Cybersecurity Goes Quantum

José Simão, ISEL/IPL

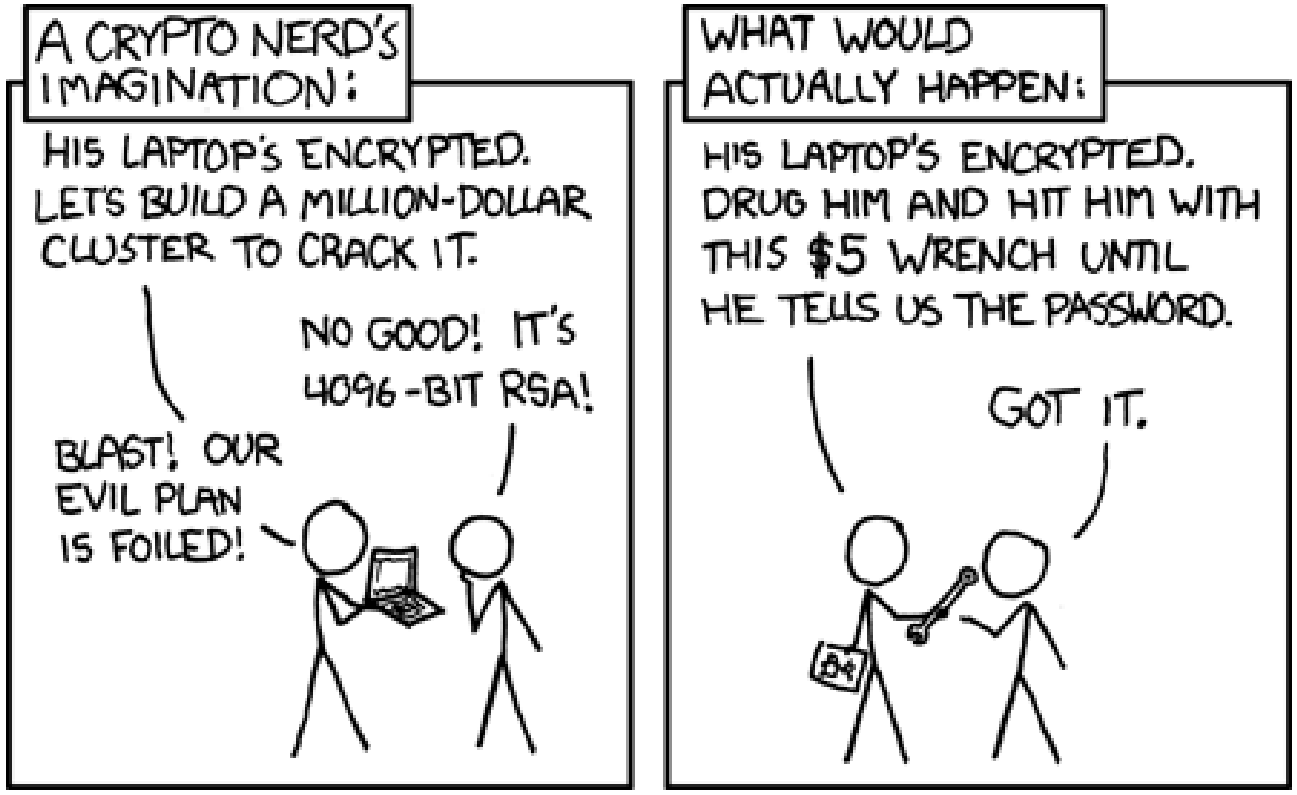
PTQCI Summer School Quantum Communication & Space
September 11-12, Lisbon

Summary

- Cybersecurity 101
- Protecting data with cryptography
- Classic and quantum threats to cryptography
- Solutions

Cybersecurity 101

- People
  - Training and awareness
  - Security culture
- Technology
  - Hardware and software solutions
  - Continuous updates and patches
- Processes
  - Security policies and procedures
  - Incident response plans
- Regulation
  - Compliance with laws and standards
  - Data protection regulations



https://xkcd.com/538/

Cybersecurity 101 – CIA triad

- Confidentiality
  - Protects sensitive information
  - Ensures authorized access only
- Integrity
  - Maintains data accuracy and consistency
  - Prevents unauthorized modifications
- Availability
  - Ensures timely access to resources
  - Maintains system reliability

Breaking CIA - Types of attacks

- **Passive attacks**: Listen to network traffic or system activities to gather information, without interrupting or modifying communication

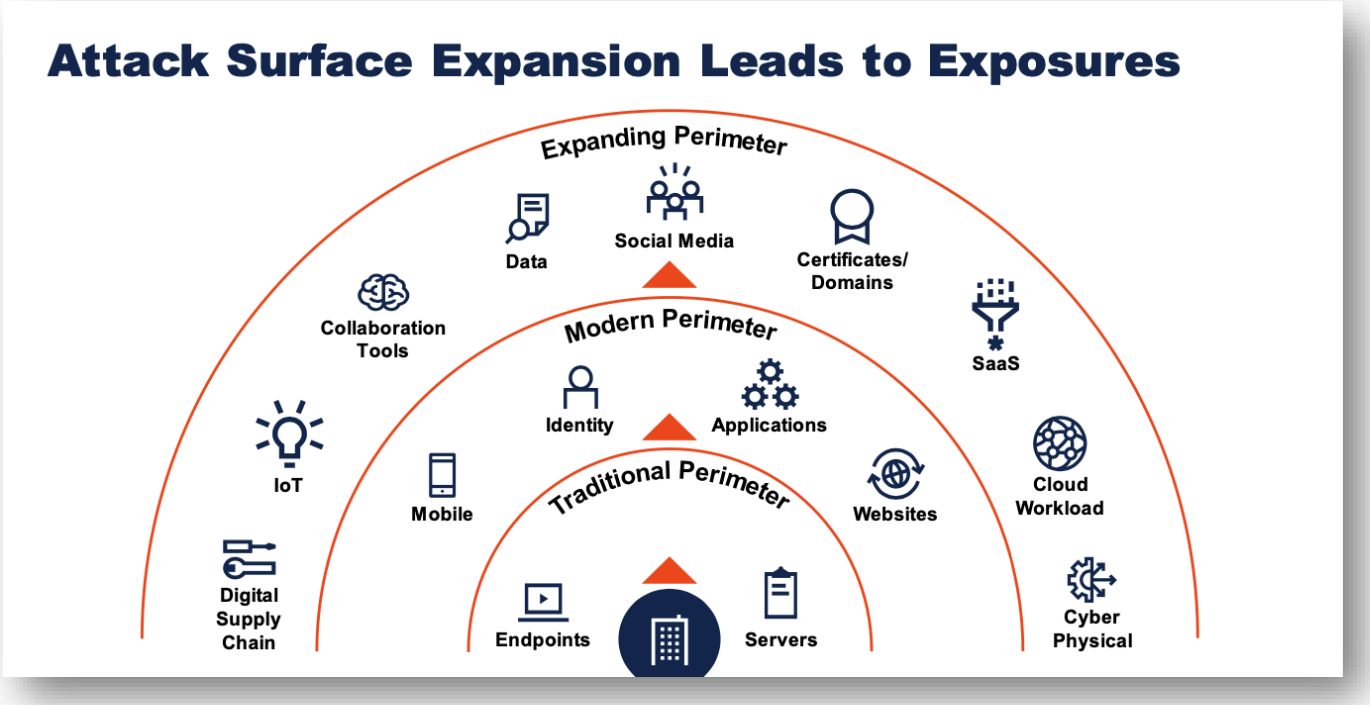
- **Active attacks**: Aim to interrupt, modify or destroy data or systems. For example, denial-of-service (DoS) attacks and man-in-the-middle (MitM)

- **Distributed attacks**: Involve multiple computers or devices working together to carry out an attack. Distributed attacks can be passive or active, and often use botnets (networks of compromised devices)

Attack surface

- The interface through which a system can be compromised

- Technical attacks
  - Network
  - Application server, runtimes
  - Operating system
  - Hardware
- Social engineering attacks
  - Users
  - Staff



Emerging Cybersecurity Market Trends and Growth Opportunities, Gartner, June 2023

Mechanisms to keep CIA properties

- Confidentiality
  - Symmetric Encryption (e.g., AES, DES)
  - Asymmetric Encryption (e.g., RSA, ECC)
  - Key Management Systems
- Integrity
  - Hash Functions (e.g., SHA-256, MD5)
  - Digital Signatures
  - Message Authentication Codes (MACs)
- Availability
  - Redundancy and regular backups encryption, Distributed Systems
  - Access Control Mechanisms

	Symmetric	Asymmetric
Confidentiality	**Symmetric Cipher**	**Assymetric Cipher**
Authenticity (integrity of origin)	**MAC**	**Digital Signatures**

ENISA – Threat landscape 2023

European Union Agency for Cybersecurity

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

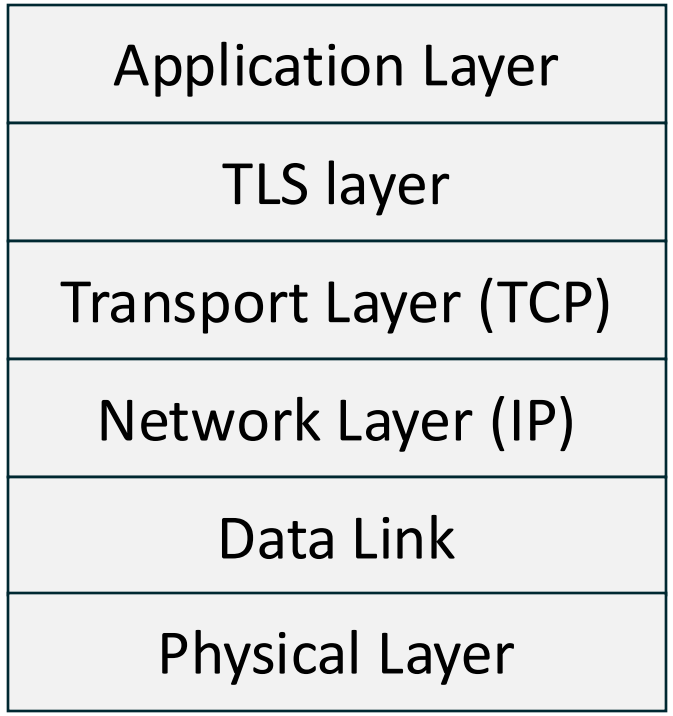
Threats Againts Data

- Threats against data: **data breach** or **data leak**
- **Data breach** is an intentional cyber-attack brought by a cybercriminal with the goal of gaining unauthorised access and release sensitive, confidential or protected data
- **Data leak** is an event (e.g. misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data

Protecting Data in Transit

- At rest, data can be protected by cryptography or access controls
- In transit, data is protected using cryptographic protocols
- Transport Layer Secure (TLS) used in everyday Web communications
  - Since 1999, current version 1.3, inherits some elements from SSL v3.0
  - Confidentiality: Only the endpoints can see the content of the transmitted data
  - Integrity: Any changes made to the data during transmission can be detected
  - Authentication: At least one endpoint on the channel needs to be authenticated

Transport Layer Security

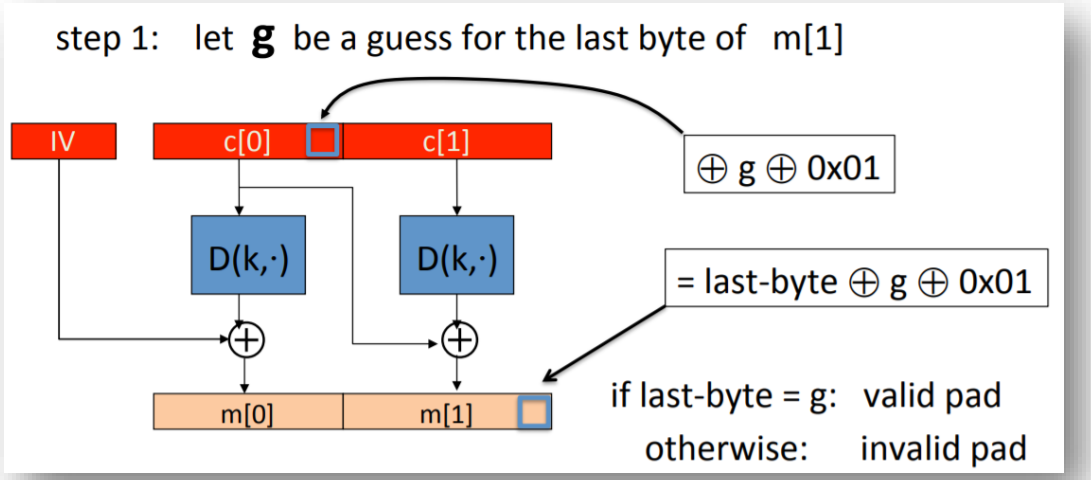


- Two main sub-protocols: **Handshake** and **Record**
- **Handshake -** a combination of asymmetric and symmetric cryptographic mechanisms to *ensure the exchange of a secret*
- **Record** - symmetric mechanisms *based on the shared secret*

TLS attacks

- TLS is currently safe
- There are however many known attacks based on certain implementations or configurations
- The Heartbleed Bug

- Padding Oracle



https://xianmu.github.io/posts/2018-11-30-padding-oracle-attack.html
https://www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf

Perfect Forward Secrecy

- Key exchange with RSA relies on the browser to use the server's public key to encrypt the pre-master secret
- This process is, currently, secure and guarantees confidentiality of the pre-master secret

- What happens if the private key is compromised?

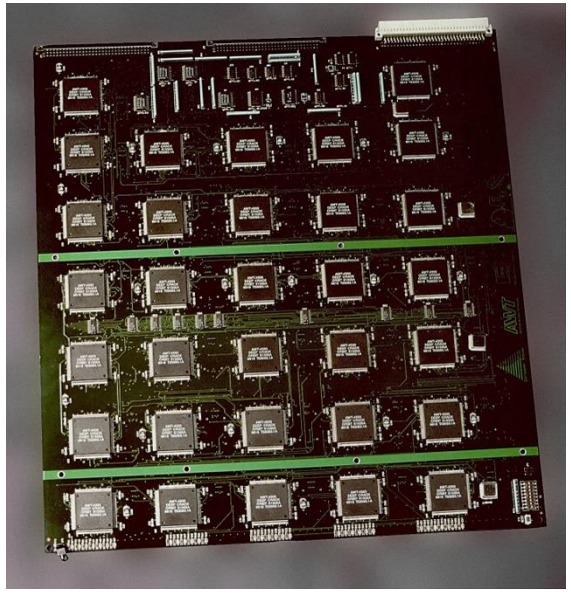
  - The attacker can decrypt the pre-master secret and then the messages in previously saved frames of the Record Protocol (✗ PFS)
  - Current TLS 1.3 removes some RSA support and only shares keys with perfect forward secrecy algorithms, such as Elliptic Curve (EC) Diffie-Hellman (✓ PFS)

Other exemples of use of RSA and EC

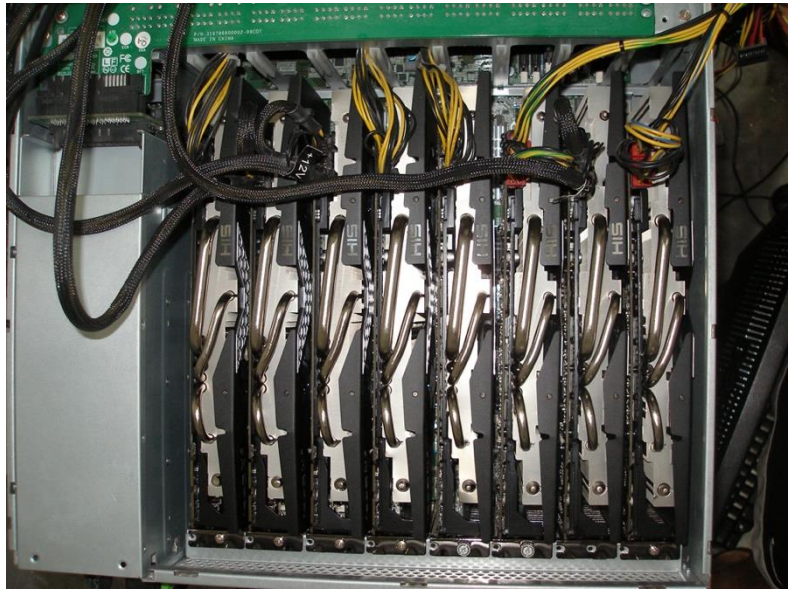
- Certifications X.509 of Public Key Infrastructure
- Secure Software Distribution
- Federate Authorization
- Secure Email (S/MIME)
- Virtual Private Network (IPSec)

Current threat: The Classic Computer

- Computers can break some cryptographic mechanisms



"Deep Crack" chips to break DES in 1998

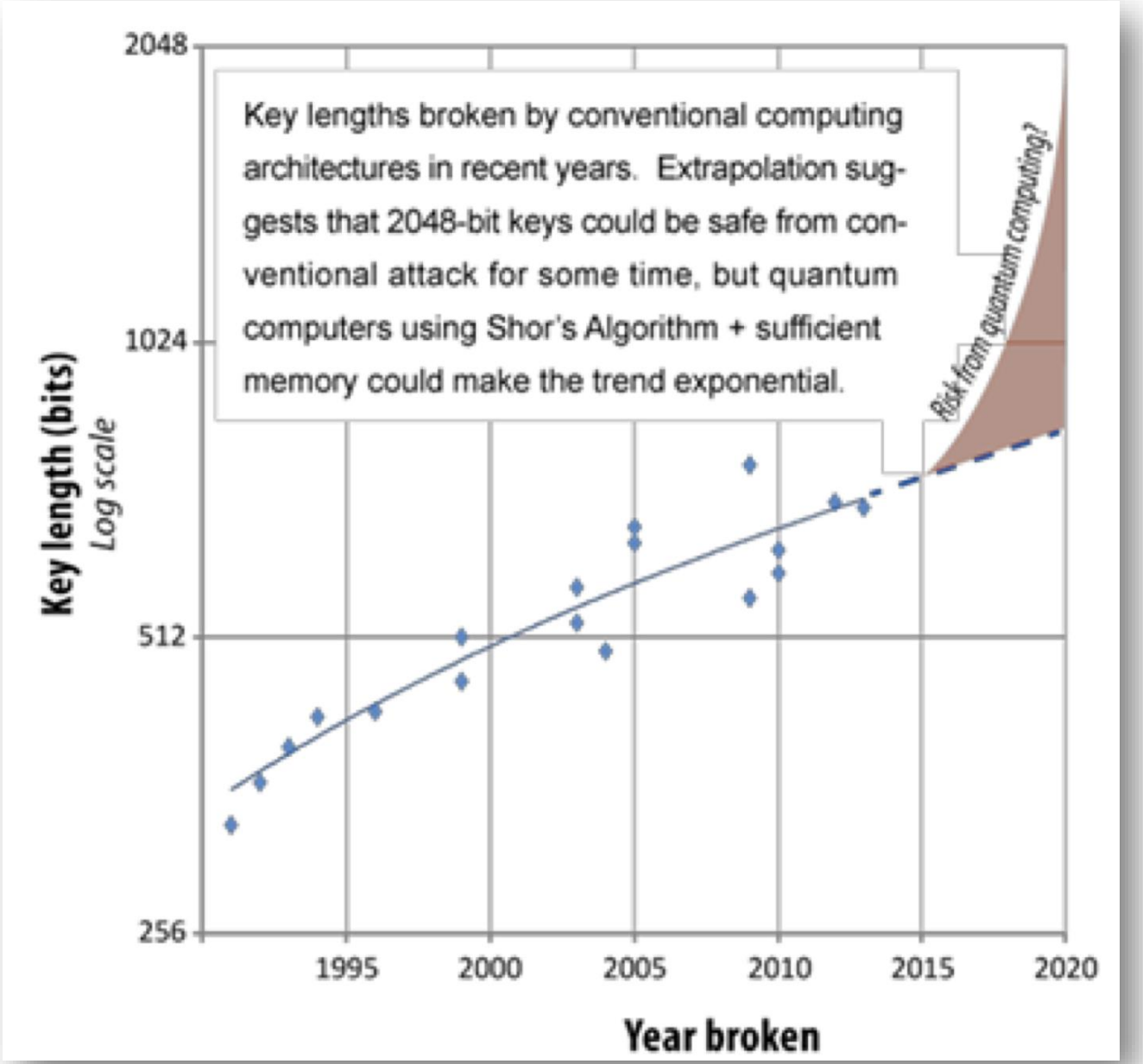


GPU are good to find collision in older hash functions

Breaks of RSA by key size

Breaks of the RSA cryptosystem in recent year using conventional computation

Adapted from ETSI "Quantum Safe Cryptography and Security"



Future threat: The Quantum Computer

- Y: “how many years it will take us to make our IT infrastructure quantum-safe”
- X: “how many years we need our encryption to be secure”
- Z: “how many years before a large-scale quantum computer will be built”
- When X+Y > Z, classic crypto will not be secure to use

M. Mosca (2013), “Setting the Scene for the ETSI Quantum-safe Cryptography Workshop”, https://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf

Quantum algorithms

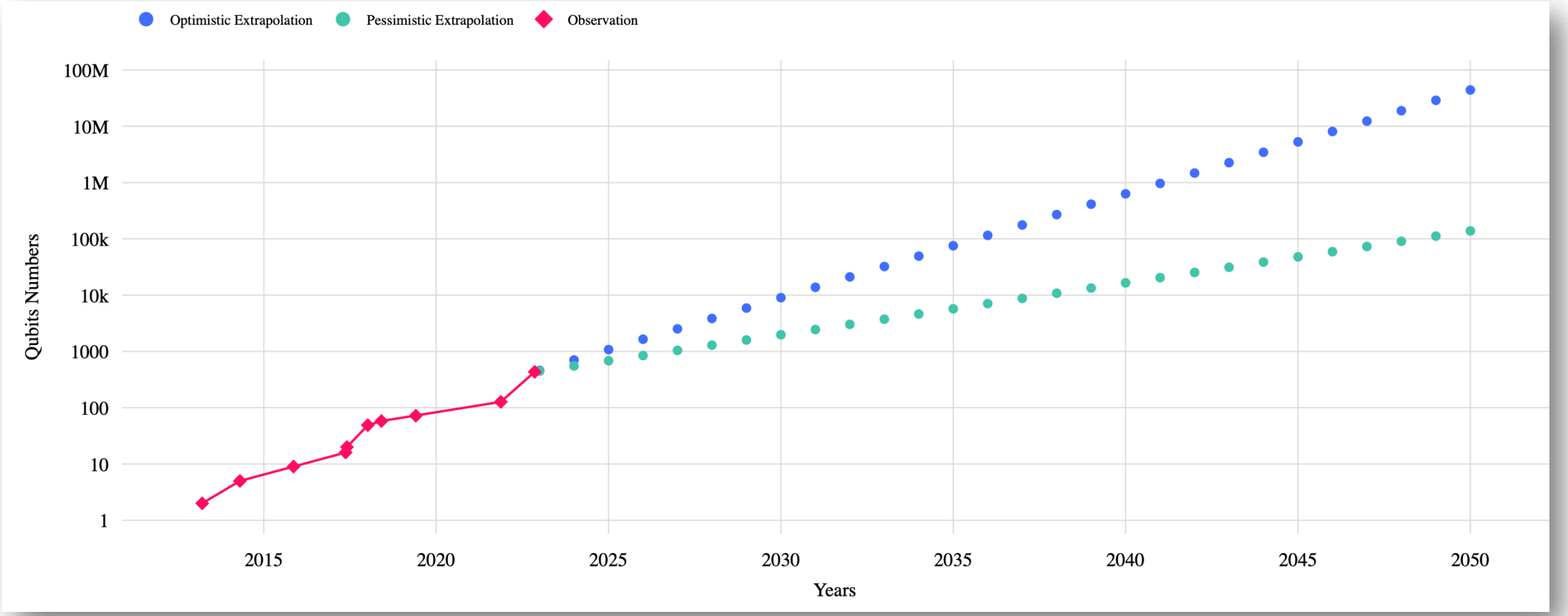
- Quantum algorithms have the potential to break current crypto (find keys faster)
  - Quantum computer use properties of superposition and entanglement
- Grover's Algorithm (https://arxiv.org/pdf/quant-ph/9605043)
  - Faster search algorithm for unsorted data
  - E.g. In AES 128, a brute force would need $\sqrt{2^{128}}$ or 2^{64} calculation instead of $\frac{2^{128}}{2}$ or 2^{127}
- Shor's Algorithm (https://arxiv.org/abs/quant-ph/9508027)
  - Can break asymmetric algorithms (RSA, DH, ECC)
  - Solves the underlying hard-problems – factoring prime numbers, discrete logarithm – exponentially faster than best known classic algorithm

Breaking RSA and ECC

- Currently 3072 bits are considered safe for RSA
- If Quantum key attack capabilities double every two years...
- ... Conventional computing becomes 8x slower and 2x more space, quickly outpacing Moore's Law and requiring impractical bandwidth.

- ECC break can occur sooner than RSA
  - Microsoft Research: ~2500 qubits could break P-256 (EC signature with 256 bits) [https://doi.org/10.1007/978-3-319-70697-9_9]
  - RSA with 2048 bits is expected to require ~14500 qubits, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits"[https://quantum-journal.org/papers/q-2021-04-15-433/]

Qubits, past, present and beyond



BTQ Technologies Corp, https://qbyte.btq.com


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

News about Quantum Computing

Technology

Google breakthrough paves way for large-scale quantum computers

Google has built a quantum computer that makes fewer errors as it is scaled up, and this may pave the way for machines that could solve useful real-world problems for the first time

By Matthew Sparkes

5 September 2024

Computing

Radical quantum computing theory could lead to more powerful machines than previously imagined

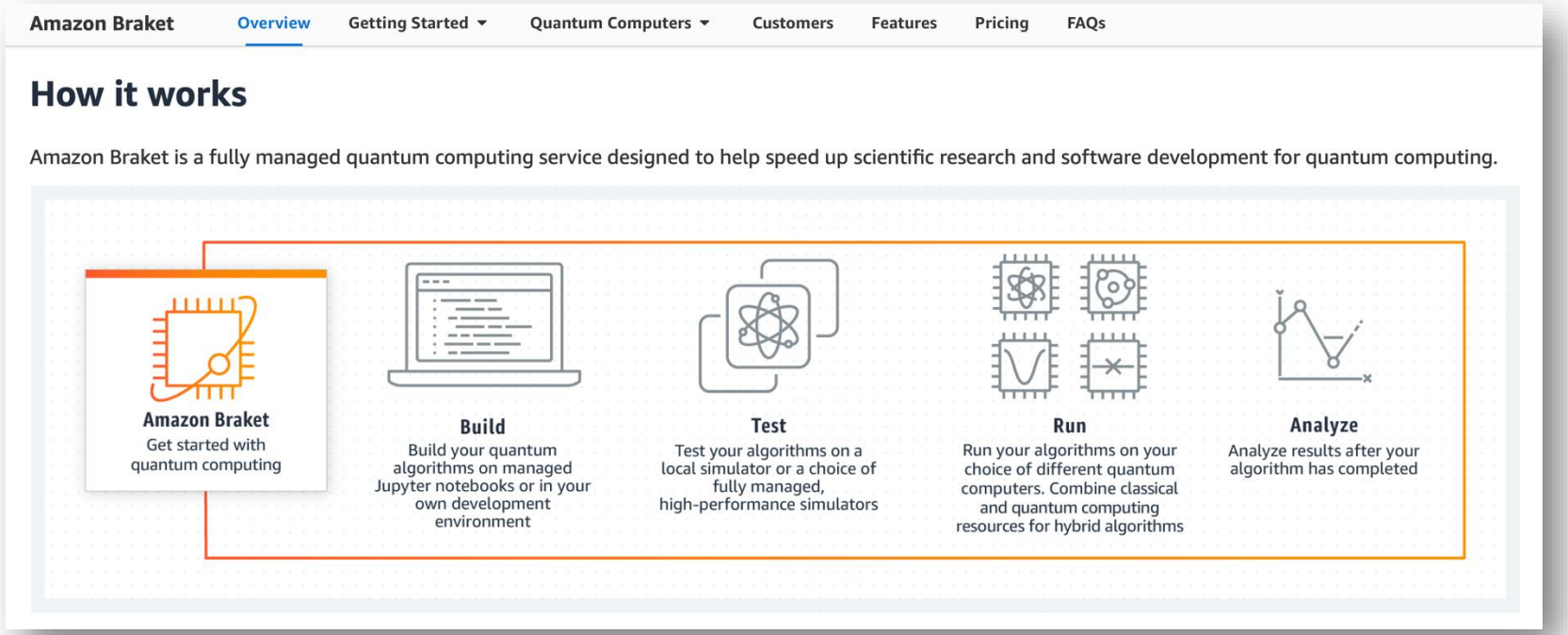
News By Keumars Afifi-Sabet published September 5, 2024

Scientists have just theorized how to connect quantum processors over vast distances to form a giant quantum computing network that acts as a single machine.

Microsoft announces the best performing logical qubits on record and will provide priority access to reliable quantum hardware in Azure Quantum

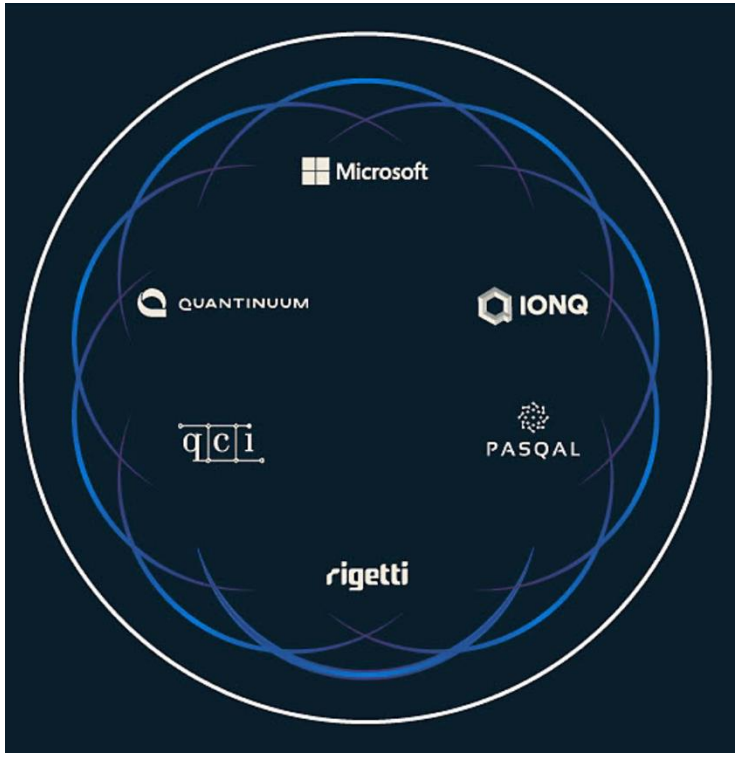
Sep 10, 2024 | Jason Zander - EVP, Strategic Missions and Technologies

Quantum Computing in the Cloud



Amazon Web Services - AWS

Microsoft Azure



Mitigations to the threats

- Current public key solutions to key exchange could be broken by a quantum computer

- Solutions:

  - Quantum Key Distribution (QKD)
    - Ensures PFS guaranteed by the laws of physics

  - Quantum resistant (Post-quantum) Cryptography
    - Aims to ensure PFS using new mathematical tecnhiques

Mitigation to the threat - QKD

- Quantum Key Distribution to sync secret key on client and server

  - Symmetric key exchange guaranteed to be secure by Quantum physics
  - Quantum systems such as polarized photons to transmit key information
  - Any disturbance of the photons during transmission can be detected
  - Quantum transmission + public (auth.) discussion → shared symmetric keys!

  ➢ QKD keys + One Time Pad encryption - *ideal* scenario for perfect secrecy

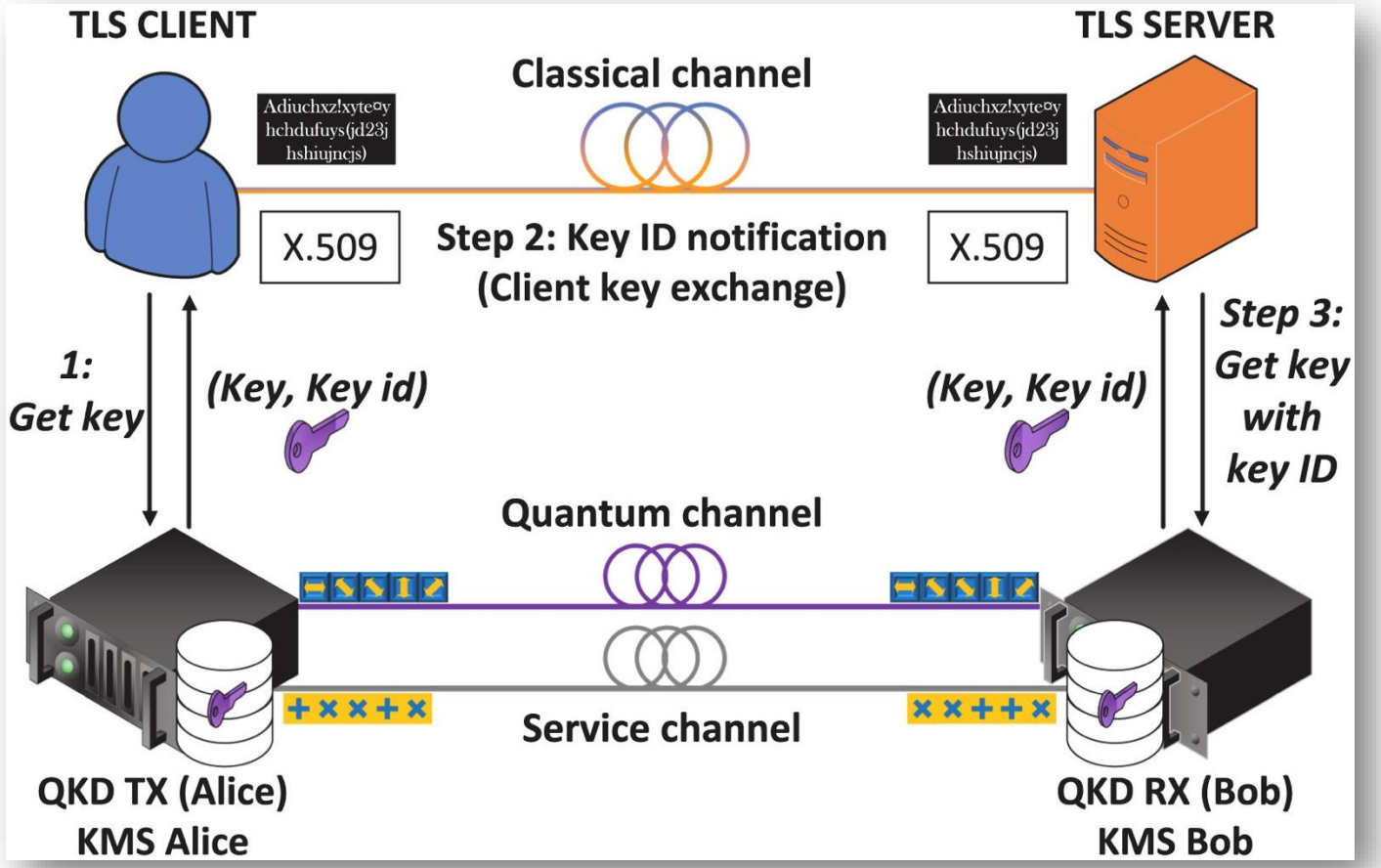
  ➢ QKD keys + AES-256 encryption - *practical* scenario for computational security

  - Ongoing standardization work (ETSI, ISO, and others)

Implementation

- Continuous or Discrete variable based on the chosen physical systems
- Free-space or fibre optics-based channel
- Trusted or untrusted intermediate nodes configurations
- Various lab and field tests; satellite-QKD demonstrations!
- Commercial solutions providing:
  - Easy plug-and-play usage and integration in the existing network infrastructure
  - Key distribution for up to 350 km
  - Secret key rates ~Mbps (Kbps) for shorter (longer) distances
- Side-channel attacks targeting different points of vulnerabilities

QKD and TLS – Architecture overview



ETSI QKD 014

Quantum-resistant Transport Layer Security, Carlos et al. (2024), https://doi.org/10.1016/j.comcom.2023.11.010

Mitigation to the threat - PQC

- Quantum resistant (*post-quantum*) public key algorithms
  - Since 2016 NIST is organizing the selection of post-quantum algorithms
  - In August'24 NIST release standards for **key agreement** and **digital signatures**
  - For key agreement NIST chose "Kyber" (https://csrc.nist.gov/pubs/fips/203/final, https://openquantumsafe.org/liboqs/algorithms/kem/kyber.html)

		Size (bytes)		Ops/sec (higher is better)		
Algorithm	PQ	**Public key**	**Ciphertext**	**Encaps**	**Decaps**	**Keygen**
Kyber512	✅	800	768	80,000	100,000	125,000
RSA-2048	❌	256	256	150,000	1,400	30

- Larger key sizes ⚠
- Faster key generation ✓
- Faster Decryption ✓
- Slower Encryption ⚠

https://blog.cloudflare.com/nist-post-quantum-surprise/

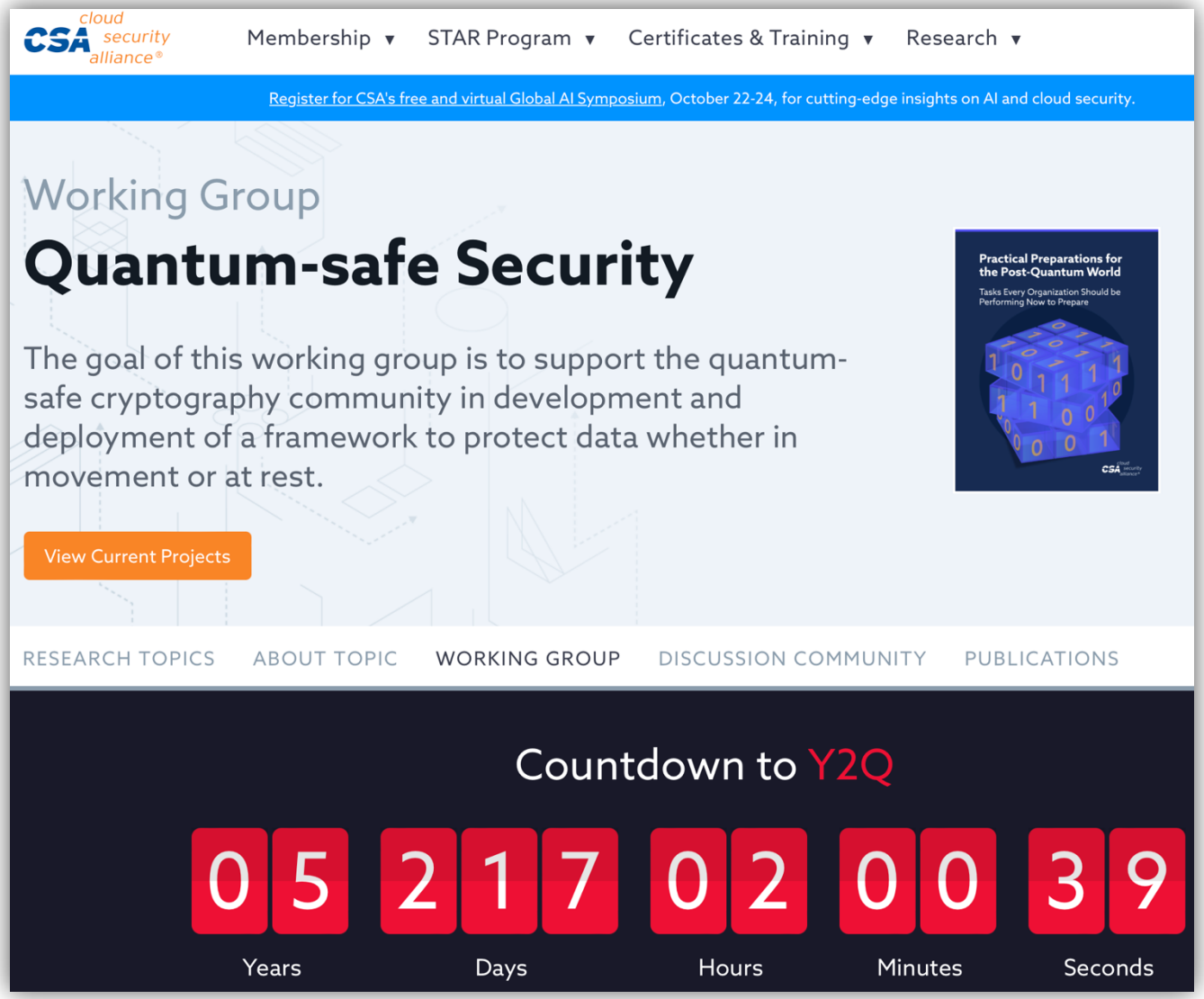
NIST PQC Security Levels

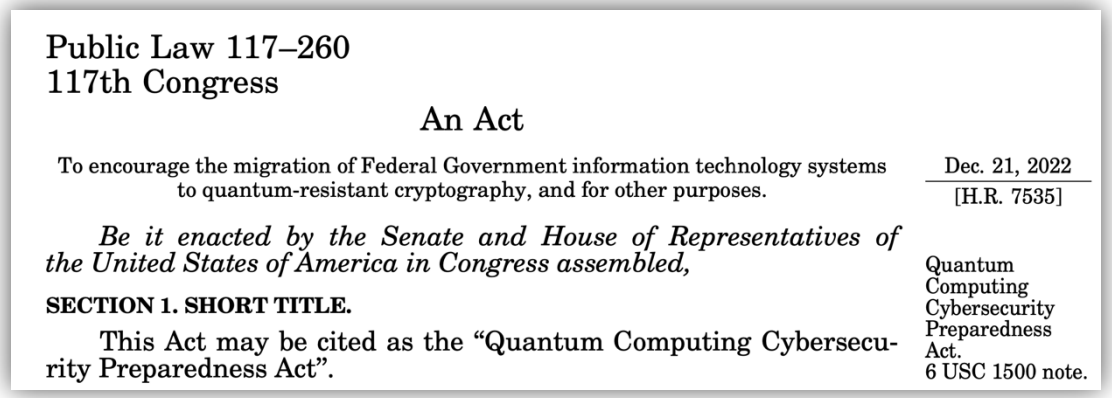
- NIST defines security categories based on the resistance of symmetric cryptography to quantum attacks
- Lower security levels (1-2) correspond to attacks requiring resources like breaking AES128 (128-bit key) or SHA256 (256-bit hash)
- Higher levels (3-5) correspond to resources required for breaking AES192, SHA384, and AES256
- Kyber_512 is as hard to break as AES-128, Kyber_768 -> AES-192, and Kyber_1024 -> AES-256

Implementation

- The Open Quantum Safe (OQS) project is an open-source project that aims to support the transition to quantum-resistant cryptography
- `liboqs` provides:
  - a collection of open-source implementations of quantum-safe key encapsulation mechanism (KEM) and digital signature algorithms
  - a common API for these algorithms
  - a test harness and benchmarking routines
- `liboqs` integrates into protocols like TLS, X.509, and S/MIME, through an OpenSSL 3 Provider

The wheels are in motion





A multi-stage strategy

Cloud Security Alliance - Practical Preparations for the Post-Quantum World

1. Recognize the challenges and get support for a post-quantum project
2. Form a post-quantum project and team, create a timeline, and plan
3. What data is at risk and if it needs to be protected with additional post-quantum mitigations
4. Select the appropriate mitigations for those needing additional protection
5. Apply policy changes and technical mitigations

Comparison

	Pros	Cons
PQC	• Easier to integrate in the existing infrastructure • Authentication scalability • Mature standardization	• Conjectured (temporary) security
QKD	• Proven (long-term) security	• Classical crypto based authentication • Less mature standardization • High hardware cost • Distance limtation

It is important to clarify that the choice between QKD and PQC is not binary. The integration of QKD with PQC can offer a hybrid solution that builds on the strengths of both technologies

——In February 2024 , the British Regulatory Horizons Coumcil (RHC) released the *Regulating Quantum Technology Applications*

Thank you

José Simão

jose.simao@isel.pt

https://jsimaoisel.github.io