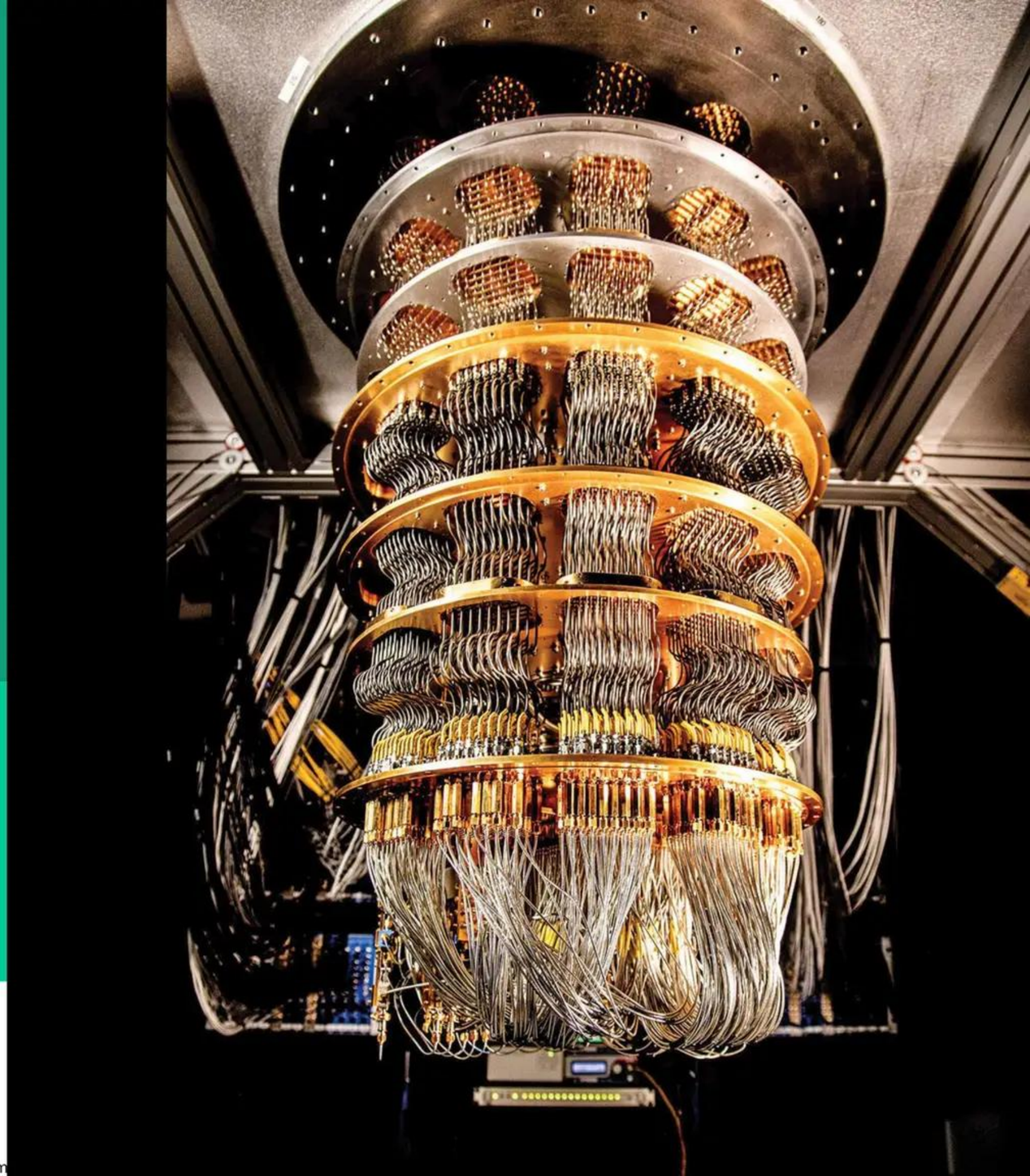
Post-Quantum Cryptography

...or how Kai almost hacked their mental health app

PALO IT

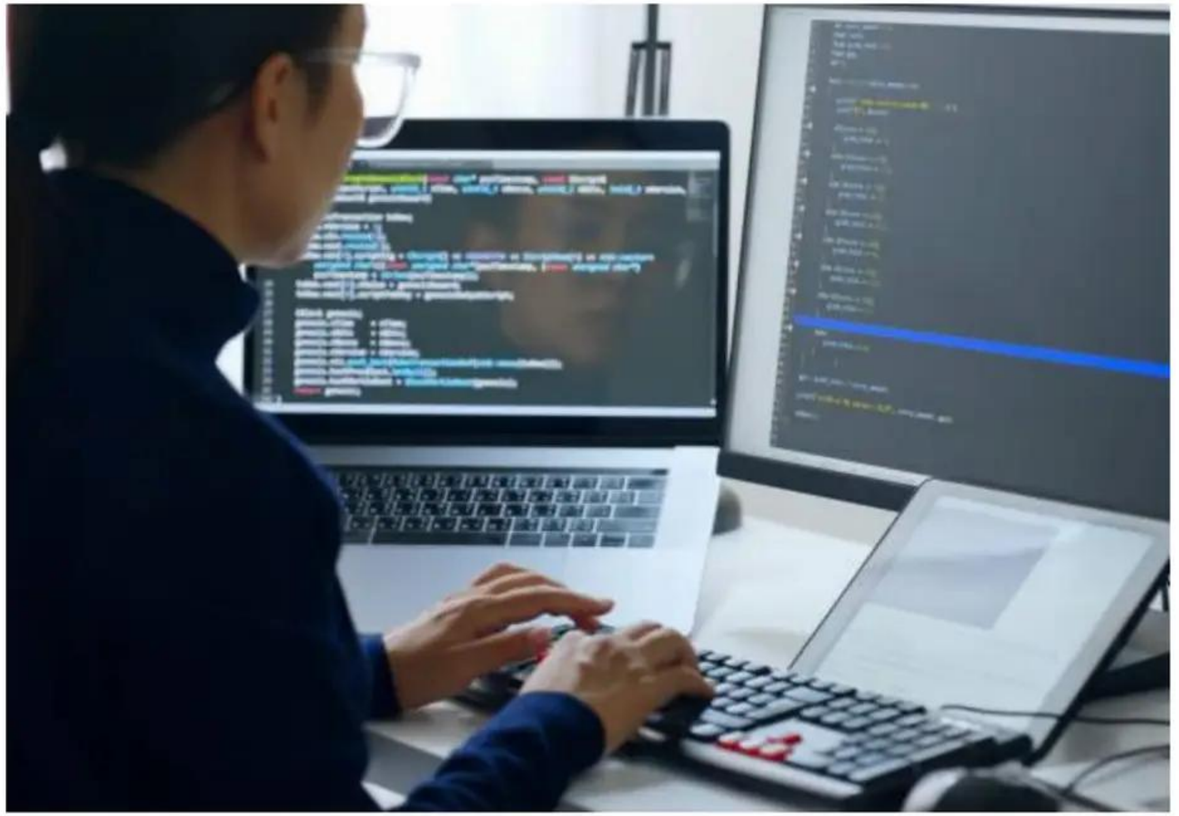


Kai and her git commit

KAI AND HER GIT COMMIT

Say hello to Kai!

- It's 2029
- Kai,
  - Full-stack engineer
  - Long-tenured MOHT employee
  - Working on a new mental health app
  - Arrives a Tuesday morning to the office...



KAI AND HER GIT COMMIT

Suweta's Code Review: "this looks strange..."

- MR for a new CRUD endpoint in a Django app (Code generation tool)
- CRUD endpoint
- Input sanitization through a serializer
- One of the fields accepts raw text → SQL injection vector
- ...but Kai is sure she didn't write that line!

KAI AND HER GIT COMMIT

Kai checks the commit...

- Checks the commit on GitLab app
- PGP signed by her
- She pushed yesterday by SSH (as usual)
- Commit is from the right time, 5:07pm
- No force-push

How could this happen?

- Kai follows good security practices:
  - locks her screen when she's away,
  - Uses strong passwords,
  - uses VPN when appropriate
  - ...

- Cracking SSH or PGP keys takes millions of years with a supercomputer, right?

Let's talk quantum

What's the type of encryption that can be broken by quantum cryptography?

PALO IT

LET'S TALK QUANTUM

To know what happened...

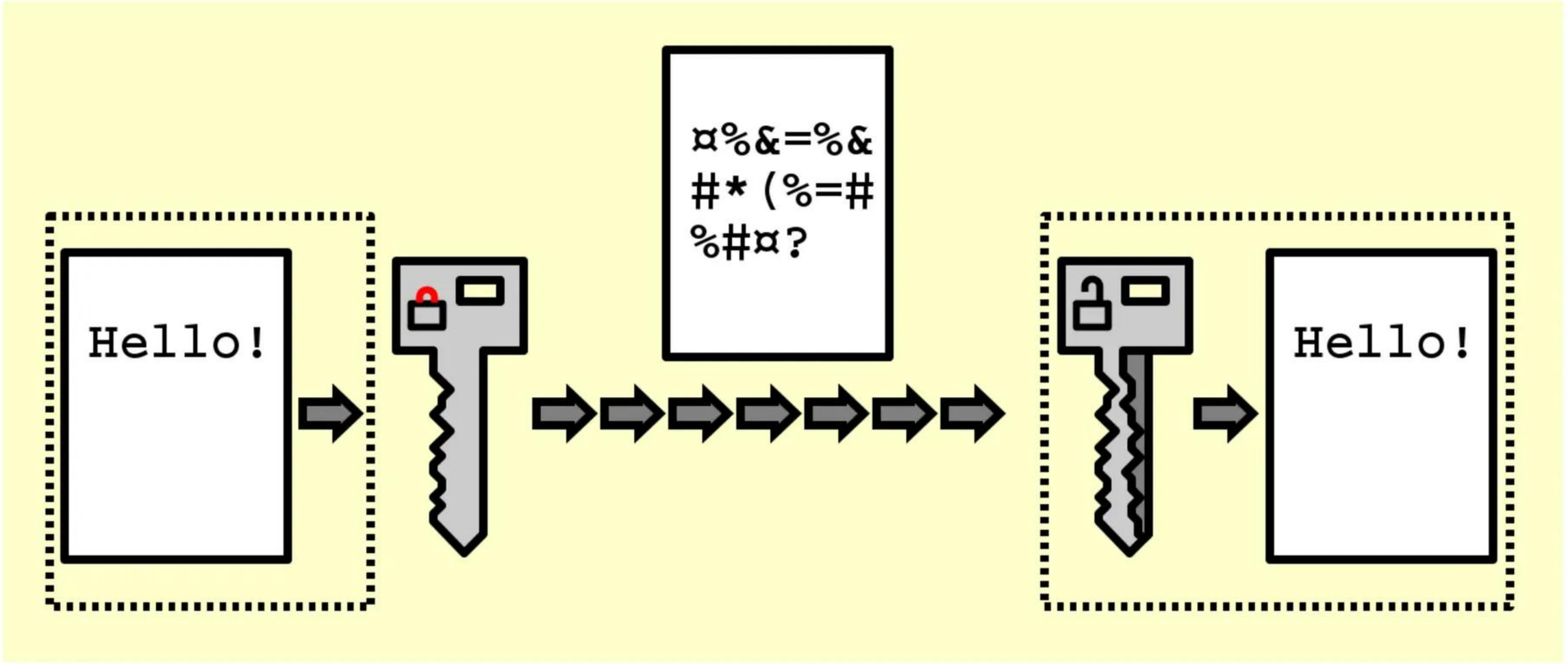
- How encryption works
- Public Key Cryptography (not symmetric)
- Integer factorization
- P versus NP problem, Complexity theory
- BQP ➡️ Quantum computers
- ...all this in 5 minutes!

Let's talk encryption

...for 5 minutes

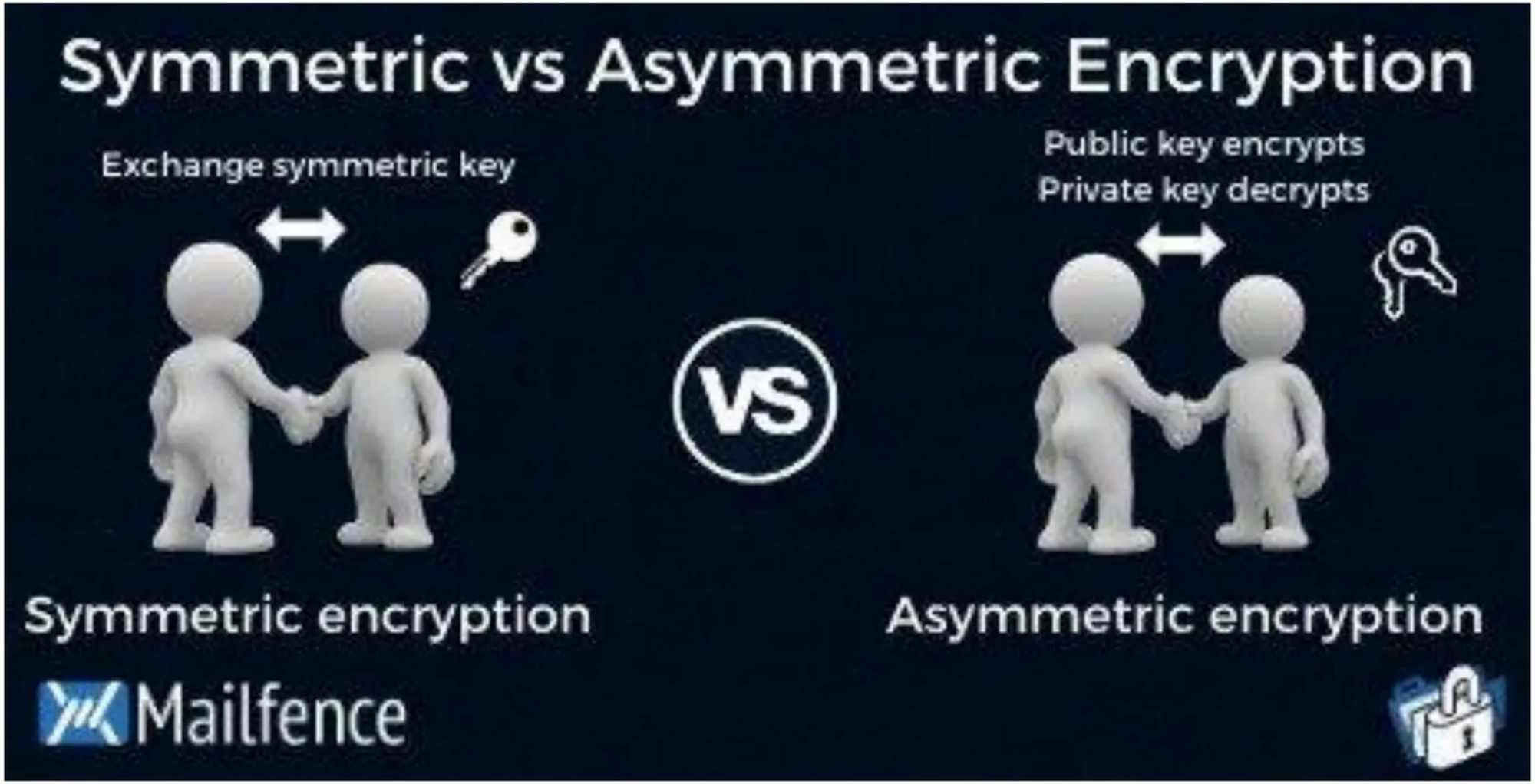
HOW ENCRYPTION WORKS

Encryption = garble & ungarble



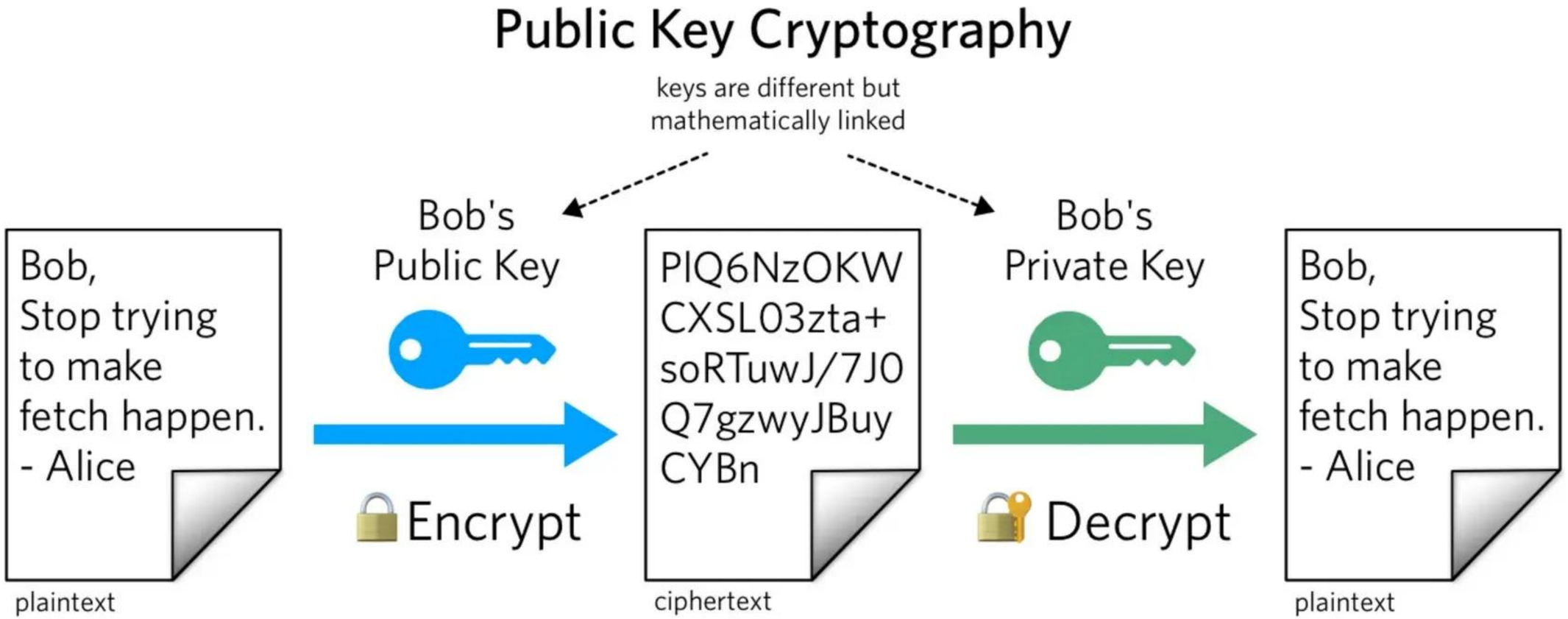
HOW ENCRYPTION WORKS

Symmetric vs Asymmetric cryptography



HOW ENCRYPTION WORKS

Public Key Cryptography: asymetric encryption



HOW ENCRYPTION WORKS

Public Key Cryptography

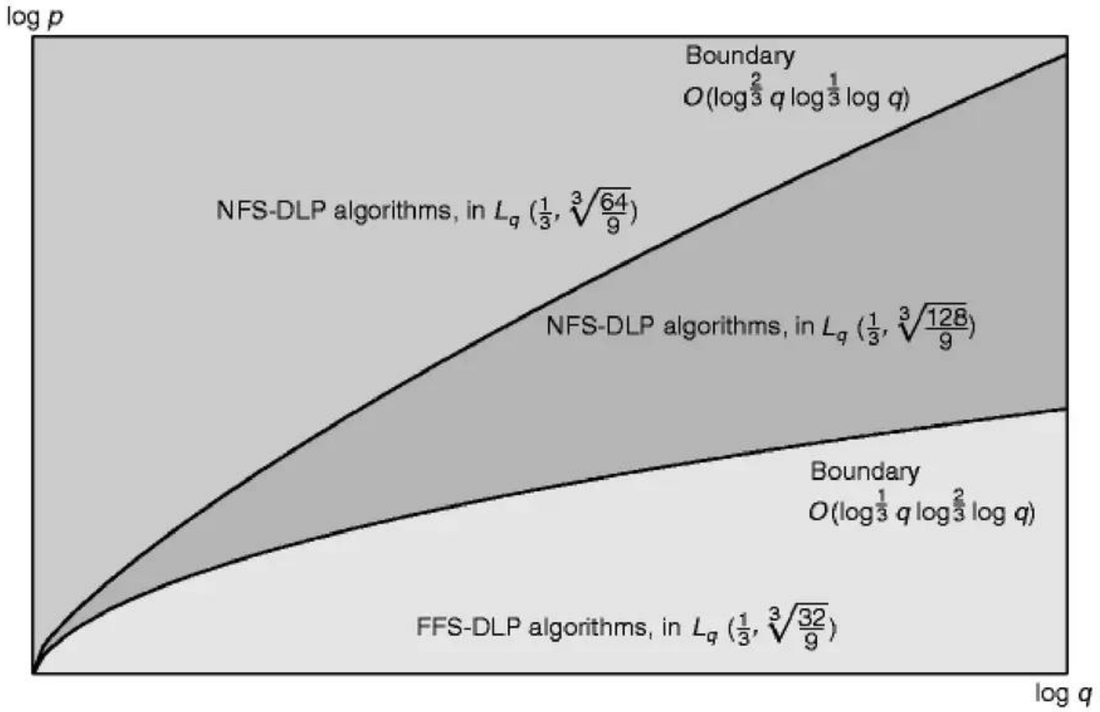
Algorithms:

- Integer factorization: RSA
- Discrete logarithm: Diffie-Hellman Key Exchange, ECDSA (GitHub keys)

...solved by Quantum Computers!

Integer Factorization

- Most efficient classical algorithm: General Number Field Sieve
- Complexity:

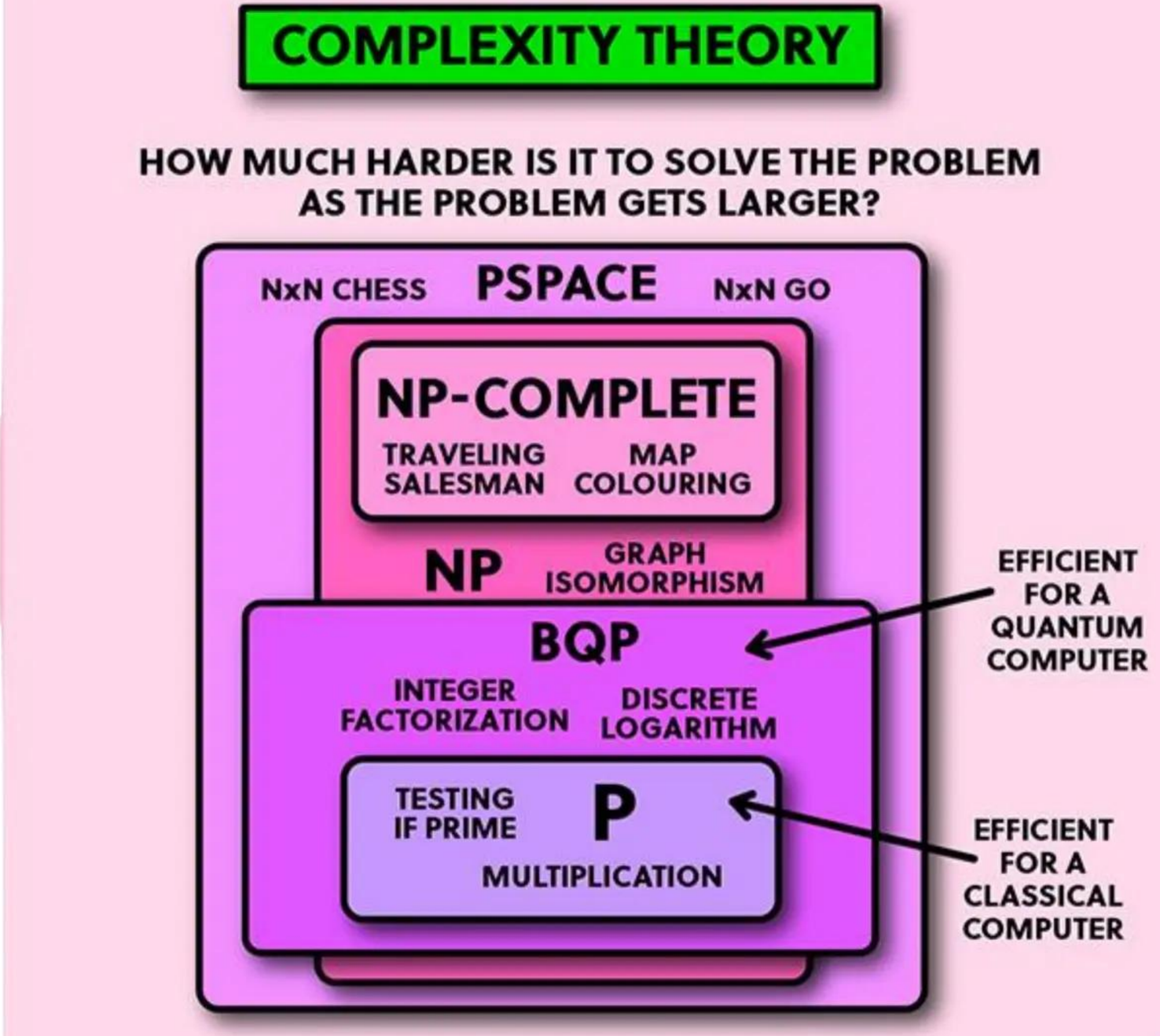


- … puts it in the NP space

HOW ENCRYPTION WORKS

Complexity Theory

- ...what is that BQP thing?
- Bounded-error Quantum Polynomial time
- Finally, Quantum Computers!



Quantum Collapse

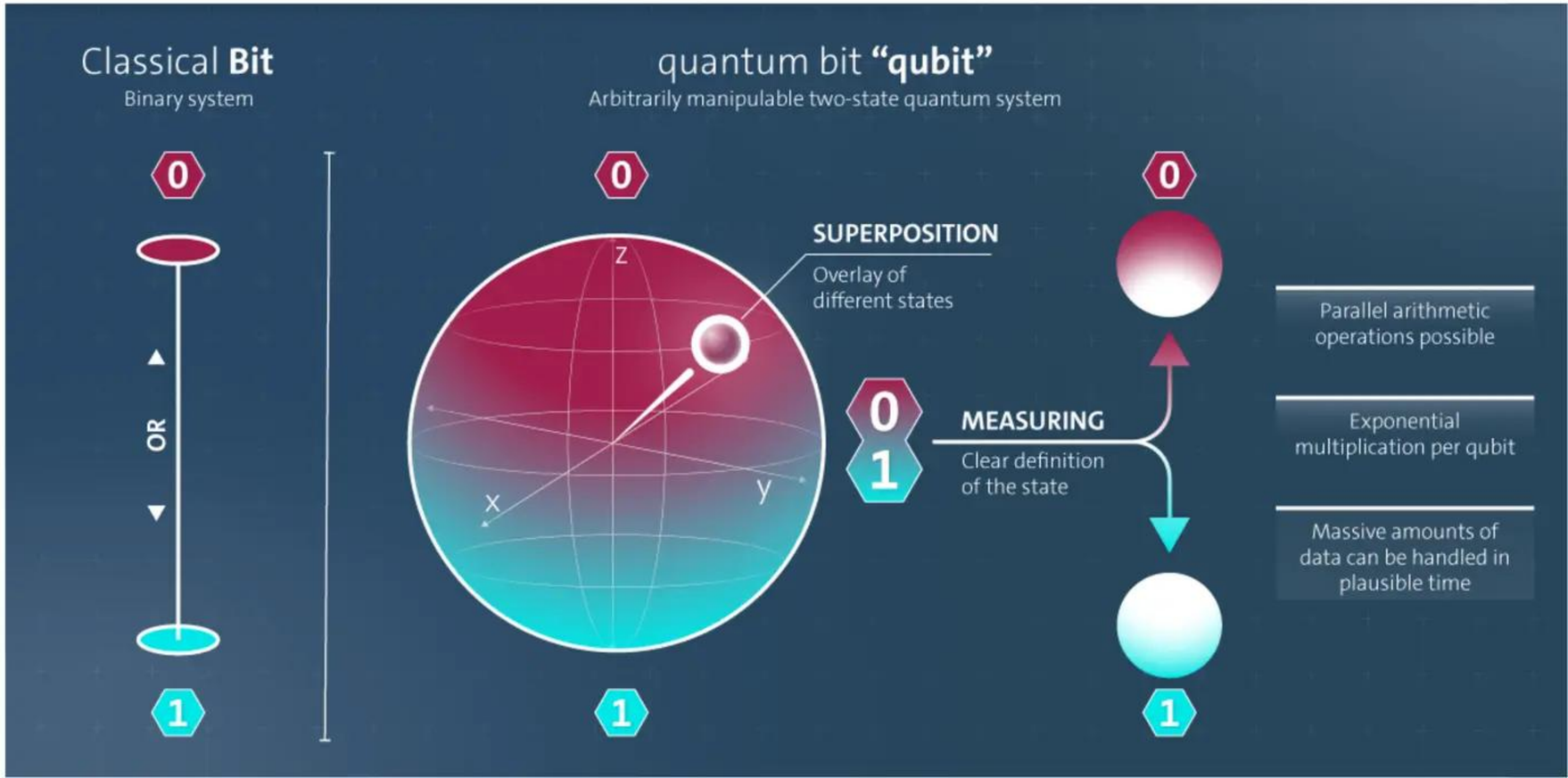
...QFT, superposition, entanglement, qubits (society as well?)

PALO IT

QUANTUM COLLAPSE

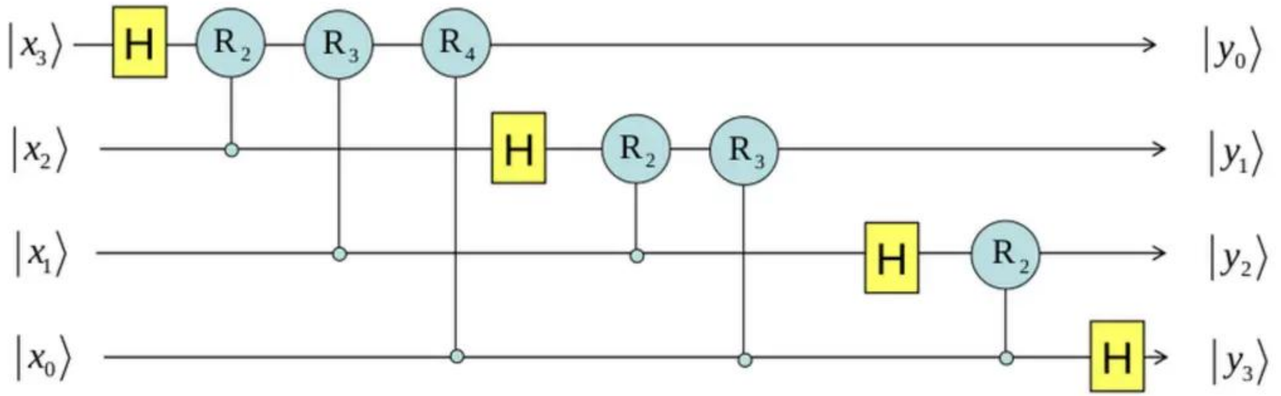
What is a qubit?

- Superposition: "Sphere of probability"
- 1 bit = 2 states, 2 bits = 4, 3 = 8... states = 2^qbit_count
- When read, collapses ➡️
  - one state appears



What do I use it for?

Quantum Fourier Transform



$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_y e^{\frac{2\pi i}{2^n} xy} |y\rangle$$

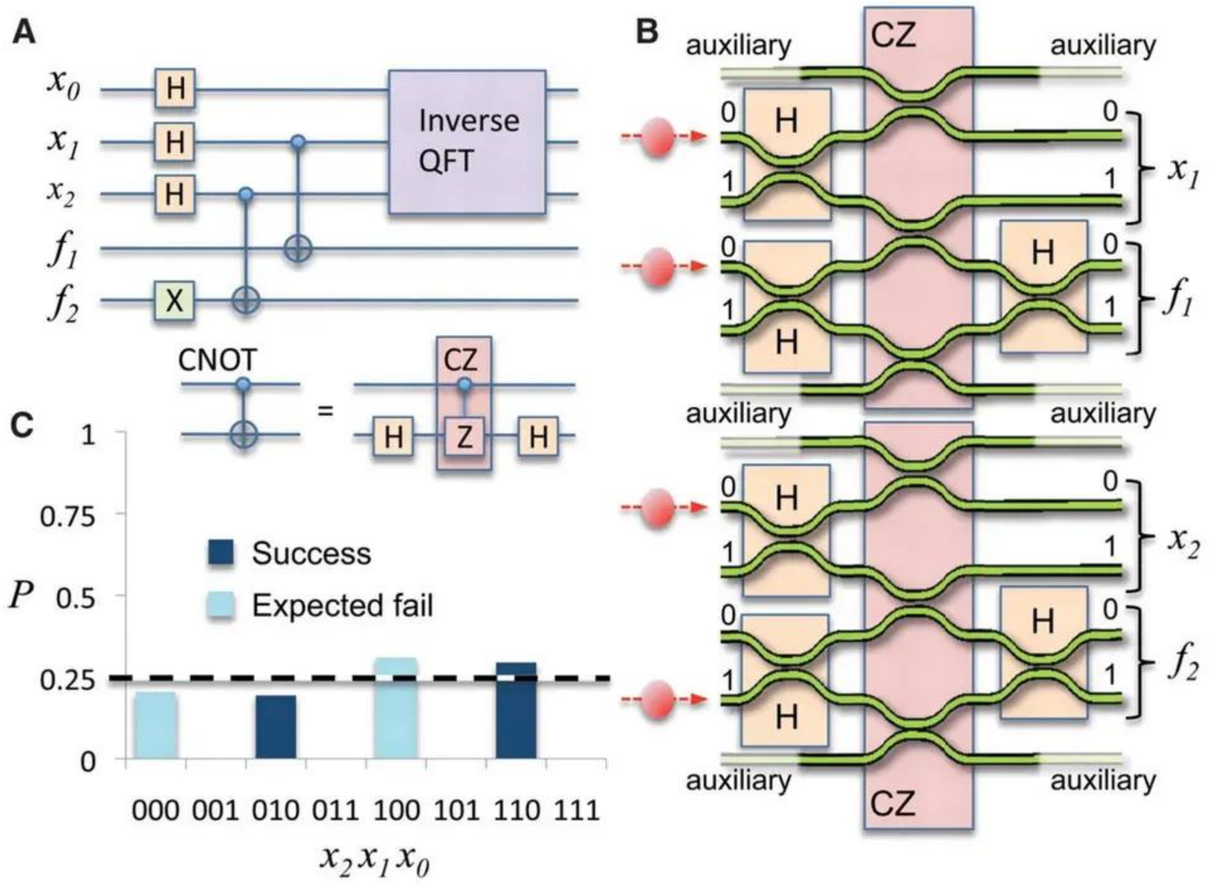
Uniform family of networks

n Hadamard gates and n(n-1)/2 phase shifts, the size of the network = n(n+1)/2

QUANTUM COLLAPSE

QFT for

- Shor's algorithm
- Solves integer factorization in BPQ time
- ...we just need a lot of qubits

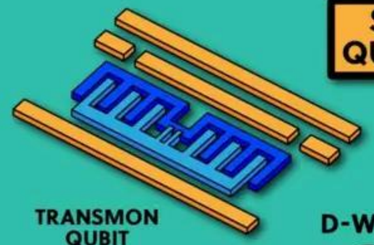


COMPANY QUBIT COUNTS JAN 2022

UNIVERSAL QC

NOT UNIVERSAL QC

SUPERCONDUCTING QUANTUM COMPUTERS



TRANSMON QUBIT

IBM 127

GOOGLE 53

D-WAVE 5760 (QUANTUM ANNEALING)

INTEL 49

QUTECH

UST OF CHINA 66

RIGETTI 80

QUANTUM CIRCUITS

ALIBABA QUANTUM LABORATORY 11

BLEXIMO

SEEQC

OXFORD QUANTUM CIRCUITS

ALICE & BOB

QUANTWARE

ORIGIN QUANTUM

IQM QUANTUM COMPUTERS

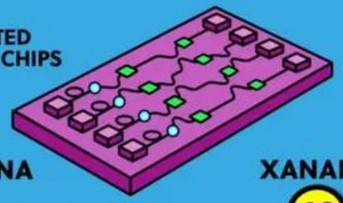
AMAZON

RAYTHEON BBN

NORTHROP GRUMMAN

OPTICAL QUANTUM COMPUTERS

INTEGRATED PHOTONICS CHIPS



UST OF CHINA 113 (NUMBER OF PHOTONS IN A BOSON SAMPLER)

XANADU 40

PSIQUANTUM

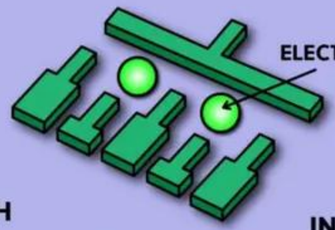
QUIX QUANTUM

ORCA COMPUTING

QUANDELA

QUANTUM DOT QUANTUM COMPUTERS

ALSO SILICON SPIN QUANTUM COMPUTERS



ELECTRONS

QUTECH

INTEL

CEA-LETI

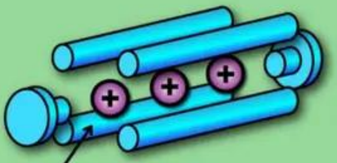
PHOTONIC

HRL LABORATORIES

QUANTUM MOTION

RIKEN CENTER FOR QUANTUM COMPUTING

TRAPPED ION QUANTUM COMPUTERS



IONISED ATOMS TRAPPED IN ELECTRIC FIELDS

QUANTINUUM 12

IONQ 32

OXIONICS

ALPINE QUANTUM TECHNOLOGIES 24

UNIVERSAL QUANTUM

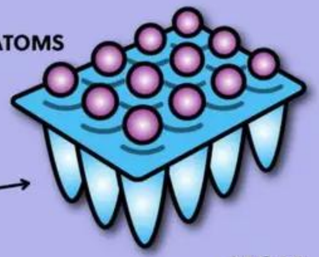
INFINEON

OXFORD IONICS

QSCOUT

NEUTRAL ATOMS IN OPTICAL TWEEZER ARRAY

TRAPPED ATOMS



TWEEZER ARRAYS

COLDQUANTA 100

ATOM COMPUTING 100

PASQAL 200 (QUANTUM SIMULATOR NUMBER OF ATOMS)

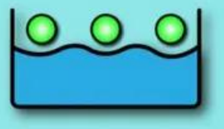
QUERA 256 (QUANTUM SIMULATOR NUMBER OF ATOMS)

TOPOLOGICAL QUANTUM COMPUTERS

MICROSOFT

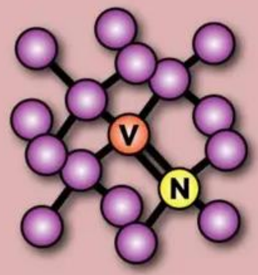
QUTECH

ELECTRON-ON-HELIUM QUANTUM COMPUTERS



EEROQ 1

COLOUR CENTRE QUANTUM COMPUTERS



QUTECH

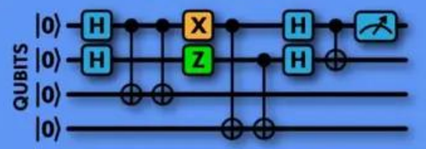
SQC

QUANTUM BRILLIANCE 2

INTERNATIONAL IBERIAN NANOTECH LAB

NON-HARDWARE QUANTUM COMPANIES

SOFTWARE TOOLS, RESEARCH AND APPLICATIONS



QUANTINUUM

RIVERLANE

MULTIVERSE COMPUTING

BLUEQAT

BAIDU

PHASECRAFT

QU & CO

CLASSIQ

ZAPATA COMPUTING

1QUBIT

HEISENBERG QUANTUM SIMULATIONS

QSIMULATE

KEYSIGHT Q

QUBITOR LABS

HORIZON

Q-CTRL

QUNASYS

ENTROPICA LABS

STRANGEWORKS

ATOS

QC WARE

PARITY QC

SOFTWARE PACKAGES

QISKIT (IBM)

PYQUIL (RIGETTI)

CIRQ (GOOGLE QUANTUM AI)

Q# (MICROSOFT)

PENNYLANE (XANADU)

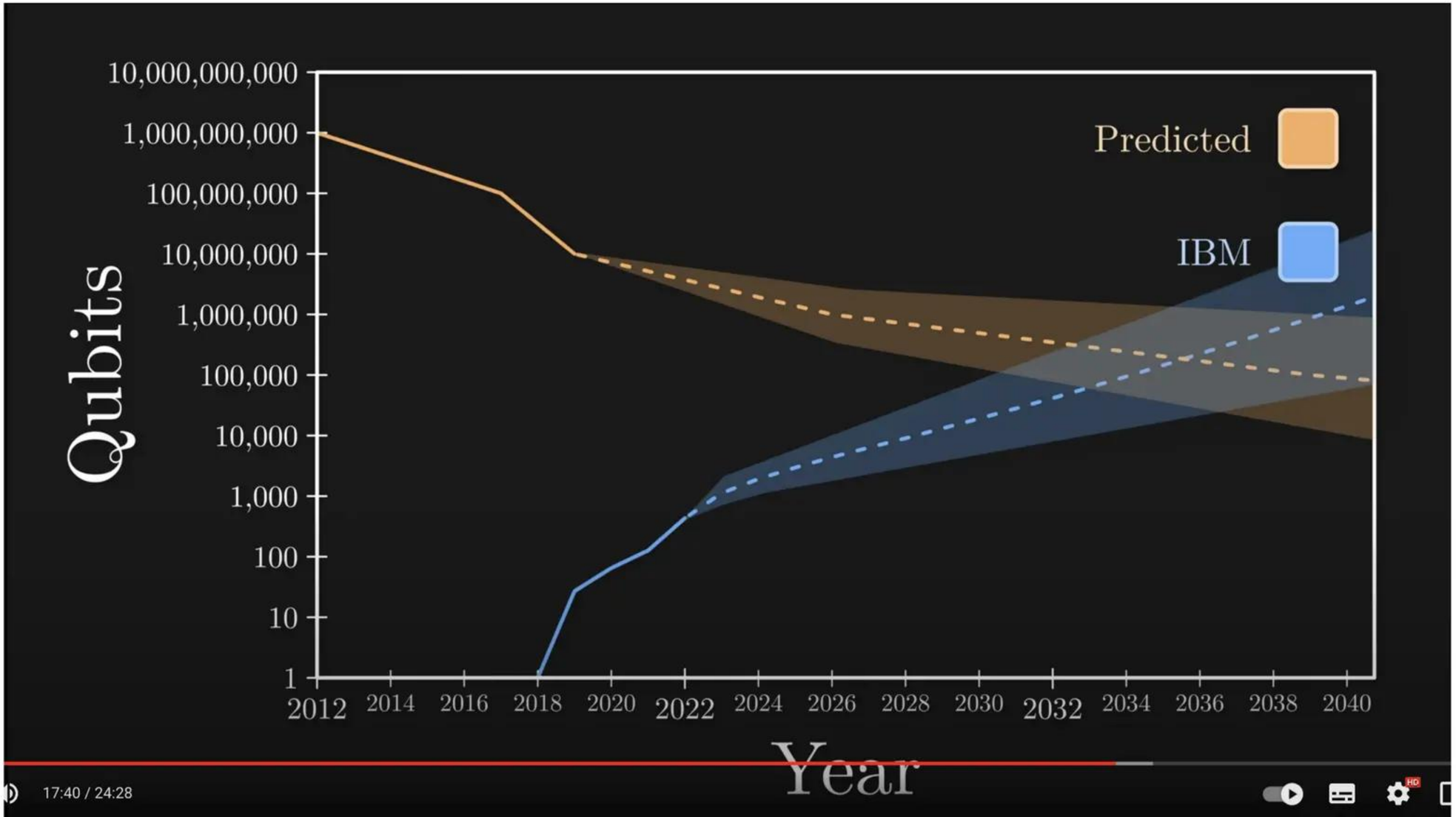
Circuit-based quantum processors [edit]

These QPUs are based on the quantum circuit and quantum logic gate-based model of computing.

Manufacturer	Name/ codename designation	Architecture	Layout	Fidelity (%)	Qubits (physical)	Release date
Atom Computing	N/A	Neutral atoms in optical lattices	35×35 lattice (with 45 vacancies)	< 99.5 (2 qubits)[6]	1180[7][8]	October 2023
IBM	IBM Condor[18] [7]	Superconducting	Honeycomb[19]	N/A	1121[17]	December 2023
CAS	Xiaohong[71]	Superconducting	N/A	N/A	504[71]	2024
IBM	IBM Osprey[7][8]	Superconducting	N/A	N/A	433[17]	November 2022
Xanadu	Borealis[69]	Photonics (Continuous-variable)	N/A	N/A	216[69]	2022[69]
M Squared Lasers	Maxwell	Neutral atoms in optical lattices		99.5 (3-qubit gate), 99.1 (4-qubit gate) [35]	200[36]	November 2022
IBM	IBM Heron R2[20]	Superconducting	Heavy hex	96.5 (2 qubits)	156	November 2024
IBM	IBM Heron[18][7]	Superconducting	N/A	N/A	133	December 2023
IBM	IBM Eagle	Superconducting transmon	N/A	N/A	127[17]	November 2021
USTC	Zuchongzhi 3.0[68]	Superconducting transmon	15 x 7	99.90 (Single-qubit gates) 99.62 (Two-qubit gates) 99.18 (Readout)	105	December 16, 2024
Atom Computing	Phoenix	Neutral atoms in optical lattices			100[5]	August 10, 2021

QUANTUM COLLAPSE

Qubit growth vs algo efficiency



QUANTUM COLLAPSE

Advances are accelerating

News • February 19, 2025 • 7 min read

Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits

by Chetan Nayak, Technical Fellow and Corporate Vice President of Quantum Hardware

The world's first Quantum Processing Unit (QPU) powered by a Topological Core, designed to scale to **a million qubits** on a single chip.

https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

What happened to Kai?

...or, "quantum computers break that too?!"

(suspend your disbelief a bit for a while please ^^)

PALO IT

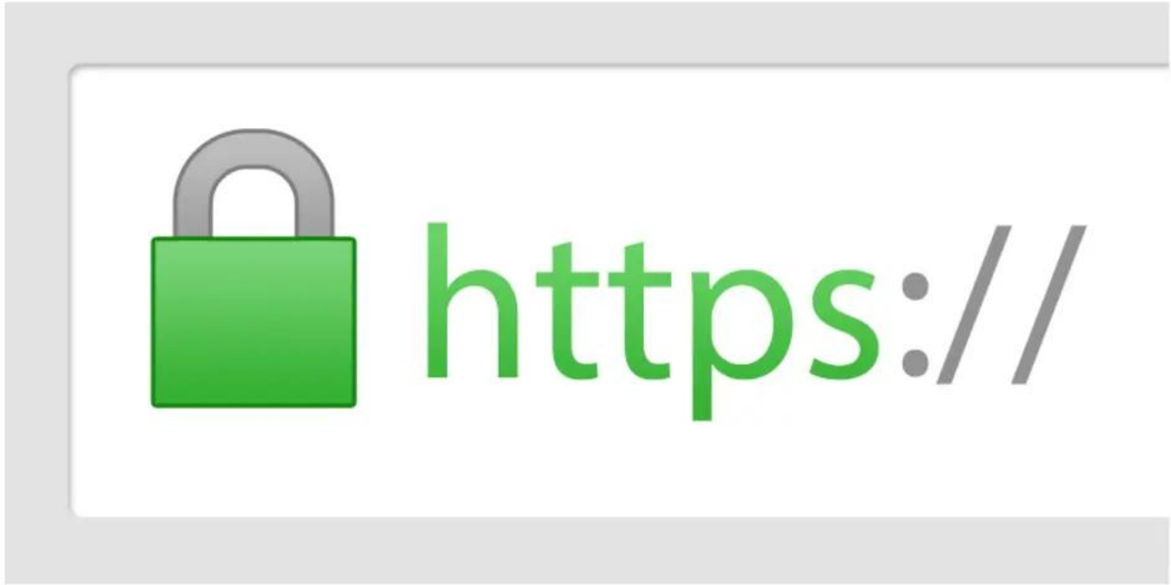
WHAT HAPPENED TO KAI?

SSH key

- Kai had an old SSH key last used 2 years ago using Ed25519
- Private key can be deduced public key can be deduced using Shor's, encryption broken!
- An attacker can't get the public key right? She set it up on GitLab's UI which uses...

HTTPS

- GitLab.com uses HTTPS, where she set her SSH public key
- Public key → Private key using Shor's, SSH auth roken!
- good thing that Kai follows security recommendations, so she was using a...



VPN

- She was using a VPN in the office to do this sensitive operation
- VPN uses AES PKC to protect the transfer of AES keys → broken!
- Anyway, she was on a WiFi with WPA3, uses safe symmetrical encryption, however…

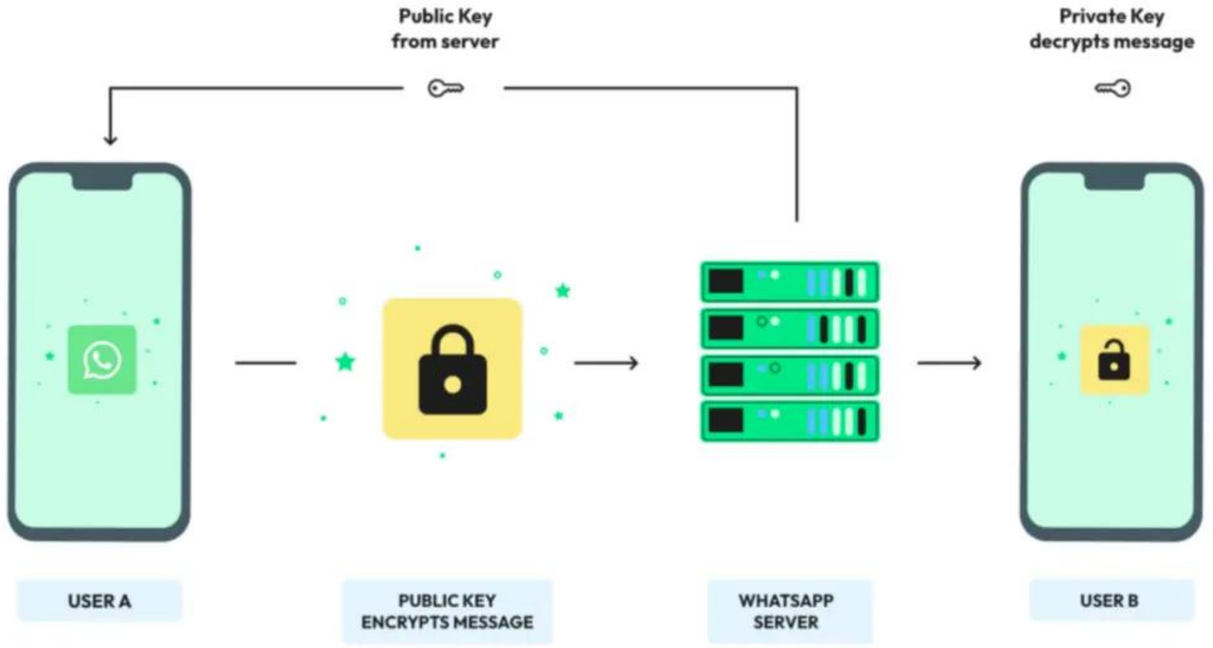
WHAT HAPPENED TO KAI?

Digital Signature

- Routers in the office get updates that are digitally-signed
- Digital Signature = PKC = broken, router was hacked!
- ...but how was Kai targeted in the first place?

E2E Encryption

- She was talking to a friend through WhatsApp about the mental health app project
- WhatsApp uses E2E encryption, uses PKC, broken!
- ...and reading her messages the hacker knew how to target the hack! But why her?



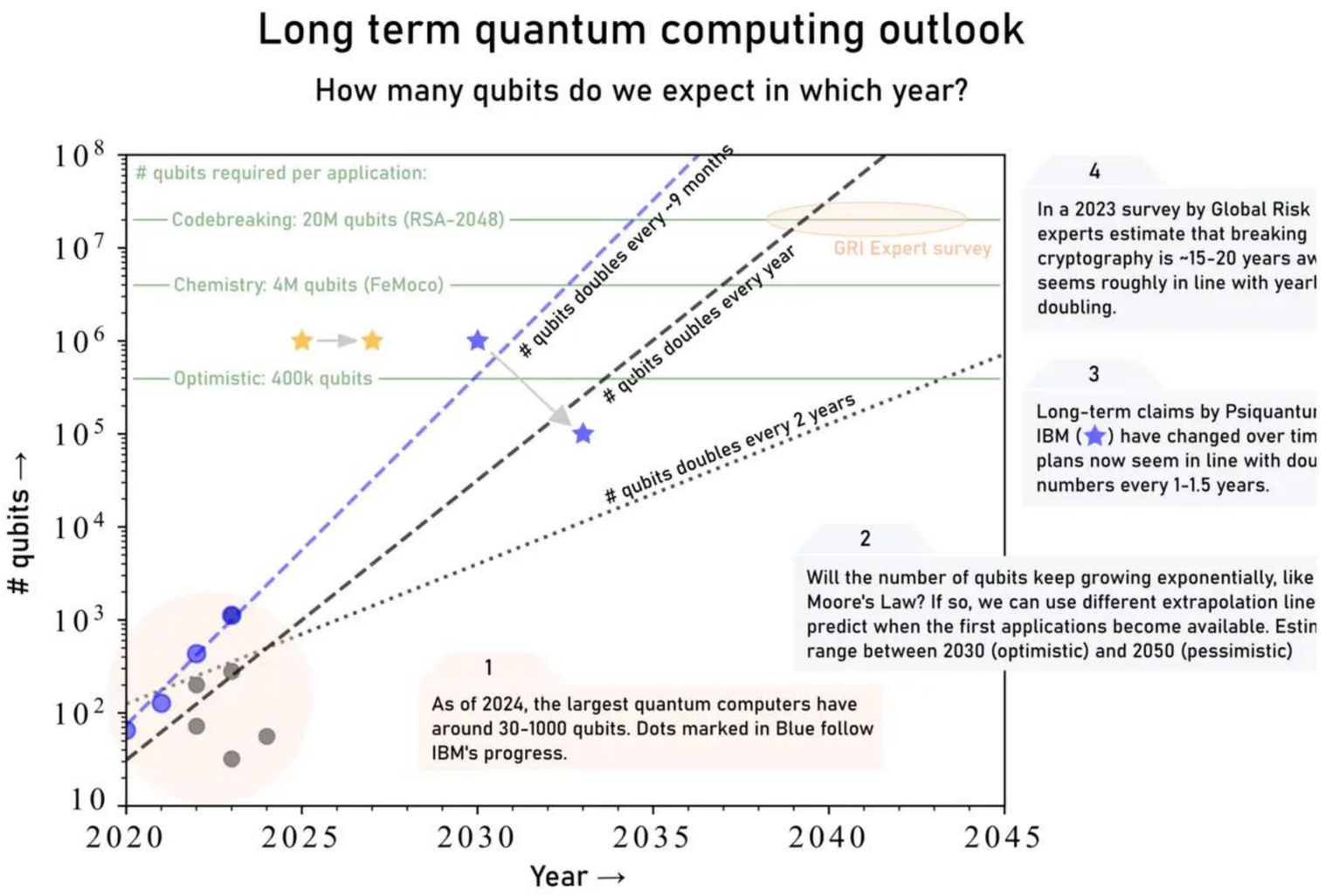
Cryptocurrencies

- Because I paid for the attack to steal the DB's data!
- I paid the hacker in crypto, but...
- Wallet addresses use PKC, broken!
- And then the hacker stole all my crypto as well!

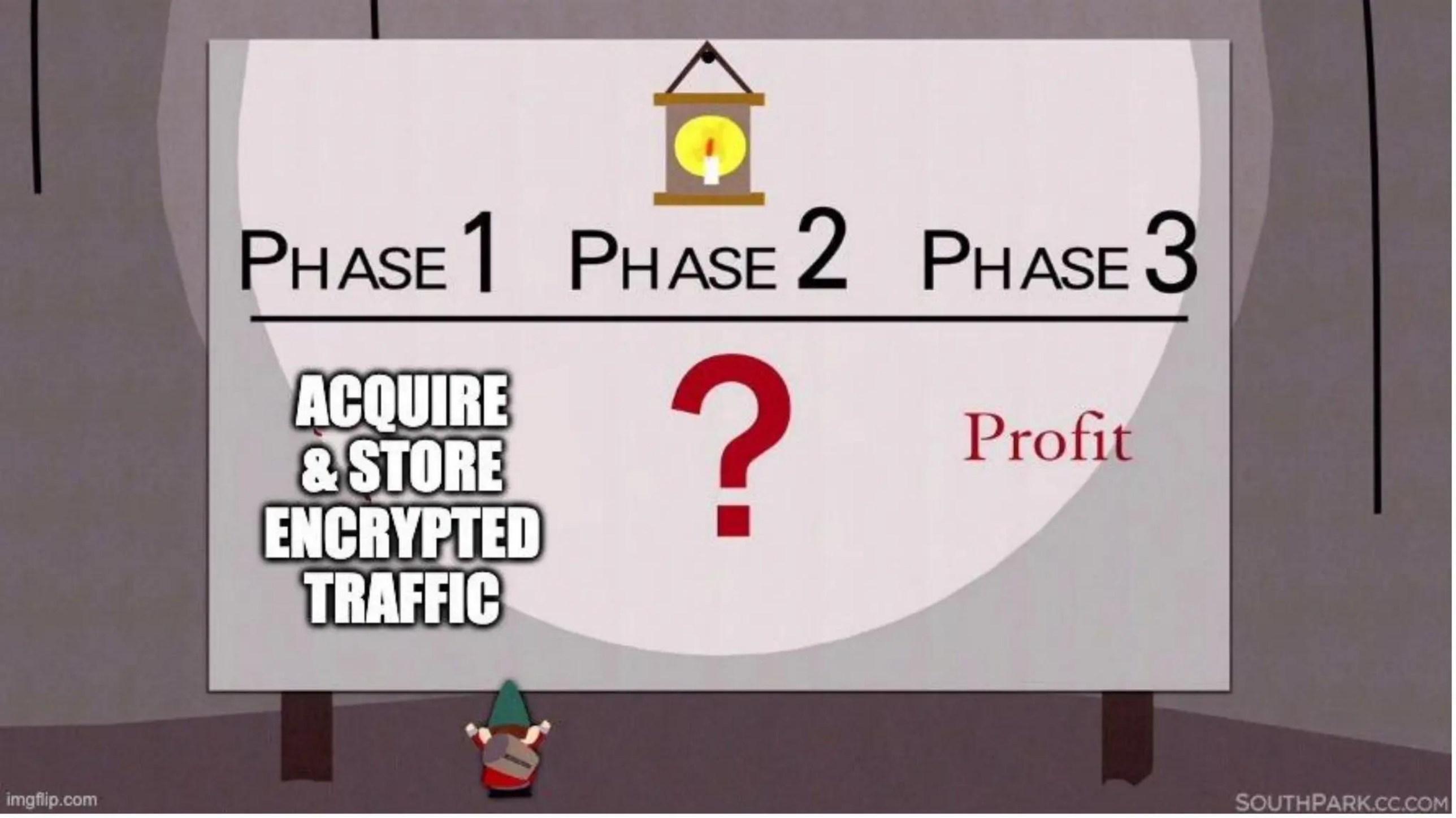
WHAT HAPPENED TO KAI?

Wait wait wait... why should I worry now?

- This is not a problem yet, right?
- 5 – 10 years horizon
- Introducing...

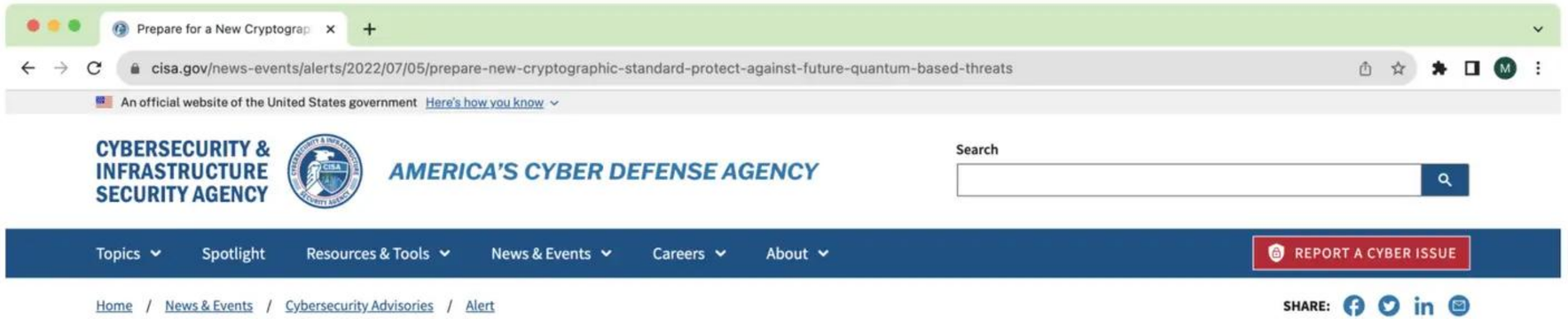


Store now, decrypt later


PHASE 1
PHASE 2
PHASE 3
ACQUIRE & STORE ENCRYPTED TRAFFIC
?
Profit
imgflip.com
SOUTHPARK.CC.COM

STORE NOW, DECRYPT LATER

The US government is preparing already



ALERT

Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats

Last Revised: July 05, 2022

The National Institute of Standards and Technology (NIST) has announced that a new post-quantum cryptographic standard will replace current public-key cryptography, which is vulnerable to quantum-based attacks. **Note:** the term "post-quantum cryptography" is often referred to as "quantum-resistant cryptography" and includes, "cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a CRQC [cryptanalytically relevant quantum computer] or classical computer." (See the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems for more information).

World Wide Web

of consequences

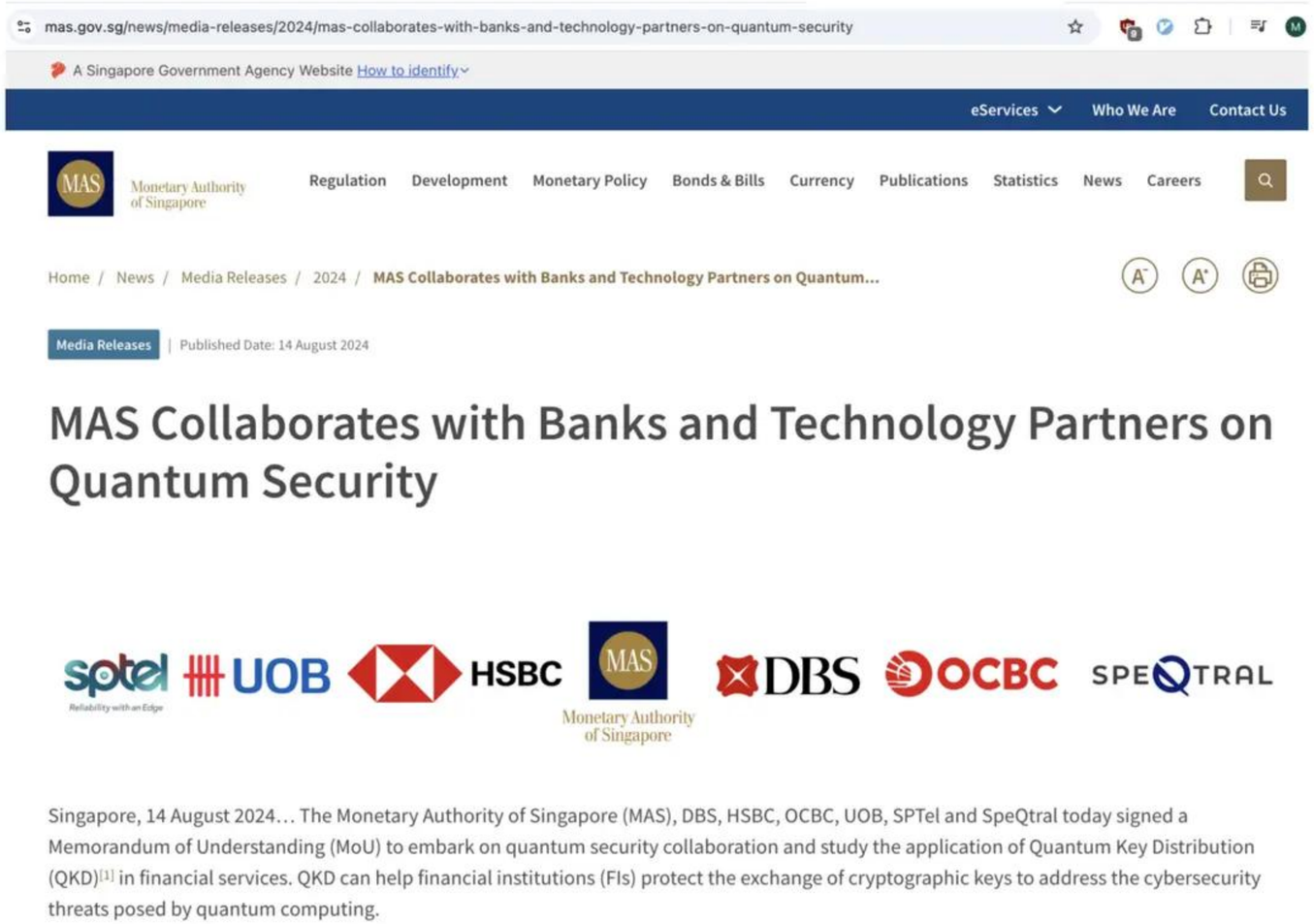
PALO IT

Governments

- Will be fine
- Most likely militaries around the world have their own quantum computers already

Big companies (including banks)

- Will be fine
- Either have their own already, will have, or will be protected beforehand
- Example: Singapore, August 2024



SMEs

- Their IT departments better stay up to date!
- ...specially if they handle money or PII

WWW OF CONSEQUENCES

Old running systems using PKC

- e.g.:
  - Servers using SSH login
  - Servers using SFTP
  - Email servers
  - VPN clients
  - Software using digitally-signed updates
- Update or be vulnerable

WWW OF CONSEQUENCES

Cryptocurrencies

- Exchanges will update
- Big chains will update: Bitcoin, Ethereum
- What about forks, altcoins?
- Self-managed wallets:
  - Live wallets: update wallet software to use PQC
  - Abandoned wallets in obsolete chains: open season!

How exactly do we prepare

- We need some PKC for the post-quantum world
- We could call that something like…

Post-Quantum Cryptography

it took a while, but yeah!

PALO IT

POST-QUANTUM CRYPTOGRAPHY

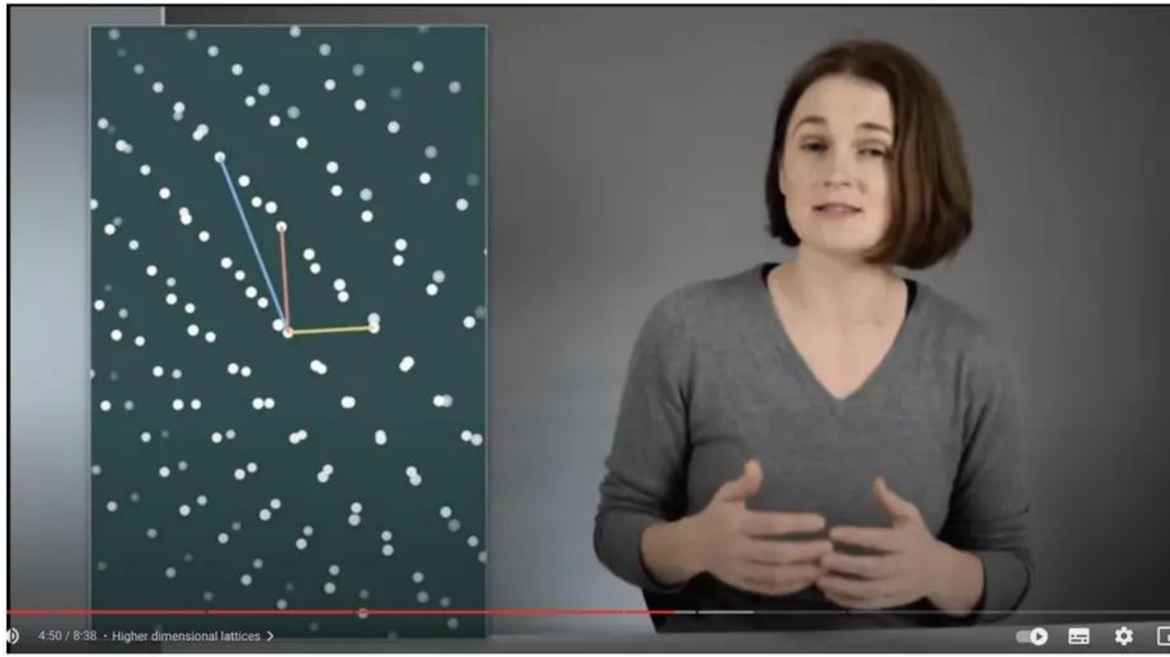
What is broken in PKC?

- Integer factorization
- Discrete logarithm

POST-QUANTUM CRYPTOGRAPHY

What is not?

- Ring-learning with errors (Ring-LWE)
  - Based on the hardness of lattice-based problems
  - Here's a video to know more:
  - youtu.be/QDdOoYdb748



POST-QUANTUM CRYPTOGRAPHY

Show me the code

4 NIST PQC Algorithms:

- From a 6-year competition

www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

POST-QUANTUM CRYPTOGRAPHY

And the winners are...

For general encryption to access secure websites:

- CRYSTALS-Kyber
  - Small encryption keys
  - Fast operation speed

POST-QUANTUM CRYPTOGRAPHY

And the winners are...

For Digital Signatures:

- CRYSTALS-Dilithium
  - High efficiency, primary
- FALCON
  - ⑩ High efficiency, smaller signatures
- SPHINCS+
  - Larger, slower
  - **Important!: Not based on lattice math**

What should I do now?

Defense Against the (future) Quantum Arts

PALO IT

WHAT SHOULD I DO NOW?

For general users

- Not much, tech people will take care of it ;)

WHAT SHOULD I DO NOW?

Tech people: Frontend

- When using public keys:
  - SSH, PGP, ...
  - Be on the lookout for new quantum-resistant algo choices
  - Use them
- Warning Horizon: ~5 years from now

WHAT SHOULD I DO NOW?

Tech people: Backend/DevOps & more

- Stakes are higher
- Inter-system communication:
  - API_TOKEN, automated SSH or SFTP, ...
  - Use QR-algos
  - Horizon: ~4-5 years
- Direct calls to PKC libraries or code:
  - Use QR-algos: ~3-2 years
- HTTP Certs, other DevOps stuff (not an expert): same applies

WHAT SHOULD I DO NOW?

Tech people: Security

- This responsibility is part of your JD ;)
- Read more about these topics
- Get acquainted with new attack vectors on PKC
- Check the 4 NIST algorithms and their usage
- Try them out! openquantumsafe.org
- Warning Horizon: now!

WHAT SHOULD I DO NOW?

Cryptocurrency user

1. Panic
2. Stay updated with your exchanges/chain(s)' work towards using QR-PKC
3. If their timeline doesn’t look good, move the assets to other QR-exchanges/chains
   - Some big ones are doing it already, but there is a lot of misinformation/blogspam.
   - DYOR

Closing notes

...those were a lot of slides!

CLOSING NOTES

Thank you all! 🤦

- We can see now that Code Reviews are useful right? Remember Suweta? ^^
- Very interesting but complicated topic, hope I picked your curiosity to delve deeper into the issue.
- Questions, comments?