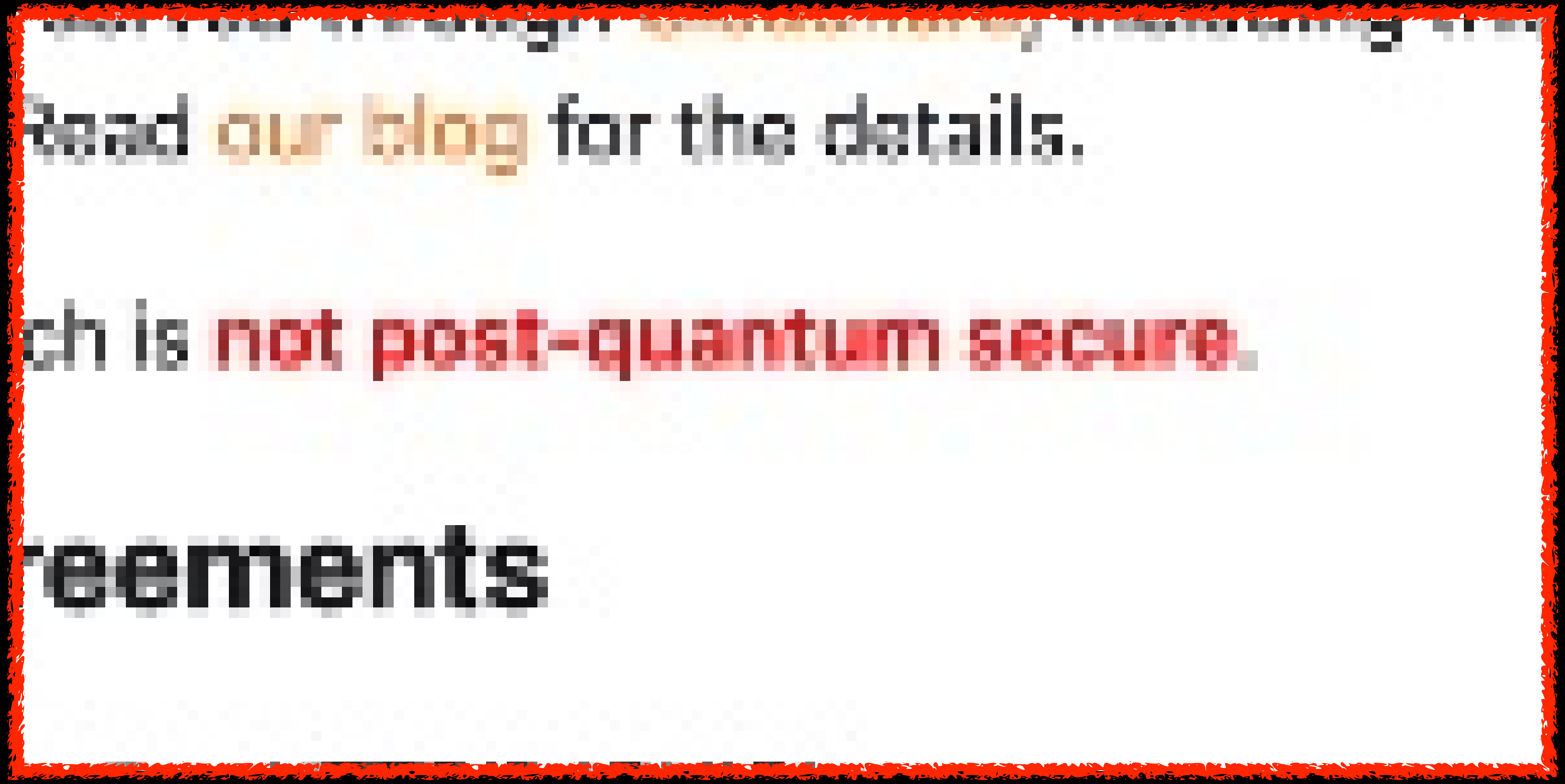
Client support

- Chrome 116+ if you turn on *TLS 1.3 hybridized Kyber support* (enable-tls13-kyber) in chrome://flags. [new!]
- Our fork of Go.
- BoringSSL [new!]. Upstream only supports 0x6399; for the others use our old fork.
- Our fork of QUIC-go.
- Goutam Tamvada's fork of Firefox.
- Open Quantum Safe. [new!]
- Zig 0.11.0+ [new!]

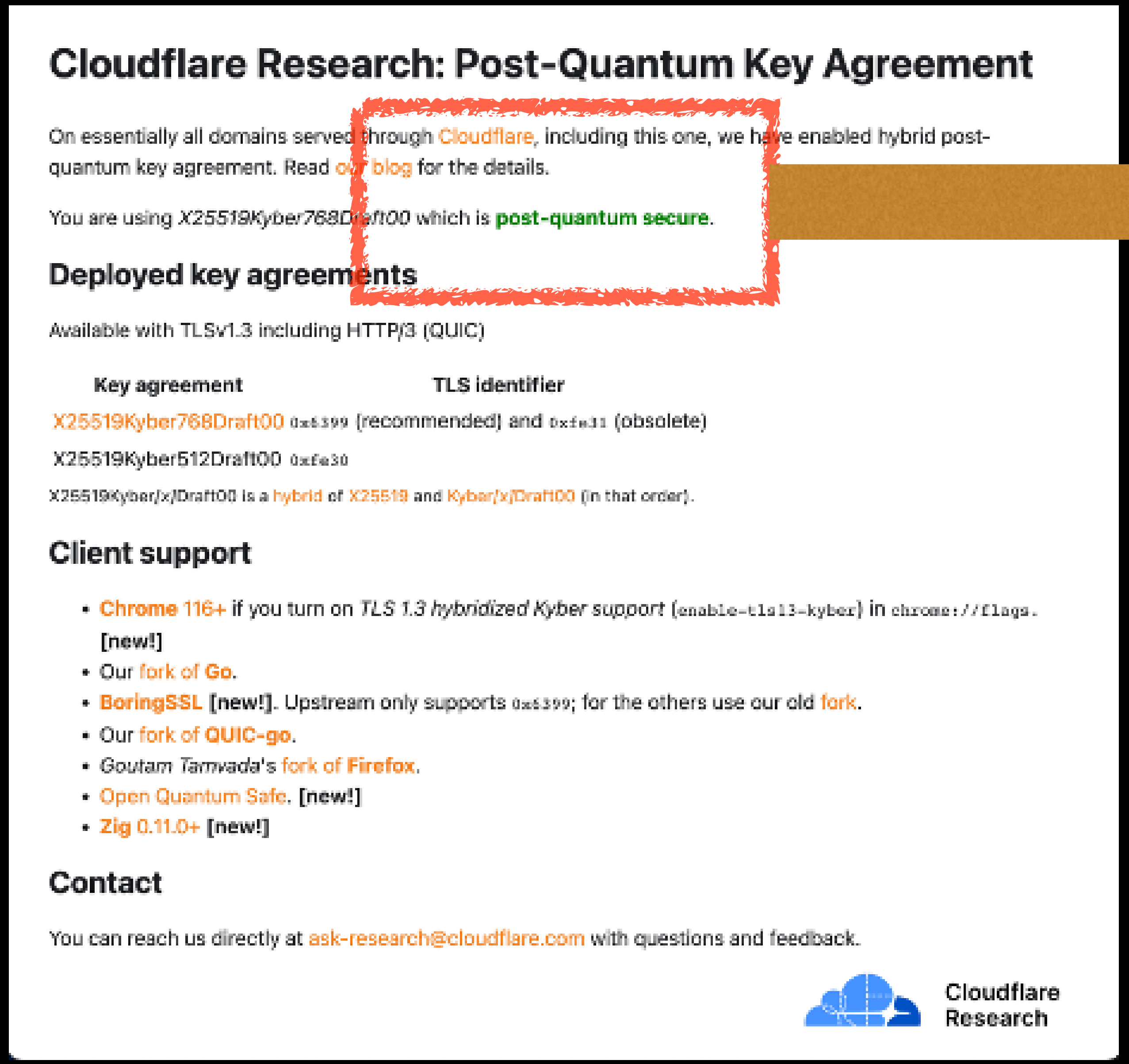
Contact

You can reach us directly at ask-research@cloudflare.com with questions and feedback.

Cloudflare Research



Chrome before enabling PQC


Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. Read our blog for the details.

You are using X25519Kyber768Draft00 which is post-quantum secure.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519Kyber768Draft00	0x6399 (recommended) and 0xfe31 (obsolete)
X25519Kyber512Draft00	0xfe30

X25519Kyber[x]Draft00 is a hybrid of X25519 and Kyber[x]Draft00 (in that order).

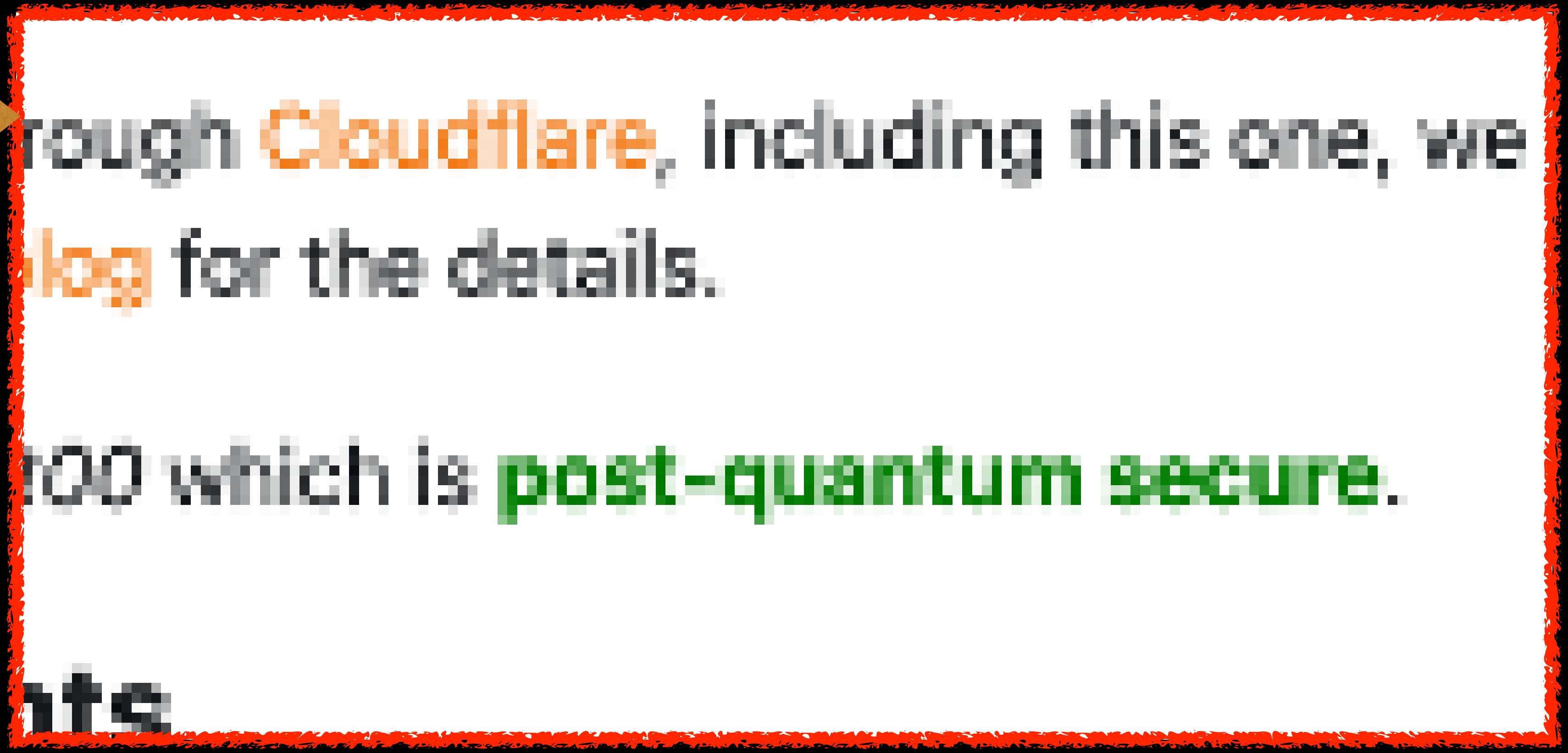
Client support

- Chrome 116+ if you turn on *TLS 1.3 hybridized Kyber support* (enable-tls13-kyber) in chrome://flags. [new!]
- Our fork of Go.
- BoringSSL [new!]. Upstream only supports 0x6399; for the others use our old fork.
- Our fork of QUIC-go.
- Goutam Tamvada's fork of Firefox.
- Open Quantum Safe. [new!]
- Zig 0.11.0+ [new!]

Contact

You can reach us directly at ask-research@cloudflare.com with questions and feedback.

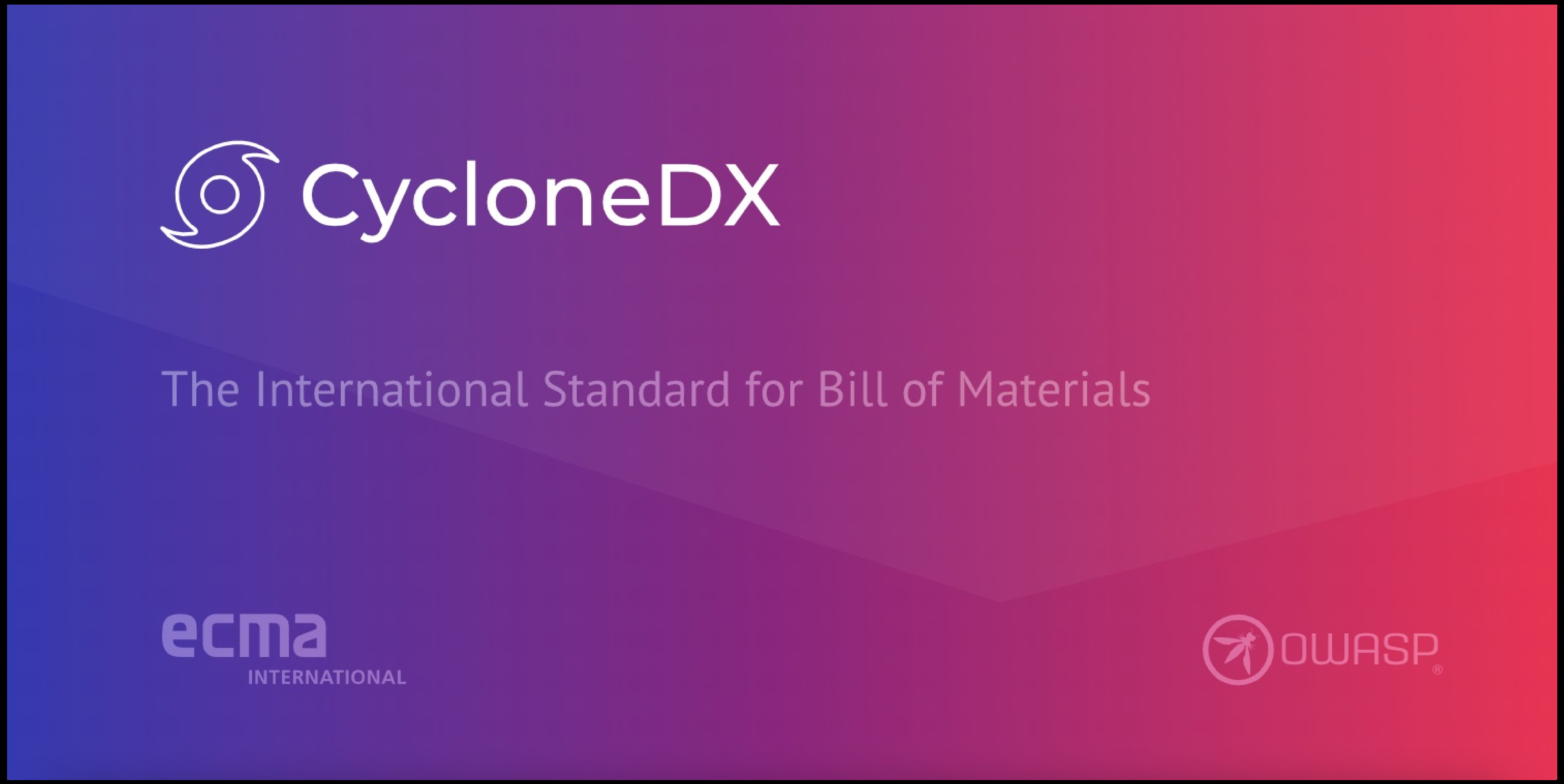
Cloudflare Research



Chrome after enabling PQC

Considerations

- PQC key sizes are may times larger
- Performance profiles are different
  - not always worse though
- Some algorithms still young
- CycloneDX now support a CBOM

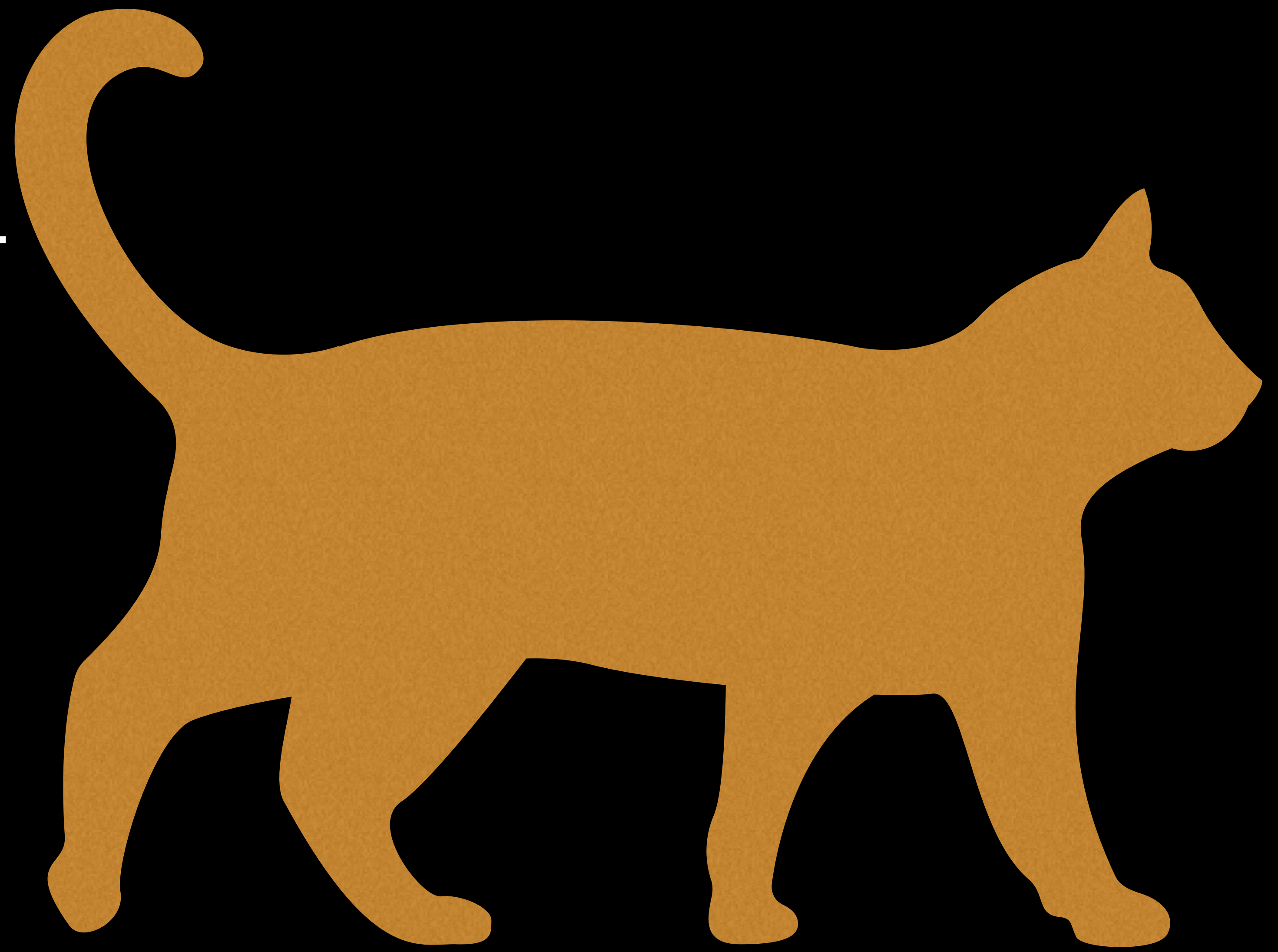


But should you care?

- Yes if,
  - you need your network traffic to stay secret > 10 years
  - Have very bandwidth, memory or CPU constrained devices
- If not then sit back and relax :-)

Main takeaway IMHO

- Threat to asymmetric cryptography is still theoretical
- We have 10 years, (error: +never, -5 years)
- If you have strict requirements start planning now
- Otherwise, wait until vendors do the work for you



https://www.trendmicro.com/vinfo/us/security/news/security-technology/...
... diving-deep-into-quantum-computing-modern-cryptography
... diving-deep-into-quantum-computing-computing-with-quantum-mechanics
... post-quantum-cryptography-quantum-computing-attacks-on-classical-cryptography
... post-quantum-cryptography-migrating-to-quantum-resistant-cryptography
... the-realities-of-quantum-machine-learning

Thanks to my colleagues
Mark Chimley and
Adam Tuaima

linkedin.com/in/mswimmer