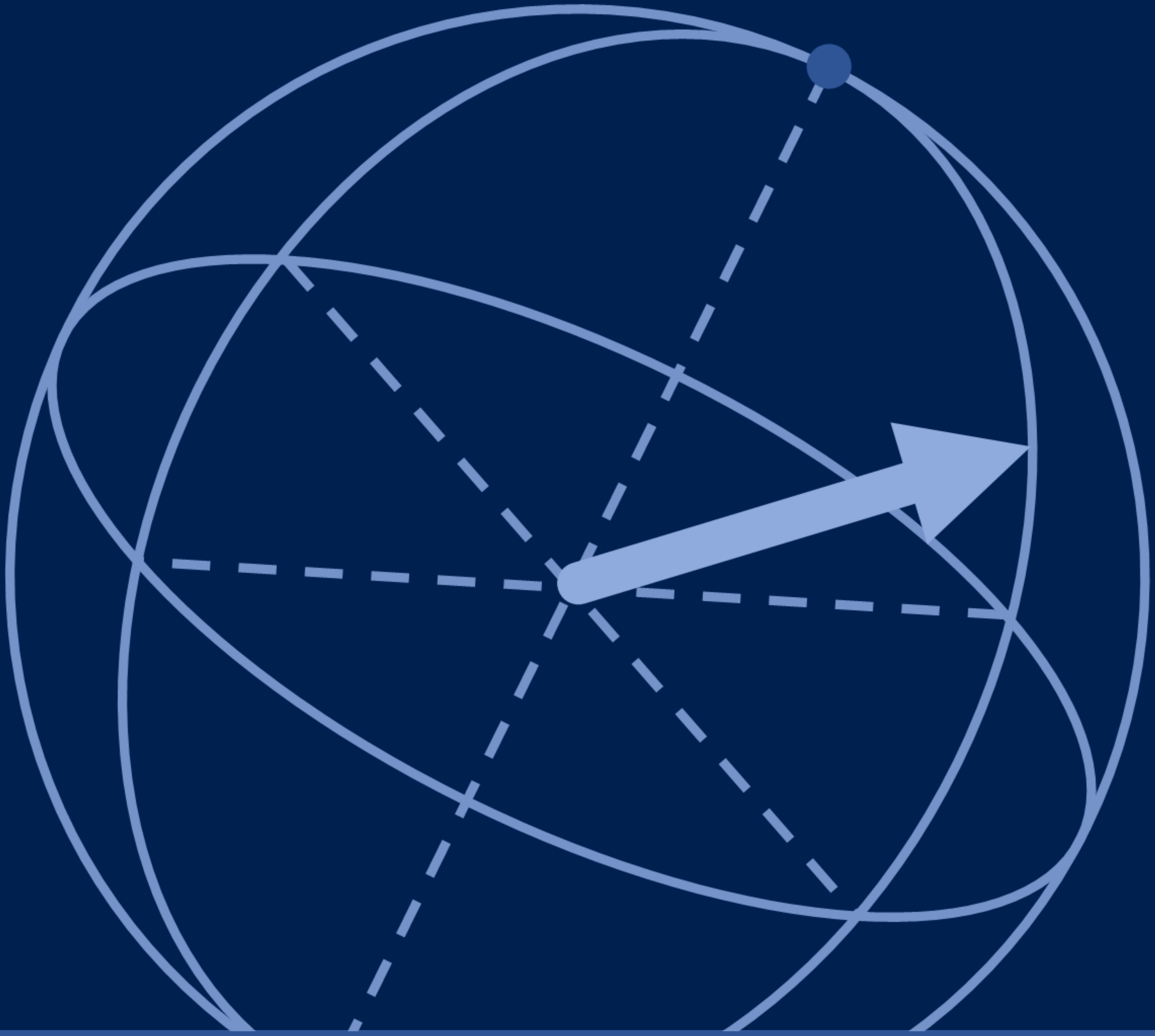
Preparing for

Post-Quantum Cryptography

in 2025



Andy Smith

@rot169

Who am I?

- 17+ years in infosec: currently a Principal Security Architect
- SANS Instructor: Defensible Security Architecture & Engineering (SEC530)
- Founding Core member of OWASP Top-10 for LLMs
- YouTube: Attack Detect Defend

I am not…

- a Quantum Physicist
- a Quantum Programmer
- a Mathematician

@rot169

@rot169@infosec.exchange

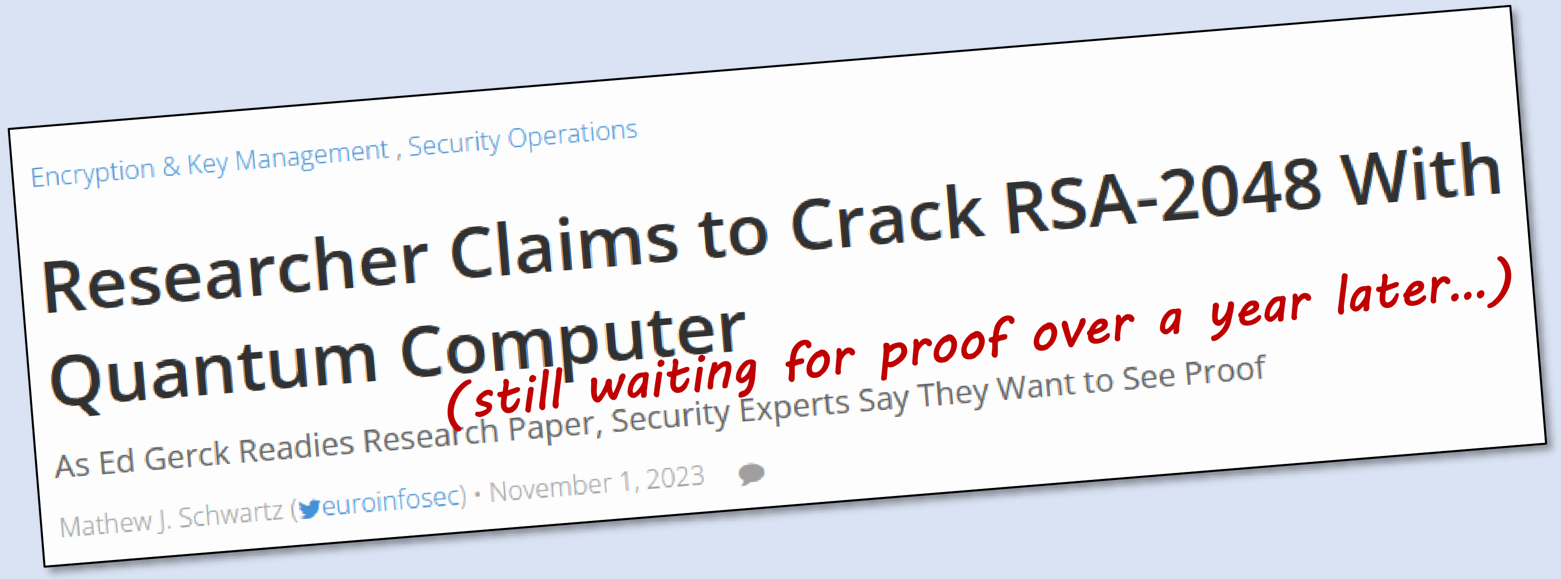
youtube.com/rot169

github.com/rot169

Objectives

1. Understand the **real threat** that quantum computing poses to security
2. Understand the **options** for dealing with the quantum threat
3. Understand the **timeline** for taking action

Cracking crypto in the news



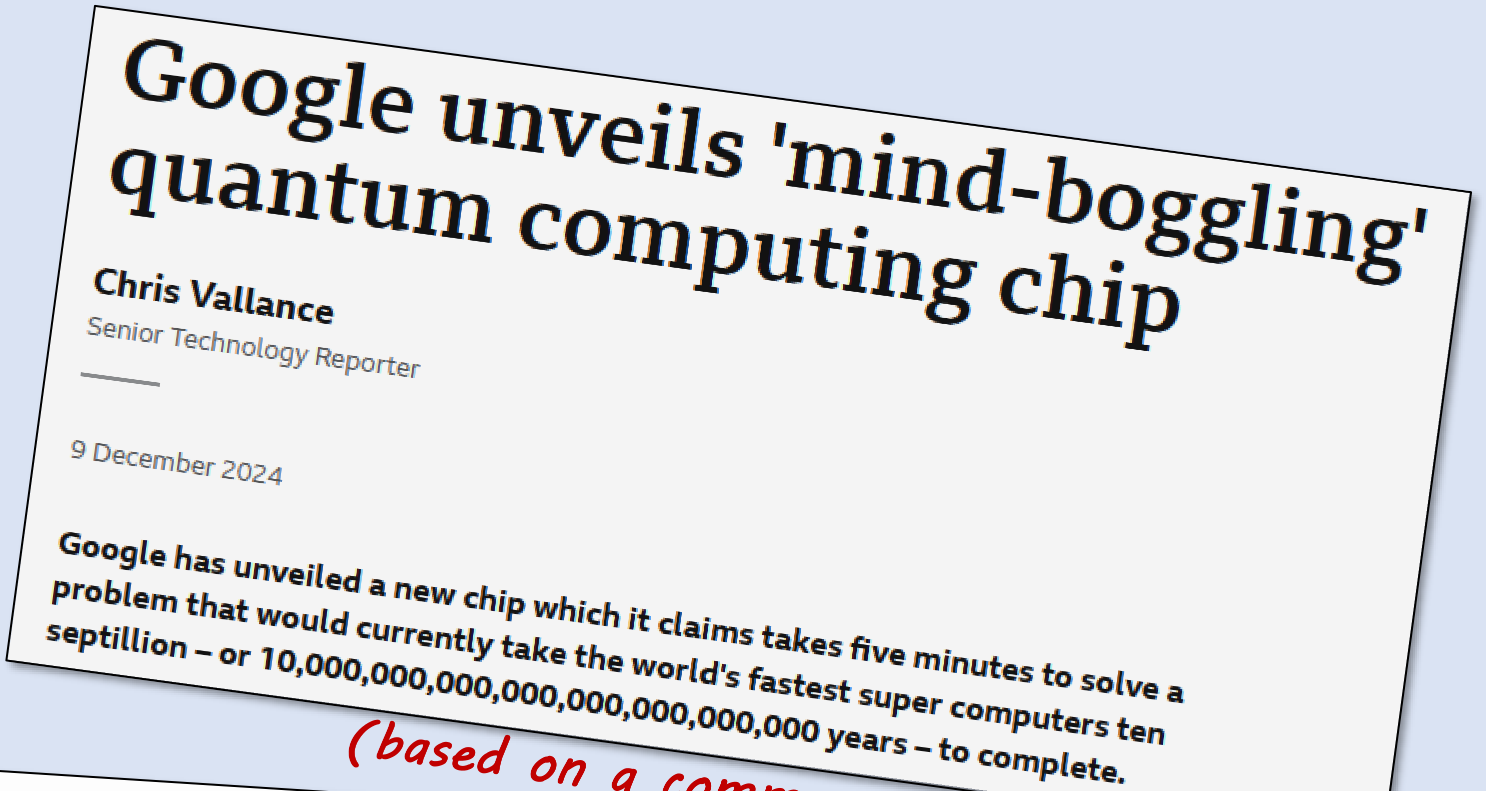
Encryption & Key Management , Security Operations

Researcher Claims to Crack RSA-2048 With Quantum Computer

As Ed Gerck Readies Research Paper, Security Experts Say They Want to See Proof

Mathew J. Schwartz (euroinfosec) • November 1, 2023

(still waiting for proof over a year later...)



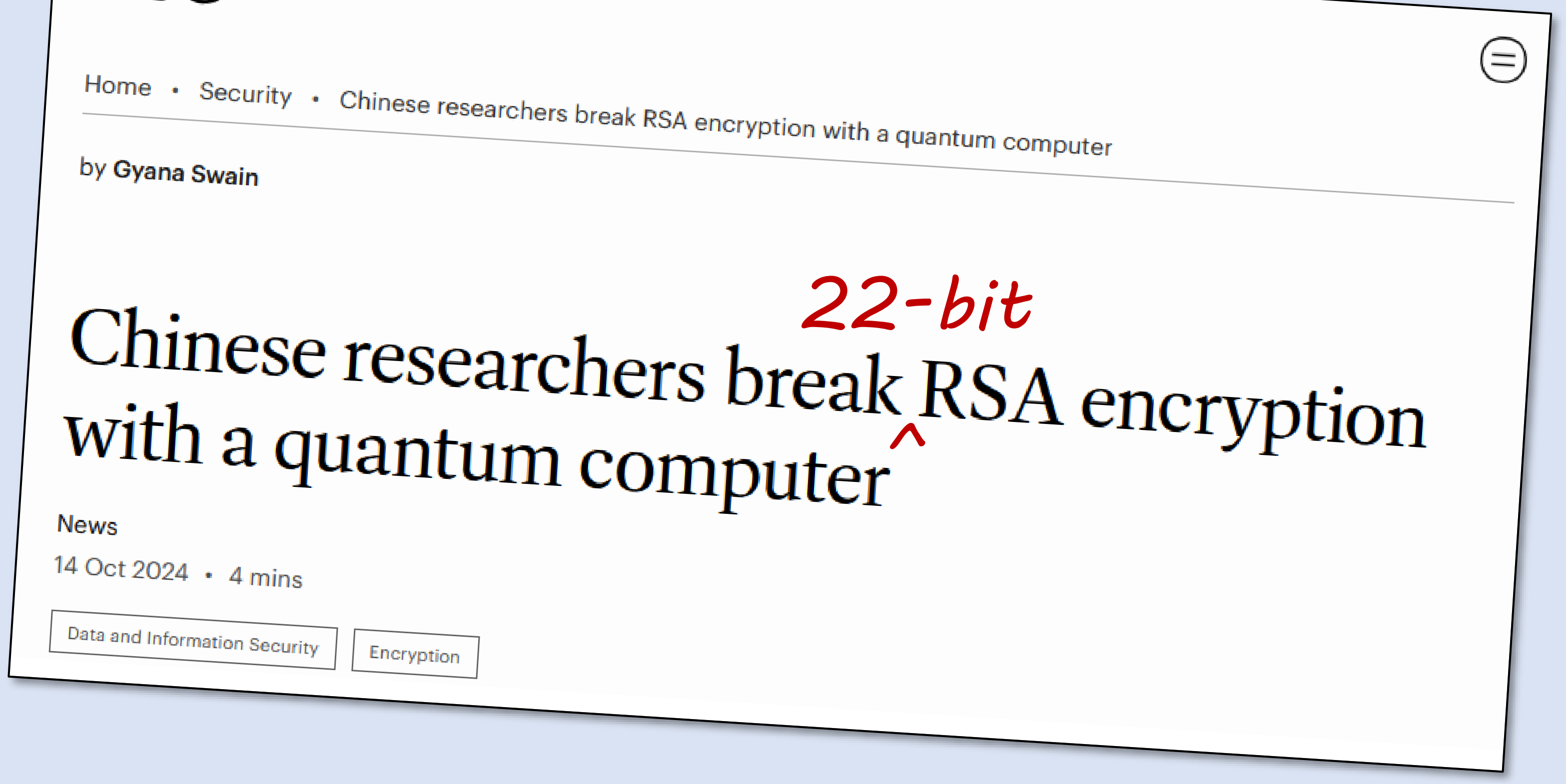
Google unveils 'mind-boggling' quantum computing chip

Chris Vallance
Senior Technology Reporter

9 December 2024

Google has unveiled a new chip which it claims takes five minutes to solve a problem that would currently take the world's fastest super computers ten septillion – or 10,000,000,000,000,000,000,000,000 years – to complete.

(based on a commercially-useless metric)



CSO

Home • Security • Chinese researchers break RSA encryption with a quantum computer

by Gyana Swain

Chinese researchers break RSA encryption with a quantum computer

22-bit ^

News

14 Oct 2024 • 4 mins

Data and Information Security | Encryption

https://www.bbc.co.uk/news/articles/c791ng0zvl3o
https://www.bankinfosecurity.com/blogs/researcher-claims-to-crack-rsa-2048-quantum-computer-p-3536
https://www.csoonline.com/article/3562701/chinese-researchers-break-rsa-encryption-with-a-quantum-computer.html

Demystifying Quantum

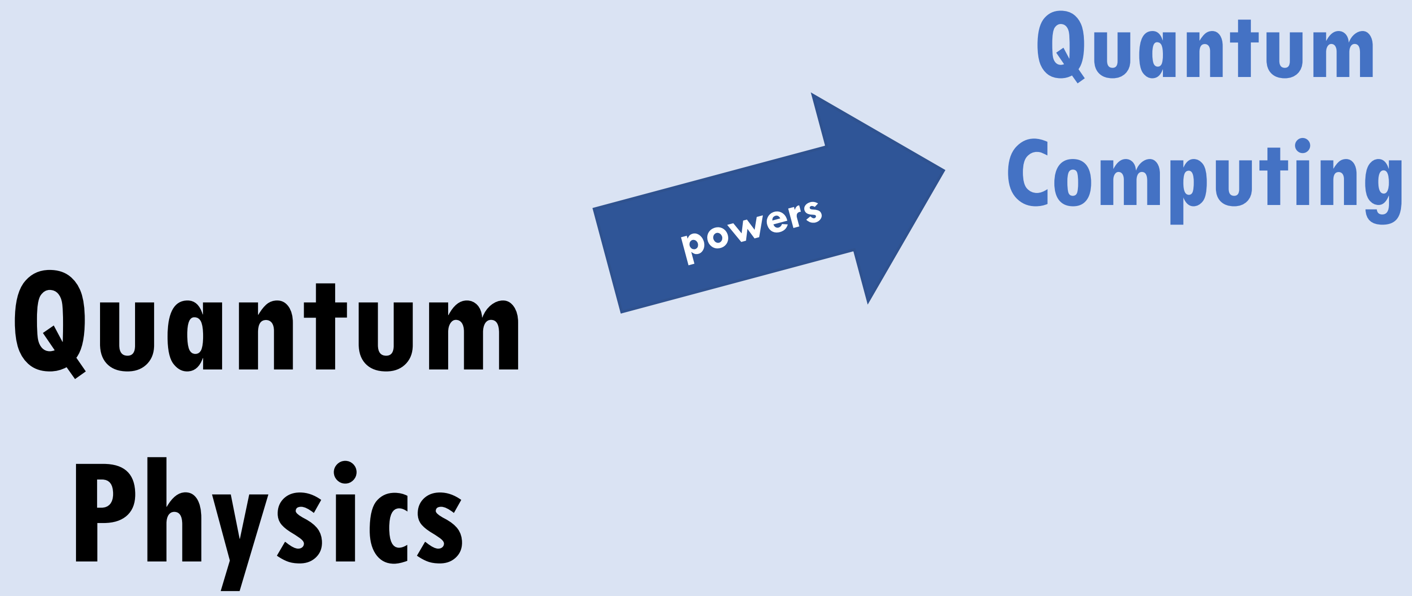
Quantum

Physics

Quantum Physics

- Things get weird at sub-atomic scales!
  - Wave-particle duality (e.g., double-slit experiment)
  - Superpositions (e.g., Schrodinger's cat)
  - Entanglement (e.g., spooky action at a distance)

Demystifying Quantum



Quantum Physics

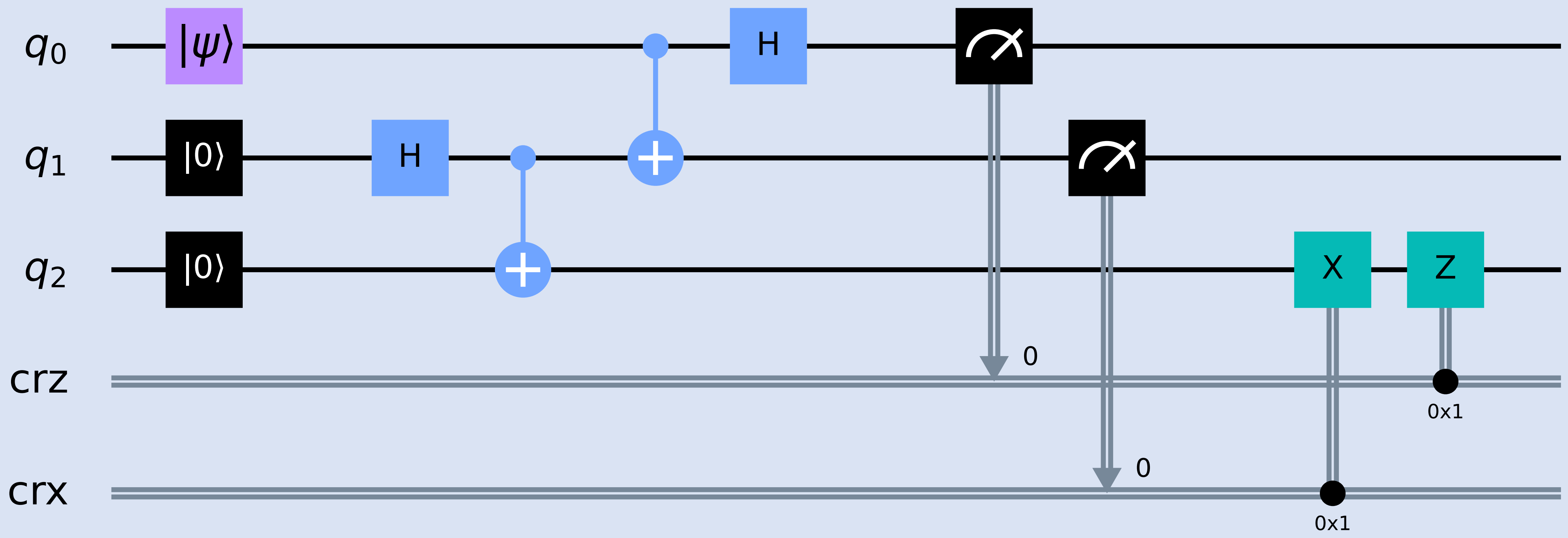
powers

Quantum Computing

Quantum Computing

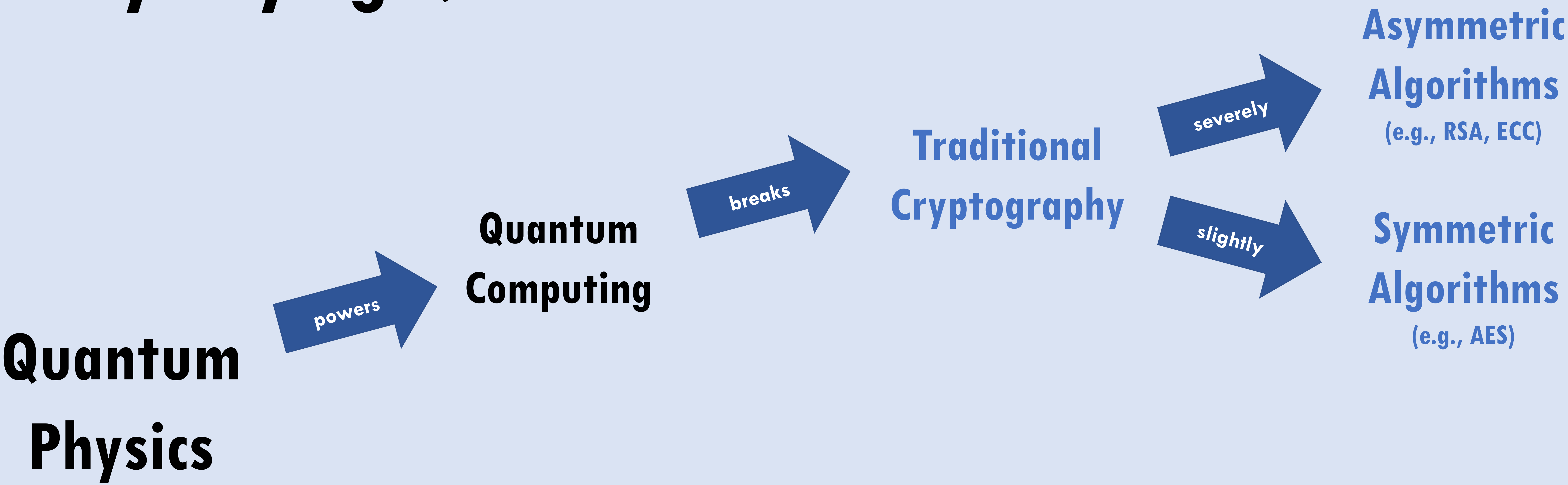
- Using quantum weirdness to perform calculations that classical computers cannot.
- Different quantum computers use different physics (e.g., electron spin, polarisation of photons, etc).
- Processing is undertaken on q-bits (quantum bits) which are in a superposition until measured.
- Operations include X, Y, Z, H, S, T, CX, CZ, CCX – fundamentally different to classical AND, NOT, OR, etc.
- Successful computation relies on not just number of q-bits! Also:
  - Physical vs. logical qbits
  - Qbit coherence vs. gate speed
  - Gate fidelity
  - Connectivity between gates

Quantum volume = # of qubits × Circuit depth



https://qiskit.org/textbook/ch-algorithms/defining-quantum-circuits.html

Demystifying Quantum



Quantum Physics

powers

Quantum Computing

breaks

Traditional Cryptography

severely

Asymmetric Algorithms

(e.g., RSA, ECC)

slightly

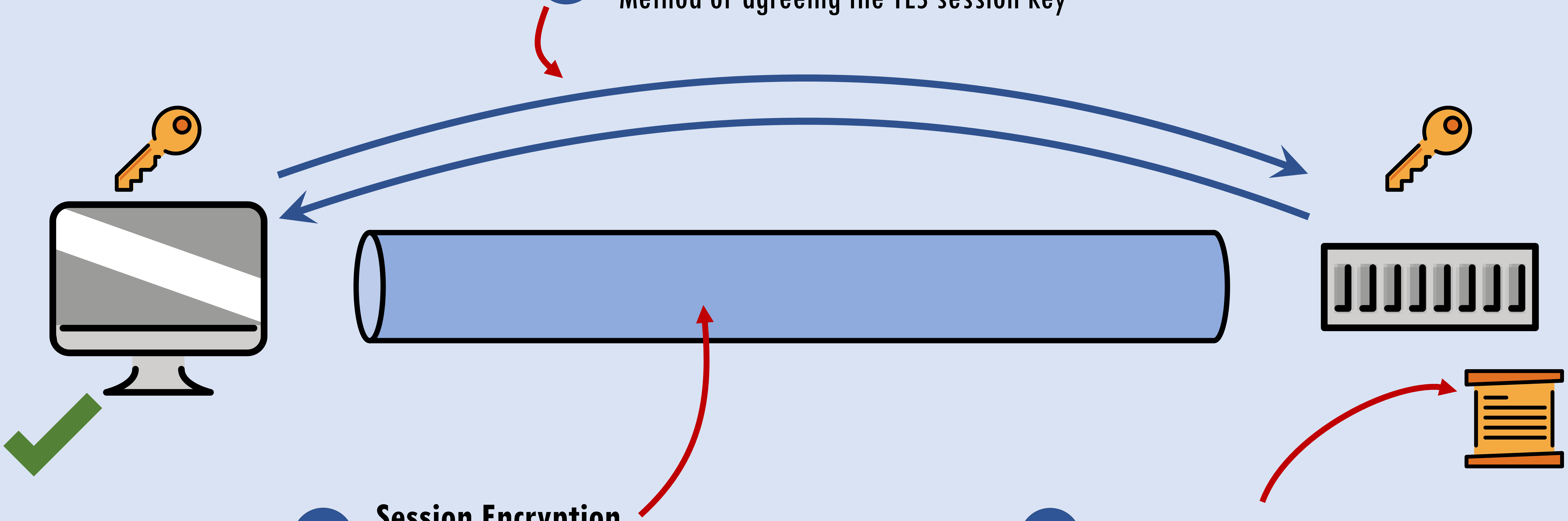
Symmetric Algorithms

(e.g., AES)

Traditional Cryptography

- Grover’s Algorithm:
  - Solves opaque-box functions quadratically faster.
  - Reduces time to brute force symmetric ciphers (e.g., AES).
  - AES-128 requires 2^{128} iterations to brute-force using traditional computing vs 2^{64} using Grover’s algorithm.

- Shor’s Algorithm:
  - Factoring primes exponentially faster (breaks RSA).
  - Calculates discrete logarithms too (breaks ECC).
  - Also breaks Diffie-Hellman (based on RSA / ECC).



1 **Key Exchange Mechanism**

Method of agreeing the TLS session key

2 **Session Encryption**

A unique symmetric key
for this TLS session

3 **Digital Signature**

Used to sign the certificate
which authenticates the
server to the client

What can we do?

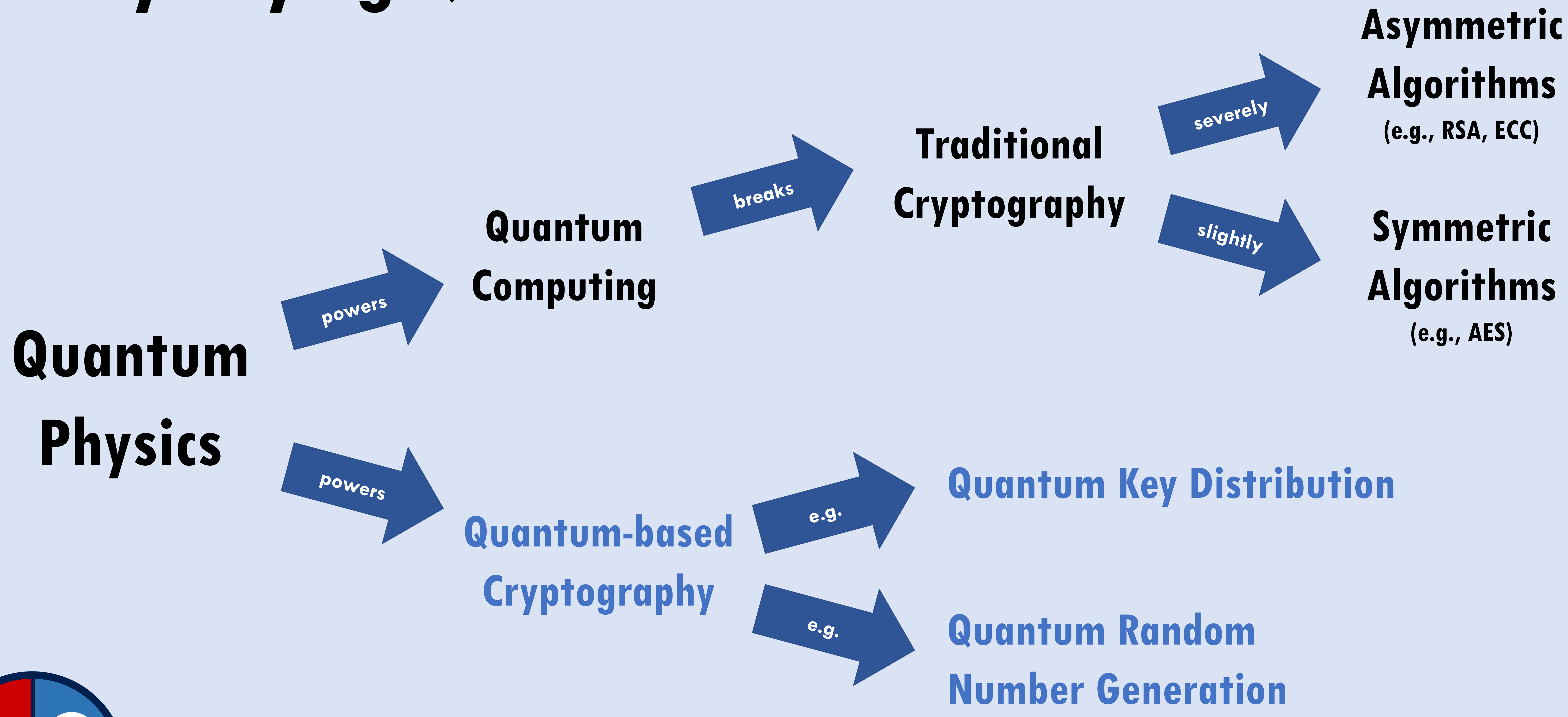
- For symmetric ciphers: just double the key length!
  - E.g., use AES-256 to regain 128-bits of security.

- For asymmetric ciphers:
  a) Create new cryptosystems based on the weirdness of quantum physics.
  b) Create new cryptosystems using a mathematical problem that can’t be accelerated using quantum computing.
  c) Avoid asymmetric ciphers altogether!

Recap on Objectives

1. Understand the **real threat** that quantum computing poses to security ✓
2. Understand the **options** for dealing with the quantum threat ←
3. Understand the **timeline** for taking action

Demystifying Quantum



Quantum Physics

Quantum Computing

Traditional Cryptography

Asymmetric Algorithms (e.g., RSA, ECC)

Symmetric Algorithms (e.g., AES)

Quantum-based Cryptography

Quantum Key Distribution

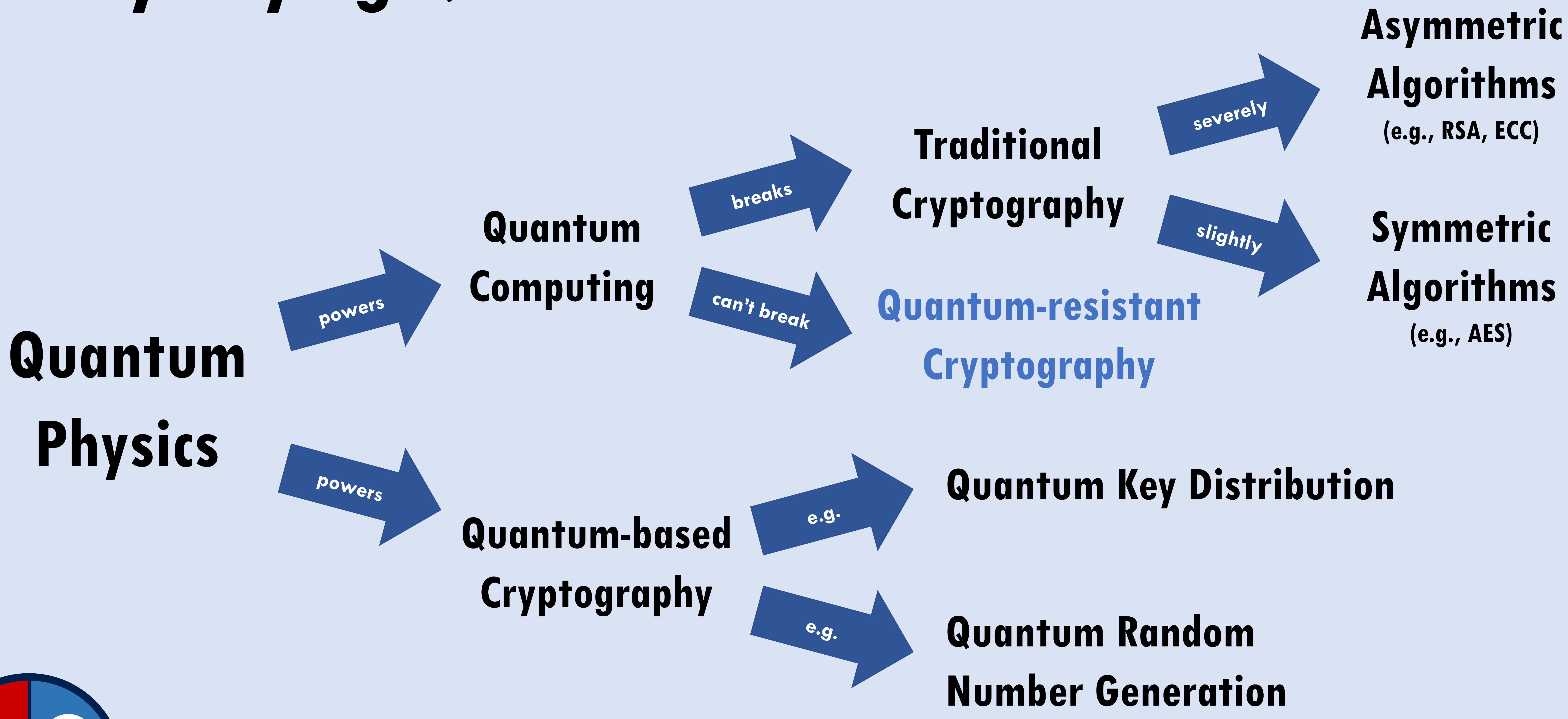
Quantum Random Number Generation

Quantum-based Crypto

- Quantum Key Distribution (QKD):
  - Use quantum properties (e.g., the polarisation of photons, entanglement, etc) to agree a symmetric key.
  - Requires specialist hardware for endpoints.
  - Impractical for end-to-end encryption.
- Quantum Random Number Generation (QRNG):
  - Use quantum properties to create numbers which are more random.
  - Random numbers are important to crypto; we've seen attacks based on poor randomness.
  - Current (non-quantum) cryptographically-secure RND seems good enough?
  - Oh, and QRND doesn't solve the quantum threat.

…but what about digital signatures… and public-key encryption?

Demystifying Quantum



Quantum Physics

Quantum Computing

Quantum-based Cryptography

Traditional Cryptography

Quantum-resistant Cryptography

Asymmetric Algorithms (e.g., RSA, ECC)

Symmetric Algorithms (e.g., AES)

Quantum Key Distribution

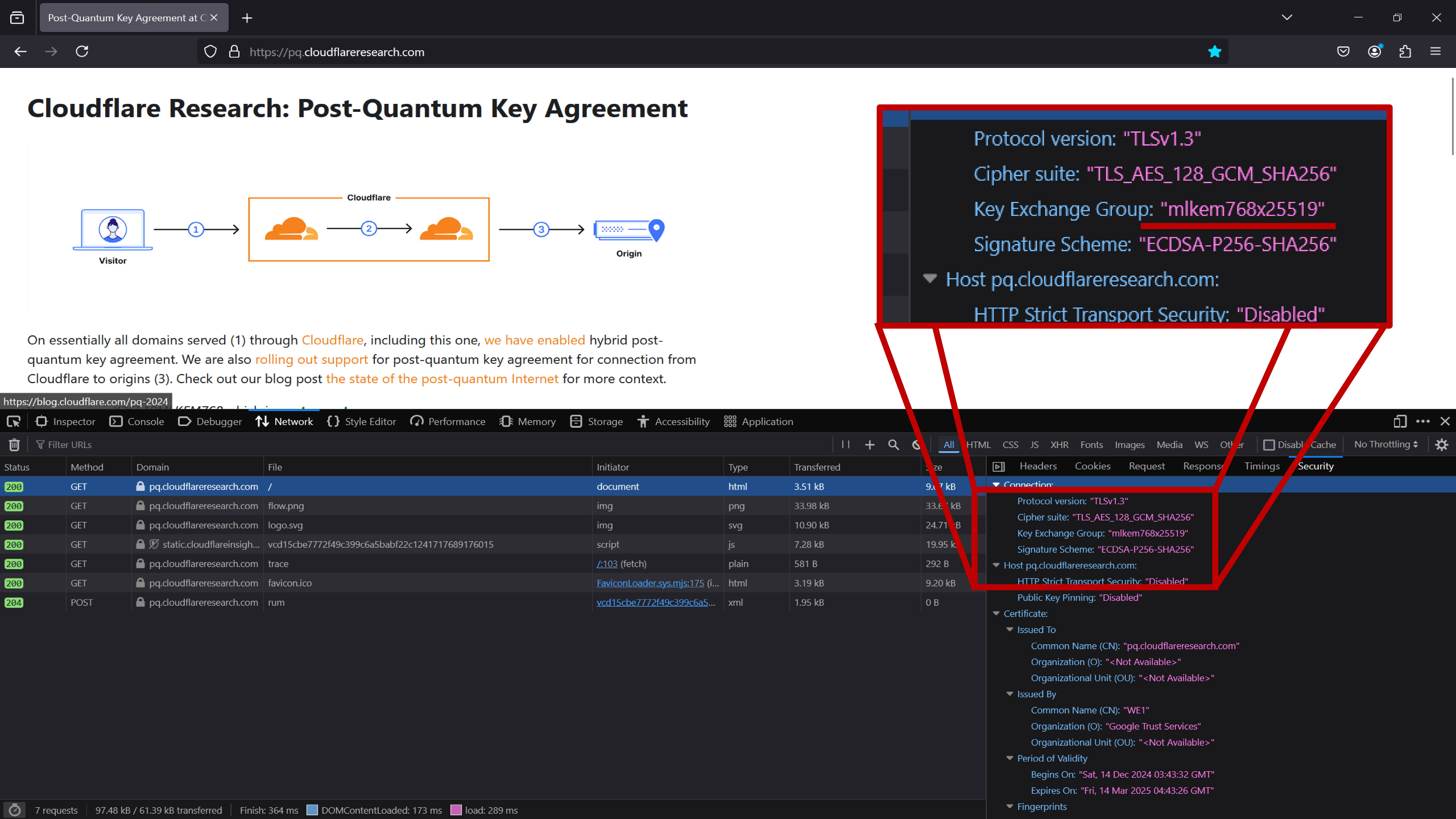
Quantum Random Number Generation

Quantum-resistant Crypto

- Runs on a classical computer.
- Based on mathematical problems that quantum computing cannot meaningfully accelerate.*
- NIST have been running a selection programme; first three algorithms standardised Aug 2024:
  - ML-KEM: Module-Lattice-Based Key-Encapsulation Algorithm (FIPS 203) – formerly CRYSTALS-Kyber
  - ML-DSA: Module-Lattice-Based Digital Signature Algorithm (FIPS 204) – formerly CRYSTALS-Dilithium
  - SLH-DSA: Stateless Hash-Based Digital Signature Algorithm (FIPS 205) – formerly SPHINCS+
- Standards available at: https://www.nist.gov/pqcrypto
- Experimental implementations available (www.openquantumsafe.org); production libraries in-flight.
- X25519+MLKEM768 built into Firefox, Chrome and Cloudflare.

Hybrid crypto!

* that we know of today



Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served (1) through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. We are also rolling out support for post-quantum key agreement for connection from Cloudflare to origins (3). Check out our blog post the state of the post-quantum Internet for more context.

Protocol version: "TLSv1.3"
Cipher suite: "TLS_AES_128_GCM_SHA256"
Key Exchange Group: "mlkem768x25519"
Signature Scheme: "ECDSA-P256-SHA256"
Host pq.cloudflareresearch.com:
HTTP Strict Transport Security: "Disabled"

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	pq.cloudflareresearch.com	/	document	html	3.51 kB	9.67 kB
200	GET	pq.cloudflareresearch.com	flow.png	img	png	33.98 kB	33.65 kB
200	GET	pq.cloudflareresearch.com	logo.svg	img	svg	10.90 kB	24.71 kB
200	GET	static.cloudflareinsigh...	vcd15cbe7772f49c399c6a5babf22c1241717689176015	script	js	7.28 kB	19.95 kB
200	GET	pq.cloudflareresearch.com	trace	/:103 (fetch)	plain	581 B	292 B
200	GET	pq.cloudflareresearch.com	favicon.ico	FaviconLoader.sys.mjs:175 (i...	html	3.19 kB	9.20 kB
204	POST	pq.cloudflareresearch.com	rum	vcd15cbe7772f49c399c6a5...	xml	1.95 kB	0 B

```
▼ Connection:
    Protocol version: "TLSv1.3"
    Cipher suite: "TLS_AES_128_GCM_SHA256"
    Key Exchange Group: "mlkem768x25519"
    Signature Scheme: "ECDSA-P256-SHA256"
▼ Host pq.cloudflareresearch.com:
    HTTP Strict Transport Security: "Disabled"
    Public Key Pinning: "Disabled"
▼ Certificate:
  ▼ Issued To
      Common Name (CN): "pq.cloudflareresearch.com"
      Organization (O): "<Not Available>"
      Organizational Unit (OU): "<Not Available>"
  ▼ Issued By
      Common Name (CN): "WE1"
      Organization (O): "Google Trust Services"
      Organizational Unit (OU): "<Not Available>"
  ▼ Period of Validity
      Begins On: "Sat, 14 Dec 2024 03:43:32 GMT"
      Expires On: "Fri, 14 Mar 2025 04:43:26 GMT"
  ▼ Fingerprints
```

7 requests | 97.48 kB / 61.39 kB transferred | Finish: 364 ms | DOMContentLoaded: 173 ms | load: 289 ms

Some basic intuition on lattice-based crypto

RSA

- Choose two large primes p and q.
- Let N = pq.
- It's easy to calculate N from p and q.
- It's hard to calculate p and q from N.

Learning with errors: encrypting with unsolvable equations

youtube.com/chalktalkmath

Learning With Errors (LWE)

- Create an array of n equations in the form:

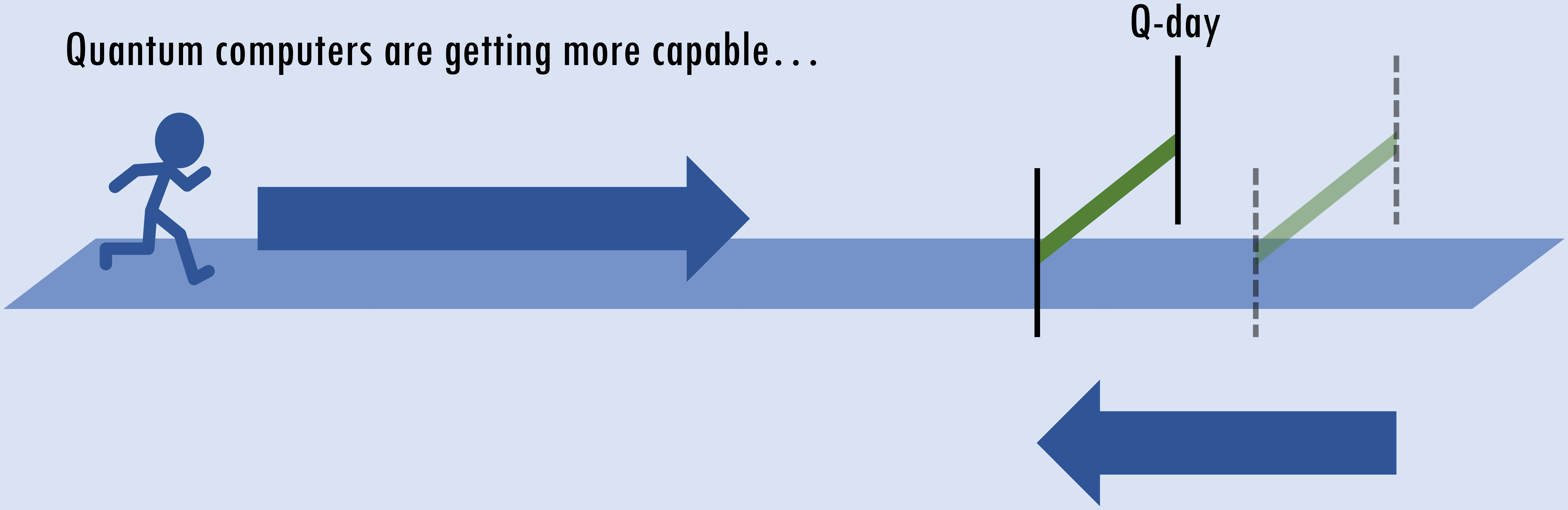
  $a_n x + b_n y + c_n z + e_n = N_n$
- Public key = [[a,b,c,N]]
- Private key = [x,y,z]
- Is hard to derive [x,y,z] due to:
  - The presence of a small error e
  - The number of equations to satisfy
- Plot twist: LWE doesn't use lattices at all! But has been shown to be an <u>equivalent</u> problem.

Recap on Objectives

1. Understand the **real threat** that quantum computing poses to security ✓
2. Understand the **options** for dealing with the quantum threat ✓
3. Understand the **timeline** for taking action ←

When do we need to worry?

Quantum computers are getting more capable…



…and researchers are finding ways to reduce the quantum volume required

When do we need to worry?

- Current quantum computers can only factor tiny numbers today.
- Pace of development is rapid… but it’s not just about # of qbits!
- “Harvest-now decrypt-later” possible – but impractical as a widescale threat.
- Possibly 2035? (Based on NSA’s own PQC plan to migrate by 2030/2033) [1]
- Transitioning is a multi-year process.
- Unlikely to be a ‘big-bang’; there’s other highly useful and easier computations that we’ll see first.
- But could a government agency already have a secret quantum computer? Maybe, but probably not.

[1] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Actions to start today

Also valuable against non-quantum threats!

- Crypto-agility: Be ready to adopt alternative cryptosystems!
  - Pluggable libraries that can be swapped in/out, with flexible data structures.
- Crypto-inventory: What crypto do you have and where, and who's accountable?
  - Algorithms, key sizes, protocols, libraries, certificates, etc.
  - Leverage existing tooling (e.g., Zeek can identify TLS crypto configs from network traffic).
  - Creates a baseline for the size and complexity of achieving crypto-agility – what's a priority, and what's hard to fix?
- Vendor engagement: What's the roadmap for the suppliers you depend upon? (inc. security vendors!)
- Experiment: Try out new algorithms, e.g., via OpenQuantumSafe, leverage proxy models, etc.
  - Identify gaps/incompatibilities, e.g., through protocol ossification or larger key sizes, etc.

Summary

- Quantum computing is a long-term threat.
- Replacing our cryptosystems is a long-term activity.
- No need to panic, but we should start planning & prioritising now.
- Beware vendor & media FUD!

Further Reading:

- https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
- https://blog.cloudflare.com/pq-2024/
- @quantum_village

Any questions?

@rot169

@rot169@infosec.exchange

youtube.com/rot169

github.com/rot169