POST-QUANTUM CRYPTOGRAPHY

JAIMEE BROWN

TERON LABS

About Me

- Research engineer at Teron Labs
- 10+ years as software engineer
- PhD in public key cryptography at QUT

About Teron Labs

- Specialise in security certifications for software and hardware modules
- Help organisations gain certifications vital to their business
- Research projects in security-related fields

POST-QUANTUM CRYPTOGRAPHY

QUANTUM-

RAPHY

Asymmetric (public key)

Cryptographic algorithms that run on classical computers

Q

Resistant to quantum computer and non-quantum computer attack

QUANTUM COMPUTING

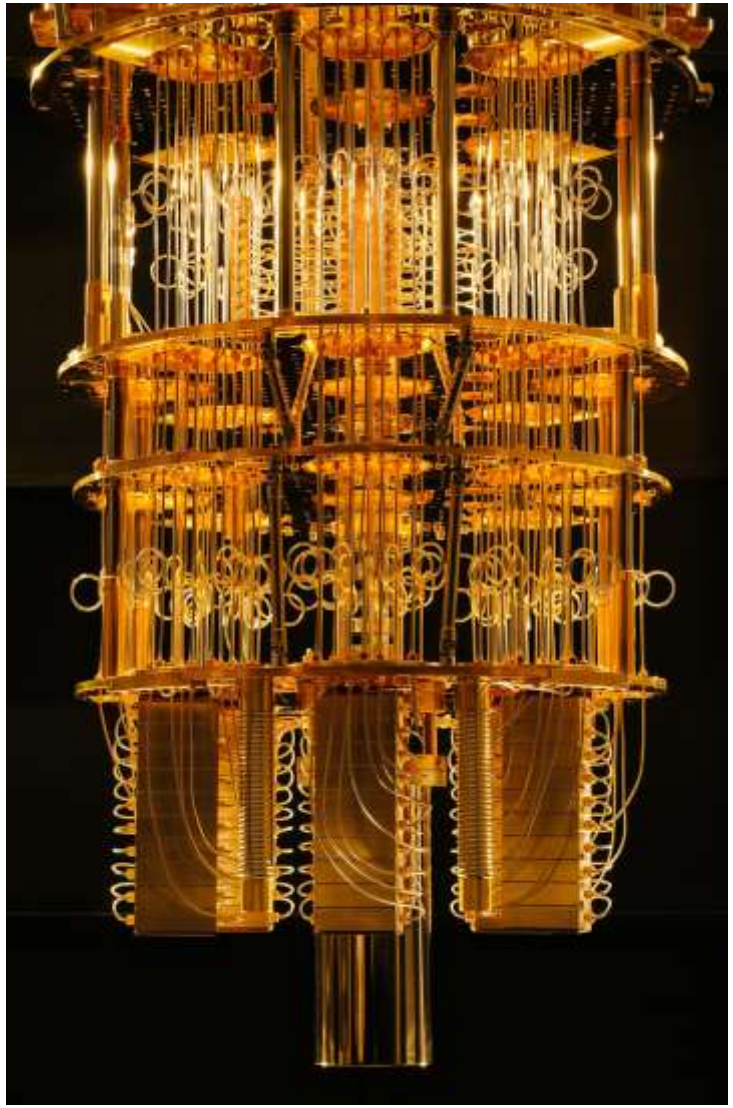
A completely different type of computing to ‘classical’ computers.

- Quantum bits (qubits)

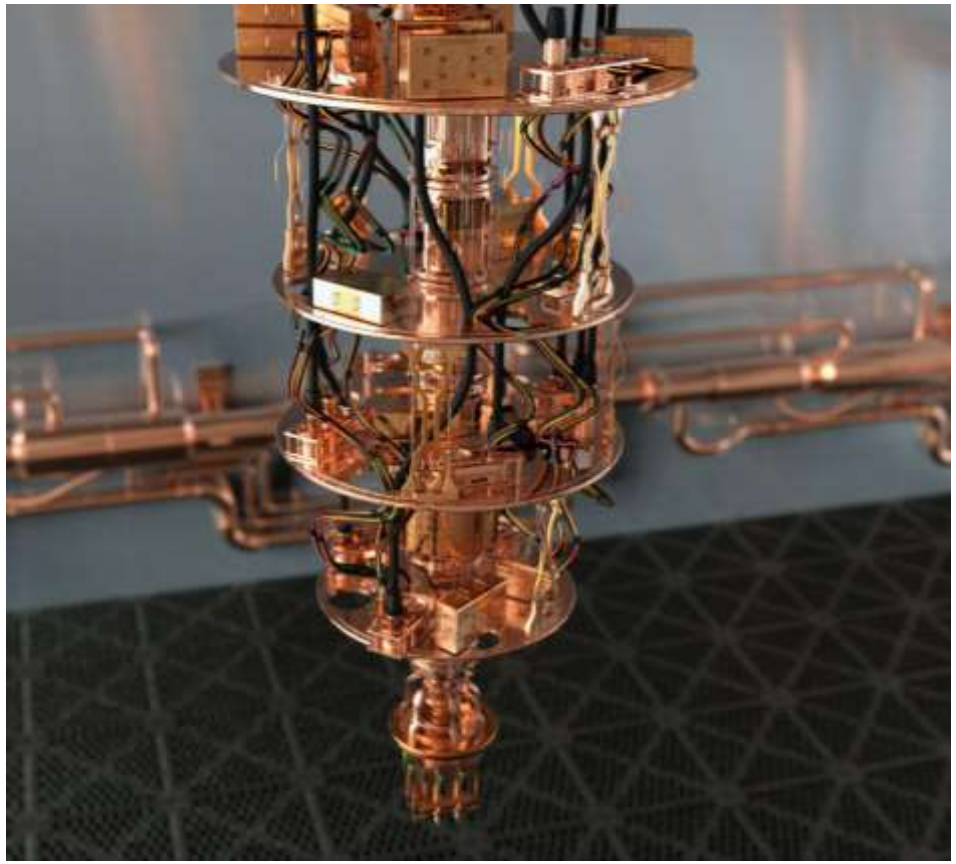
Uses fundamental principals of quantum mechanics to perform computations.

- Superposition, entanglement

Quantum computers attempt to harness the peculiarities of quantum mechanics to revolutionize computing power.



QUANTUM COMPUTING



We are still in the early stages of development of quantum computers.

Lots of investment in development from industry and government.

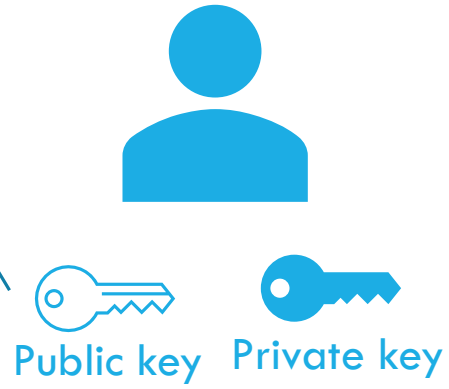
Potential to tackle complex problems far beyond the capabilities of computers today

- Machine learning
- Optimization
- Chemistry
- …
- BUT threatens current public key cryptography security.

PUBLIC KEY CRYPTOGRAPHY

Cryptographic system that uses key pair

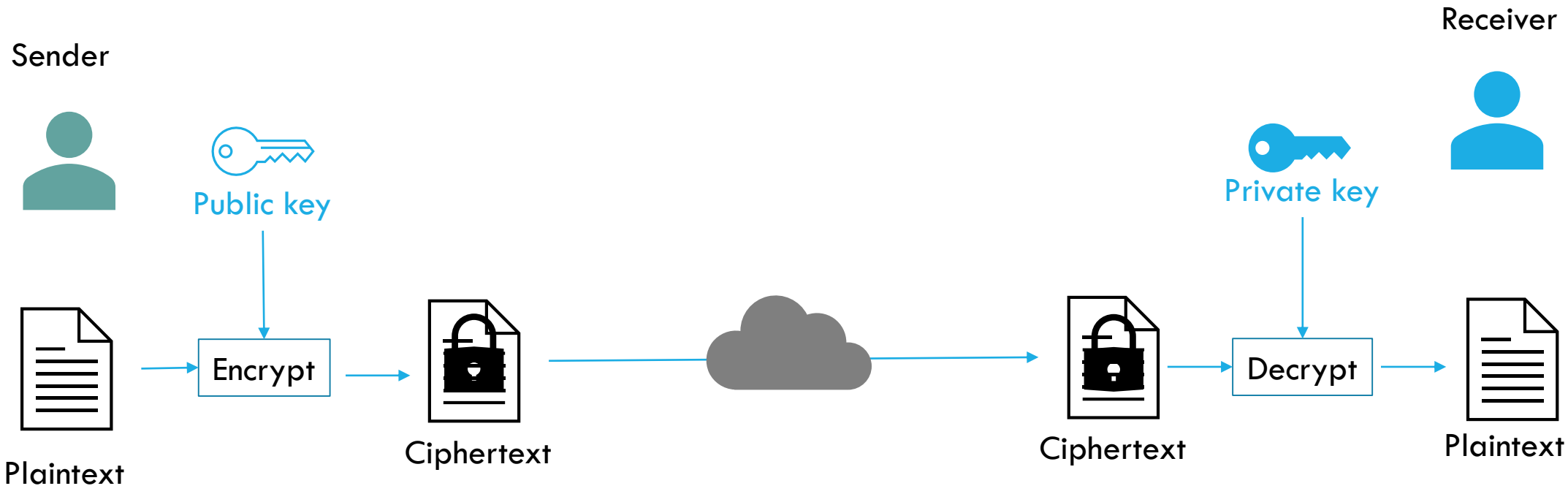
- Made publicly available
- Allows anyone to encrypt



- Kept private to owner
- Used to decrypt data (that is encrypted with corresponding public key)

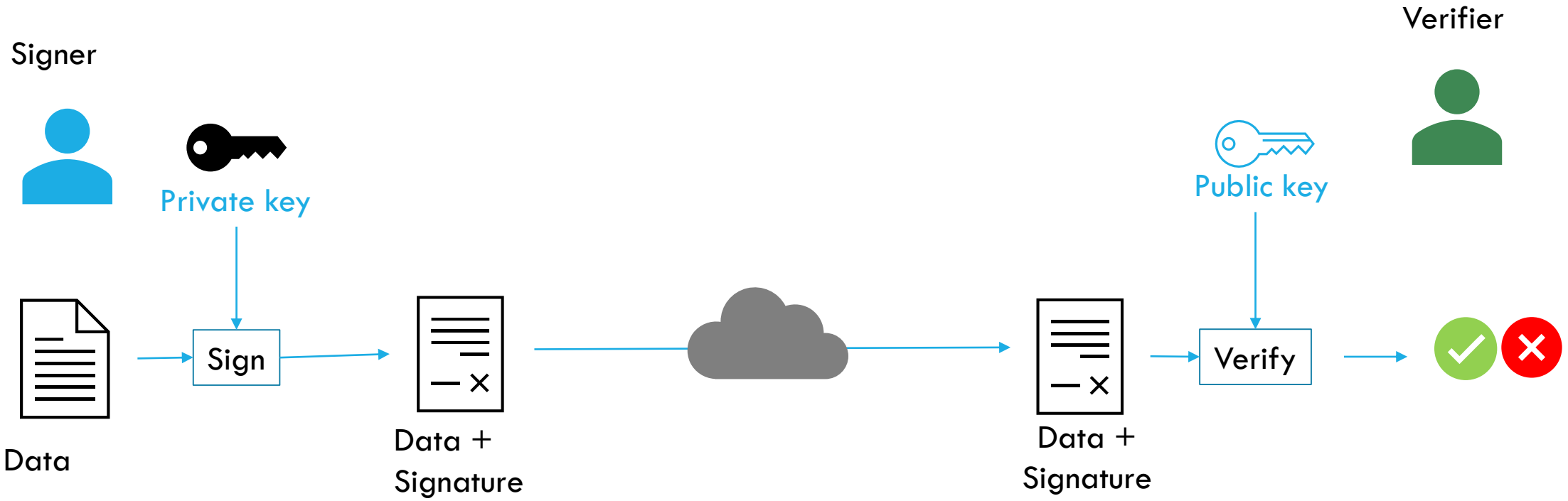
PUBLIC KEY ENCRYPTION

Ensures confidentiality of plaintext data



DIGITAL SIGNATURES

Ensures integrity and authenticity of data



PUBLIC KEY CRYPTO IS EVERYWHERE

PUBLIC KEY ALGORITHMS

The most commonly used public key cryptosystem today are

- RSA
- ECC (Elliptic Curve Cryptography)

The security of relies on the difficulty of underlying math problems

- Integer Factorization (find prime factors of large integers)
- Discrete Log Problem (finding the discrete logarithm of a point relative to another)

ie. The best known algorithms for finding solutions are **exponential** in

- Size of the Integer
- Size of the Elliptic Curve

QUANTUM THREAT – SHOR'S ALGORITHM

In 1994, Peter Shor described a theoretical polynomial-time quantum algorithm that

- Solves Integer Factorization & Discrete Logarithm Problem **exponentially faster** than classical algorithms

Current quantum computers are nowhere near large enough to carry out these attacks for the sizes of keys used by RSA, ECC

BUT if/when such large-scale quantum computers are developed, **RSA and ECC will be broken**

QUANTUM THREAT – GROVER'S ALGORITHM

For symmetric algorithms, the quantum threat is much less severe

- Ciphers, Hash, MAC, PRNG, KDF (AES, SHA-2, SHA-3, HMAC…)

In 1996, Grover described a quantum search algorithm that

- Finds input for a given output from a black-box algorithm
- Search is much 'faster' than classical computer brute-force

$O(\sqrt{N})$

$O(N)$

QUANTUM THREAT – GROVER'S ALGORITHM

Applying Grover's algorithm to symmetric algorithms theoretically reduces effective bits of security $k/2\text{-bit} \quad vs \quad k\text{-bit}$

BUT other factors suggest that Grover's algorithm would not speedup so dramatically in practice

- Quantum hardware likely more costly than classical
- Quantum computers likely to have slower clock cycle
- Grover's algorithm cannot be parallelized

Case Study: Bitcoin Mining
- Specialized hardware - ASIC
- Heavily Parallelized

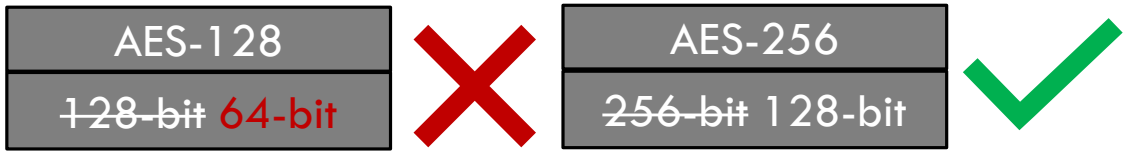
QUANTUM THREAT – OPTIMISTIC

If we take an optimistic view of future quantum technology

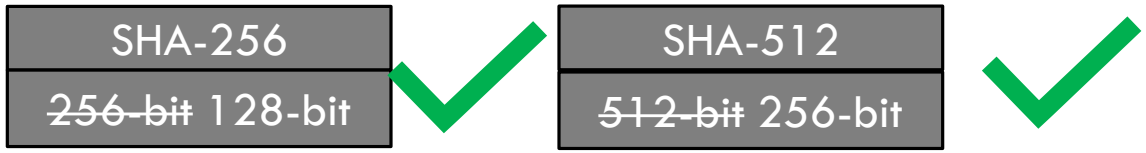
- Quantum hardware cost ≈ classical hardware cost; quantum cycles ≈ classical cycles
- Somehow parallelize attack

Current symmetric algorithms will be affected

- Block cipher security reduced from k-bits to k/2-bits



- Hash function preimage resistance from k-bits to k/2-bits



SO …

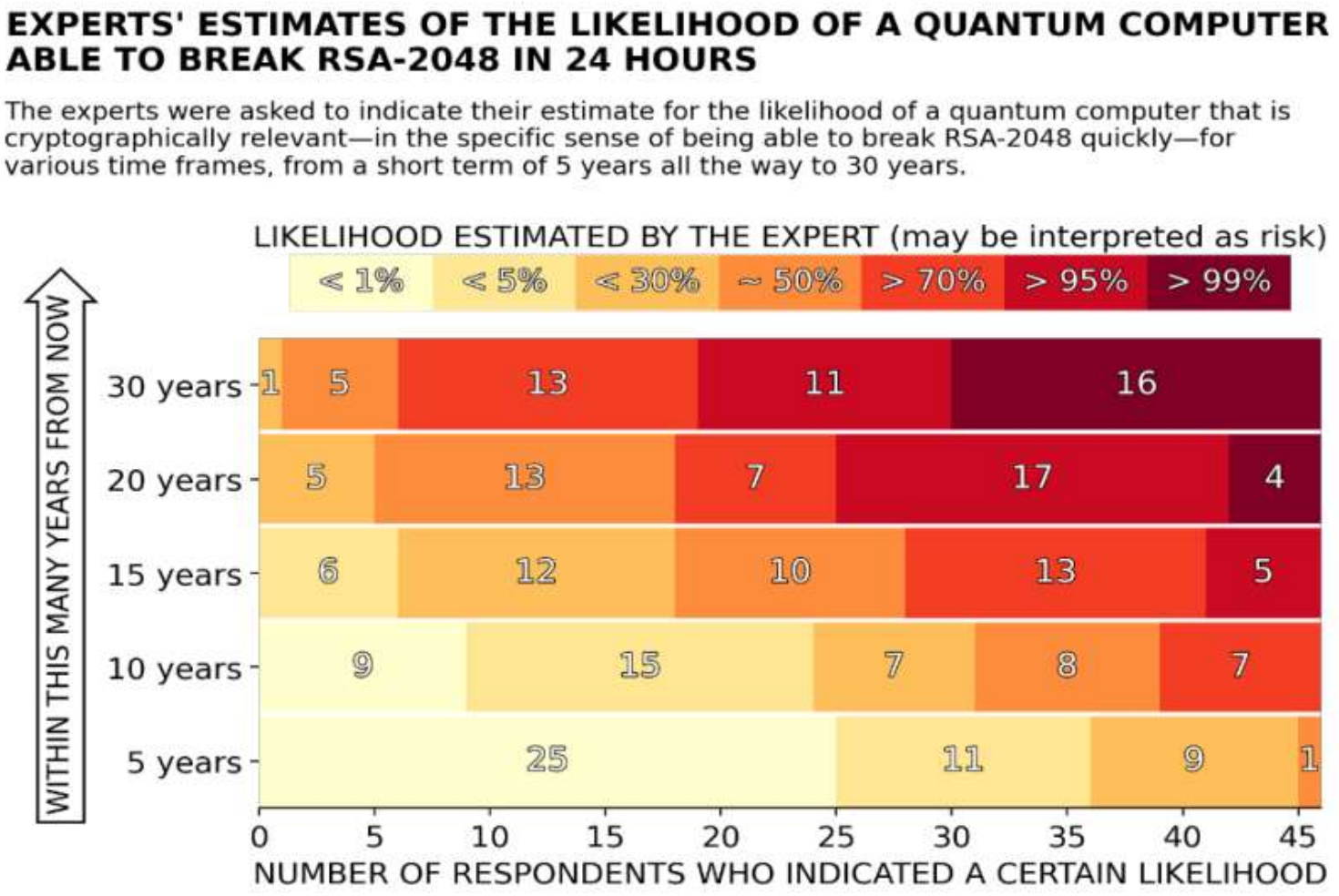
Current symmetric algorithms are considered quantum-resistant

POST QUANTUM CRYPTOGRAPHY

Current public key algorithms will be defeated by quantum computers

- We need to completely replace these vulnerable algorithms

WHEN WILL LARGE-SCALE QUANTUM COMPUTERS BE BUILT?



- Quantum Threat Timeline Report, 2021, Global Risk Institute, https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

WHY WE NEED TO ACT NOW

We need time to migrate to new quantum-resistant algorithms

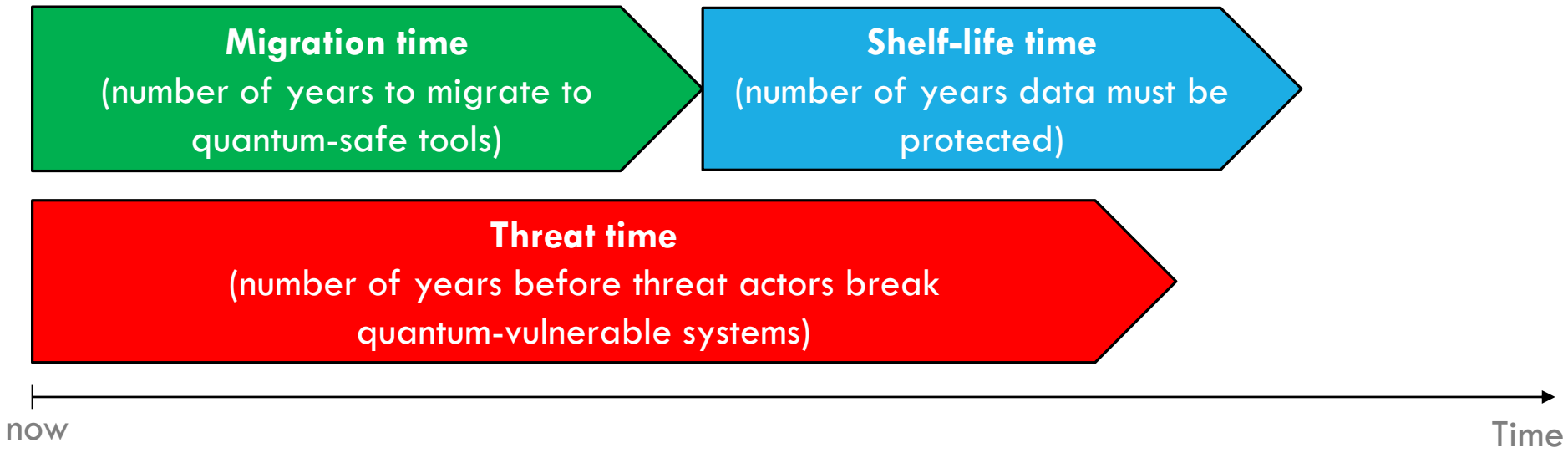
- Decide on replacement algorithms to use
- Develop new implementations and tools
- Upgrade systems to use new implementations and tools

Always takes longer than we want or expect

We need to consider store-now, decrypt-later attacks

- Powerful threat actors may be able to capture encrypted data now, to decrypt when quantum computers are developed
- Need to accommodate ‘shelf-life’ of data – ie. how long it needs to be secure

WHY WE NEED TO ACT NOW



PROBLEM **if migration time + shelf-life time > threat time**

National Institute of Standards and Technology

POST-QUANTUM CRYPTO STANDARDIZATION PROJECT

NIST began the PQC Standardization Project in 2016

NIST is a US government agency that publishes standards across a range of scientific and technology domains, including cybersecurity and cryptography

NIST Cryptography standards define the algorithms and parameters that are approved by US government to reach an acceptable level of security

- Provide guidelines for government and industry, both US and international
- Ensure interoperability between products, systems, organisations

National Institute of Standards and Technology

POST QUANTUM CRYPTO STANDARDIZATION PROJECT

Goals

- Develop public key cryptography standards that are resistant to quantum computer attack
  - Public key encryption
  - Digital signatures
- Encourage academic and industry research into new and existing quantum-resistant algorithms

National Institute of Standards and Technology

PQC PROJECT TIMELINE

2016 – Call for proposals

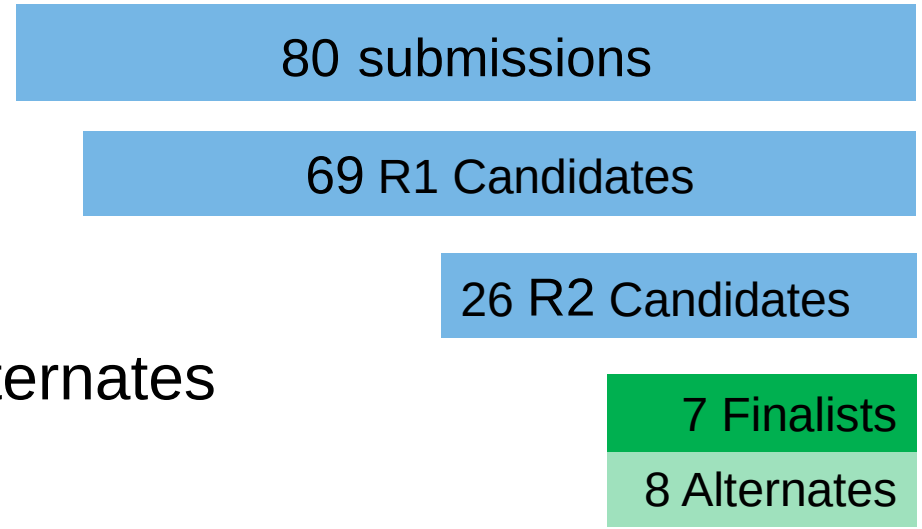
2017 – Announced 1st Round Candidates

2019 – Announced 2nd Round Candidates

2020 – Announced 3rd Round Finalists and Alternates

2022-2023 – Release Draft Standards

- *One signature scheme, one KEM from 7 finalists*



POST-QUANTUM PUBLIC KEY ALGORITHMS

Required

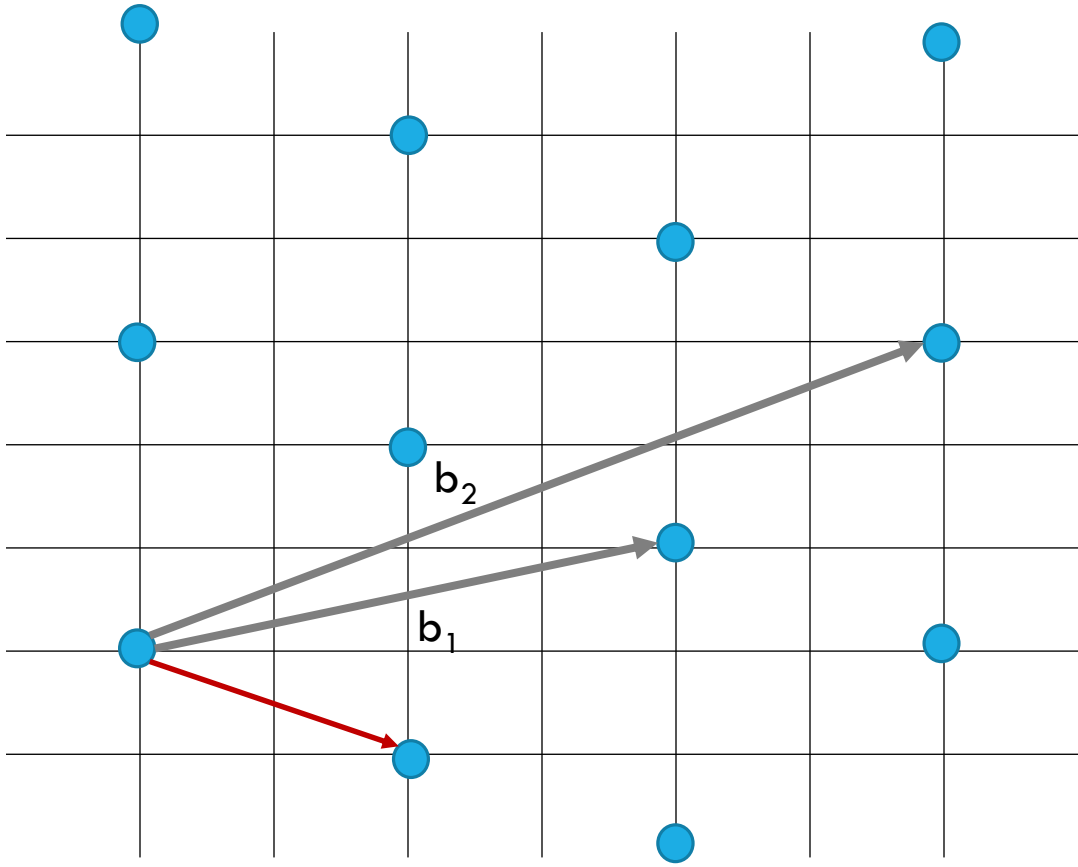
Algorithms with security based on underlying math problems that are difficult for classical and quantum computers

- Factorization-based crypto
- Discrete log-based crypto
- Lattice-based crypto
- Code-based crypto
- …

INSECURE
INSECURE

LATTICE PROBLEMS

- Lattice is a periodic grid in m dimensions over the integers
  - Defined by m basis vectors (b_1, b_2)
  - Lattice instance = all linear combinations of basis vectors
- Shortest Vector Problem (SVP)
  - Find a shortest non-zero lattice vector



LATTICE PROBLEMS

Learning with Errors (LWE): Find solution to linear equations when there is noise.

- ie. Find solution $s = (s_1, s_2, s_3, s_4)$

$$
\begin{aligned}
5s_1 + s_2 + 2s_3 + s_4 + e_1 &= 2 \pmod{13} \\
4s_1 + 7s_2 + s_3 + s_4 + e_2 &= 11 \pmod{13} \\
s_1 + 3s_2 + 2s_3 + 3s_4 + e_3 &= 3 \pmod{13} \\
s_1 + 8s_2 + s_3 + 3s_4 + e_4 &= 6 \pmod{13}
\end{aligned}
$$

"small" noise

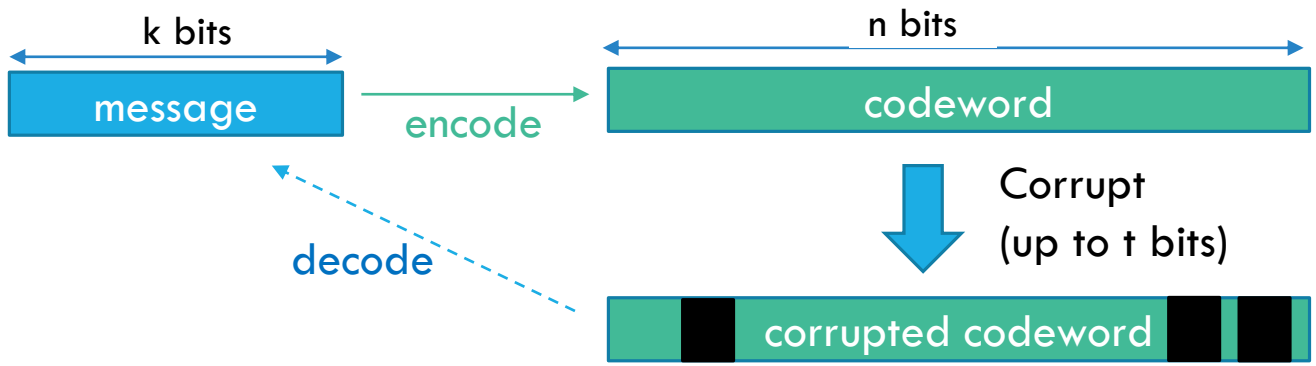
Easy to solve

Hard to solve

LWE does not use a lattice directly but can be converted into direct lattice problem

CODE-BASED PROBLEMS

- “Code”s refer to error-correcting codes / coding theory
- Coding theory goal: given corrupted codeword, find original message



- Random Goppa Decoding Problem:
  Find the original message for a corrupted codeword
  where the encode function is chosen randomly from the Goppa code family

WHY ARE THEY QUANTUM-RESISANT?

Because we don't know of any evidence otherwise

- We understand the problems quite well – decades to centuries of mathematical study
- We understand the problems to be hard on classical computers – decades of computational analysis
- Shor's algorithm (which break RSA, ECC) does not seem to apply
- No other quantum-algorithms have been discovered that are able to break them
- Lots of the world's experts are currently involved in cryptanalysis

But there are no guarantees.

Then again, there have never been guarantees about RSA, ECC on classical computers either. And they have withstood attacks for decades.

POST-QUANTUM CRYPTO EFFICIENCY

Math Problem Domain	Algorithm	Key gen (cycles)	Encrypt (cycles)	Decrypt (cycles)	Public key size (Bytes)	Ciphertext size (Bytes)
Integer Factorization	RSA	1303629853	89300	8547702	384	384
Discrete Log	ECDH	125303	135390	135390	32	32
Lattice-based	Kyber	23244	79330	93597	800	768
Lattice-based	NTRU	263590	33964	56814	930	930
Code-based	Classic McEliece	29098922	38111	120513	261120	128

Data from https://bench.cr.yp.to results: 2018 Intel Xeon E-2124; 4 x 3300MHz; r24000, supercop-20211108

CONCLUDING REMARKS

Large-scale quantum computers threaten current public key algorithms.

Although not an immediate threat, we need to work towards migrating to quantum-safe algorithms, tools and technologies.

Promising post-quantum cryptographic algorithms are available

- E.g. Lattice-based crypto
- E.g. Code-based crypto

More research required to study security, and apply to real-world applications

THANK YOU!

ANY QUESTIONS?

Interested in joining us?
Teron Labs is looking to hire future graduates.

info@teronlabs.com

Contact Me:
Jaimee Brown
jaimee@teronlabs.com

Contact Us:
www.teronlabs.com
Teron Labs | LinkedIn