THALES
Building a future we can all trust

The Quantum Threat

and its impact on Hardware Security Modules

Eric Amador
Luna HSM product manager
February 2024

HSMs protecting traditional and emerging use cases

Emerging

Protect blockchains and **crypto assets / cbdc**

Secure **5G** privacy and authentication

Create secure digital identities for **IoT** and **secure manufacturing**

Traditional

Code and document **digital signatures**

Secure **PKI** root keys

Protect **Database** encryption keys and **application** keys

Key Management Systems root of trust in the cloud and on premise

THALES

How an HSM can help - What is an HSM and Why is it Important?

- Keys secured in physical **tamper resistant** hardware
- Private **keys cannot be extracted**
- **Certified Cryptography Mechanisms** performed in a secure environment
- Keys generated with high quality **hardware entropy**
- **Crypto agility**, continuous updates to mitigate new risks (Quantum Threat)
- **Independent certification** such as FIPS 140-2 / FIPS 140-3 and Common Criteria EAL4+

THALES

The quantum computing race is on






Microsoft

Google

rigetti

IBM

IONQ

D:wave
The Quantum Computing Company™

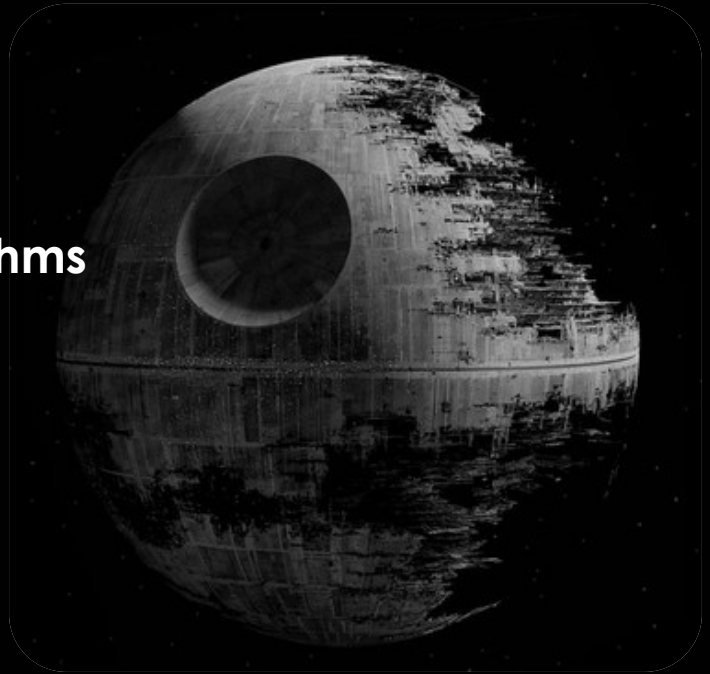
TOSHIBA
Leading Innovation

intel

Honeywell

THALES

A new threat in the IT galaxy



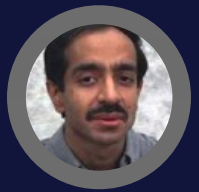
- **Quantum computing puts cryptographic algorithms at risk.**
  - ➢ especially public-key cryptography

How a quantum computer impacts cryptography

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	**No longer secure**
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	**Longer keys needed**
SHA-2, SHA-3	----------	Hash functions	**Larger output needed**

Peter SHOR



Lov GROVER

THALES

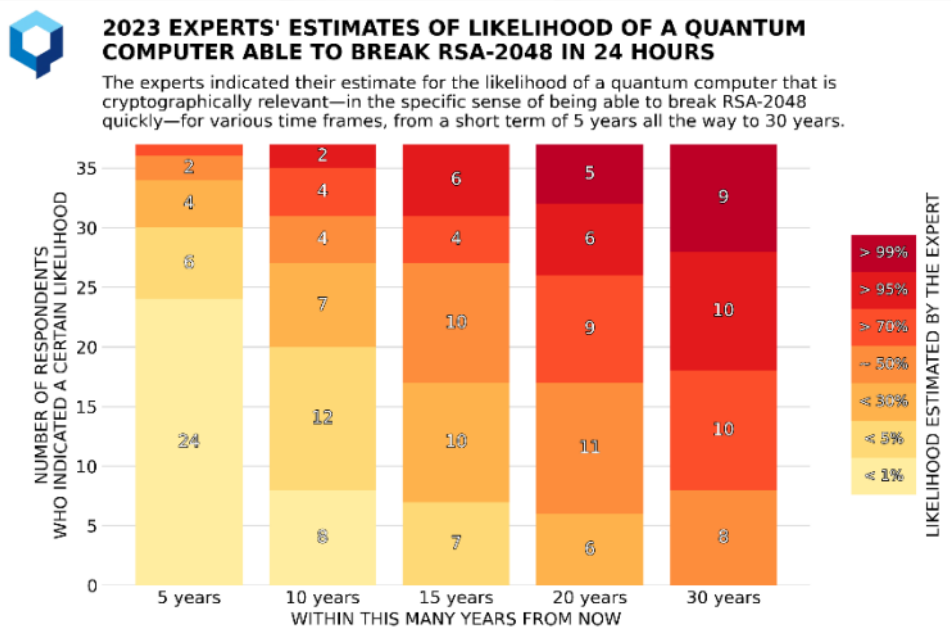
Beyond algorithms, threat impacts

OVERALL ECOSYSTEM

- **Communication protocols**
  (TLS, IPSec, SSH, …)
- **Certificates** (X.509)
  (Identities, Code Signing, Doc Signing)
- **Key management protocols**

15 to 20 years away to break current asymmetric cryptography?

LIKELIHOOD ESTIMATED BY THE EXPERT (may be interpreted as risk)



The experts indicated their estimate for the likelihood of a quantum computer that is cryptographically relevant - in the specific sense of being able to break RSA-2048 quickly - for various time frames, from a short term of 5 years all the way to 30 years.

Authors

Dr. Michele Mosca

Co-Founder & CEO, evolutionQ Inc.

Dr. Marco Piani

Senior Research Analyst, evolutionQ Inc.

GLOBAL RISK INSTITUTE evolution

DECEMBER 2023

D date still **UNCERTAIN**

THALES

Mosca's Theorem – store now,decrypt later – data at risk

"According to Michele Mosca's Theorem (X+Y)>Z, if the amount of time that data must remain secure (X) plus the time it takes to upgrade cryptographic systems (Y) is greater than when quantum computers come online with enough power to break cryptography (Z), you have already run out of time"

5 years to migrate to PQC

Encryption Data need to be protected 15 years

15 years to launch a capable quantum computer

Data are at risk !!!

"The experts' likelihood estimates for when a cryptographically relevant quantum computer will appear suggest that some companies might already be facing an intolerable risk requiring urgent action." Dr. M. Mosca.

THALES

Confidential Communications at risk

VPN Session

Handshake

Data Exchange

Quantum attack using Shor's algorithm

Key Establishment

Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext

THALES

Mosca's Theorem – connected/critical devices at risk

"According to Michele Mosca's Theorem (X+Y)>Z, if the amount of time the device must remain secure (X) plus the time it takes to upgrade the device with PQC (Y) is greater than when quantum computers come online with enough power to break cryptography (Z), you have already run out of time"

5 years to migrate to PQC

Device needs to be protected 15 years on the field

15 years to launch a capable quantum computer

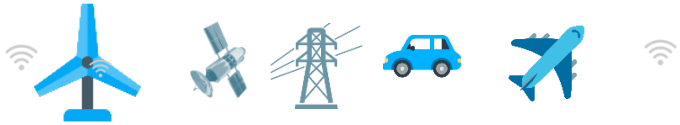
Devices are at risk !!!

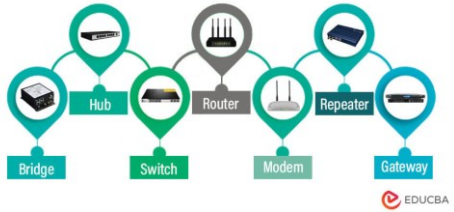
THALES

Devices at risk

What's at risk?

Durable connected devices (IoT) with **long in-field lives**





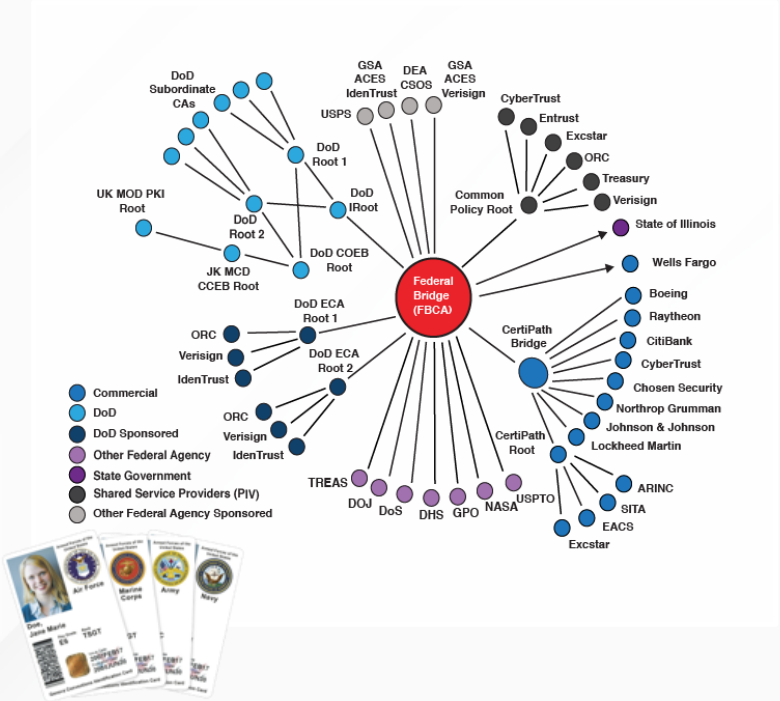
What's the attack?

Forged software updates by quantum-enabled adversaries

Code Signing → **PKI** ← **TLS**

THALES

Digital Identities at risk



There are more than
4.5 million active users
in the U.S. DoD identity management system.

Creating a quantum-safe duplicate infrastructure is time-consuming and cost prohibitive.

THALES

Guidance from agencies

NSA:

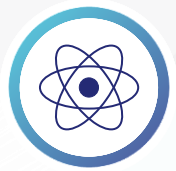
- SW/Firmware-signing: begin transition immediately
- Web browsers/servers/cloud services: support and prefer CNSA 2.0 by 2025
- Traditional networking equipment (virtual private networks, routers): support and prefer CNSA 2.0 by 2026

ANSSI: recommends introducing post-quantum defense-in-depth as soon as possible for security products aimed at offering a long-lasting protection of information

BSI: it's no longer a question of 'if' or 'when' there will be quantum computers, PQC will become the standard in the long term

THALES

Future-proof with crypto agility



Quantum is coming

Quantum capabilities are accelerating

NIST and others are finalizing quantum safe standards

PKI based crypto will become hybrid

Know your risks

Long term data is at risk, if using classic technologies

Consider that it is vulnerable to harvest now, decrypt later

Connected devices deployed on the field for a long period of time are at risks

Focus on crypto agility

Crypto Agility is the best practice; requires supporting infrastructure

Take a hybrid approach by using classic & quantum-safe crypto solutions

Stronger Together

Assess your crypto agility maturity and readiness

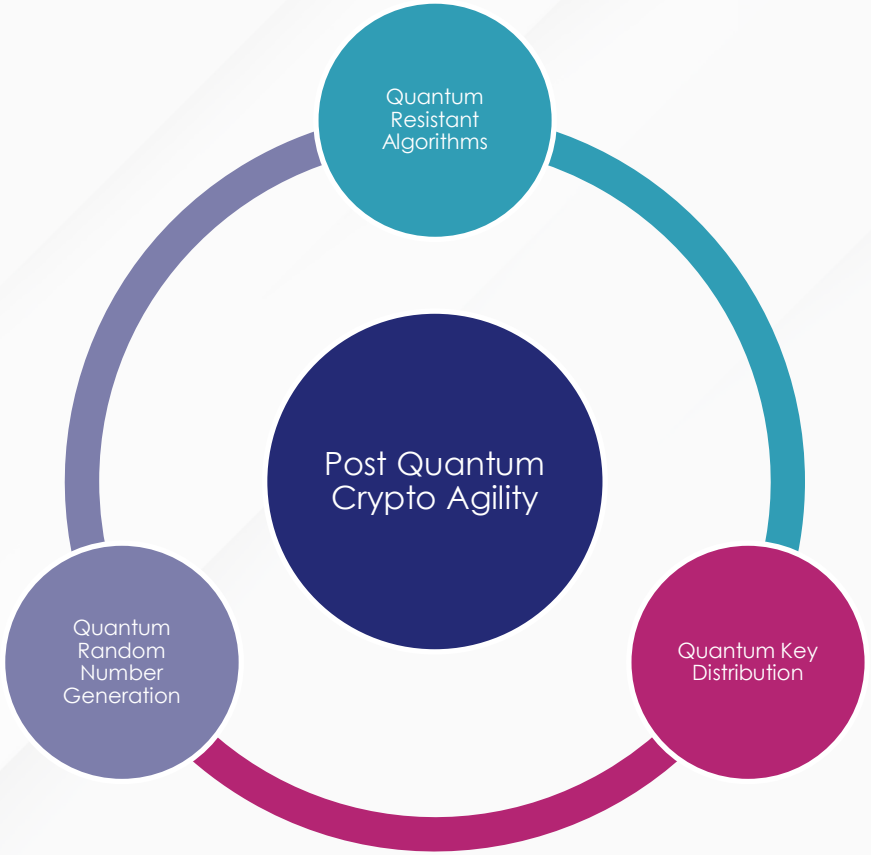
Design a quantum safe architecture

Be ready for change, even after standards are established

Evaluate solutions and partnerships in place today to support your quantum safe initiatives

THALES

Building a future-proof Quantum strategy

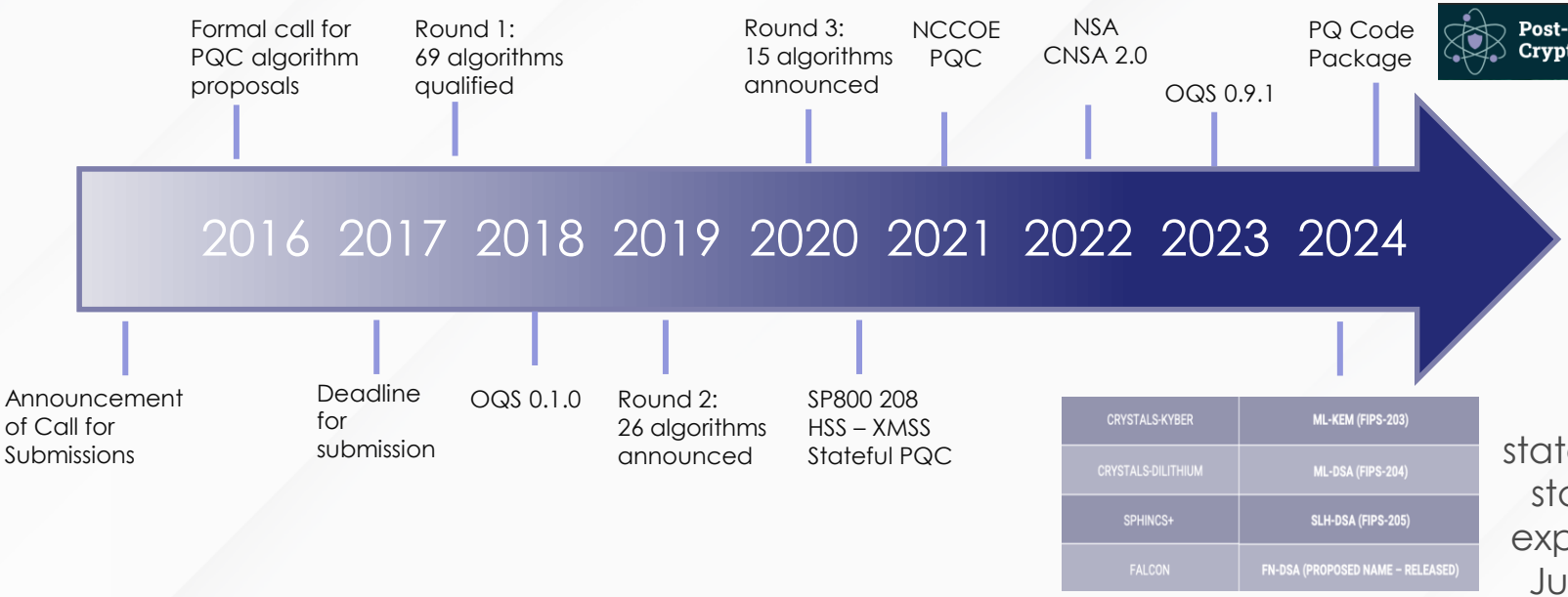


Standards

NIST
IETF
PKI Consortium
ANSI
Accredited Standards Committee X9 Inc. Financial Industry Standards
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
ETSI World Class Standards
CAB CA/BROWSER FORUM
CSA cloud security alliance®

THALES

The NIST Standardization Process and PQC implementations



First 3 stateless pqc standards expected in June **2024**

NIST finalist FALCON was sponsored and co-developed by Thales along with academic and industrial partners from France (University of Rennes 1, PQShield SAS), Switzerland (IBM), Canada (NCC Group), and the US (Brown U, Qualcomm).

THALES

Foundations of a Quantum-Safe solution

Key Management

Up to date key inventory, protect key exchanges ASAP with PQC KEM

PQC Algorithms

NIST Post Quantum Algorithms HSS, ML-DSA, ML-KEM, SHL-DSA, Classic McEliece, …

Key Generation

Enhance TRNG with QRNG (Provably Unpredictable Keys From Quantum Computers)

THALES

THALES

Thank you