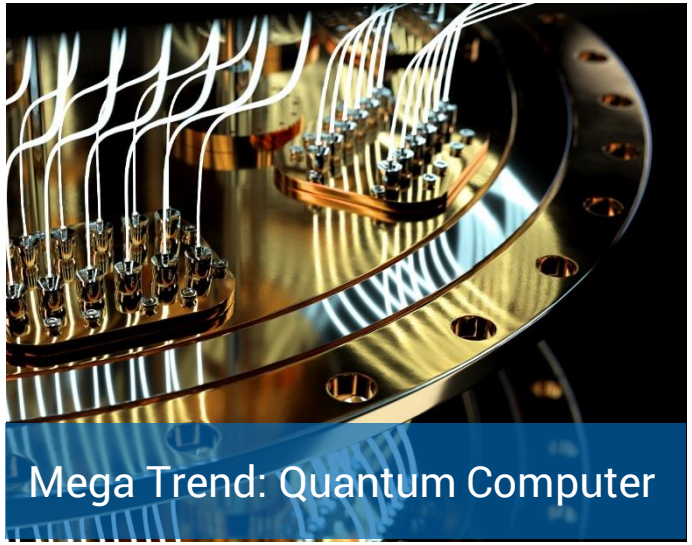
Cybersecurity and Quantum-Safe Cryptography in the Age of Quantum Computing

Dieter Bong / Chris Meyer

Creating Trust in the Digital Society

utimaco®

Agenda


Mega Trend: Quantum Computer


Problem Statement

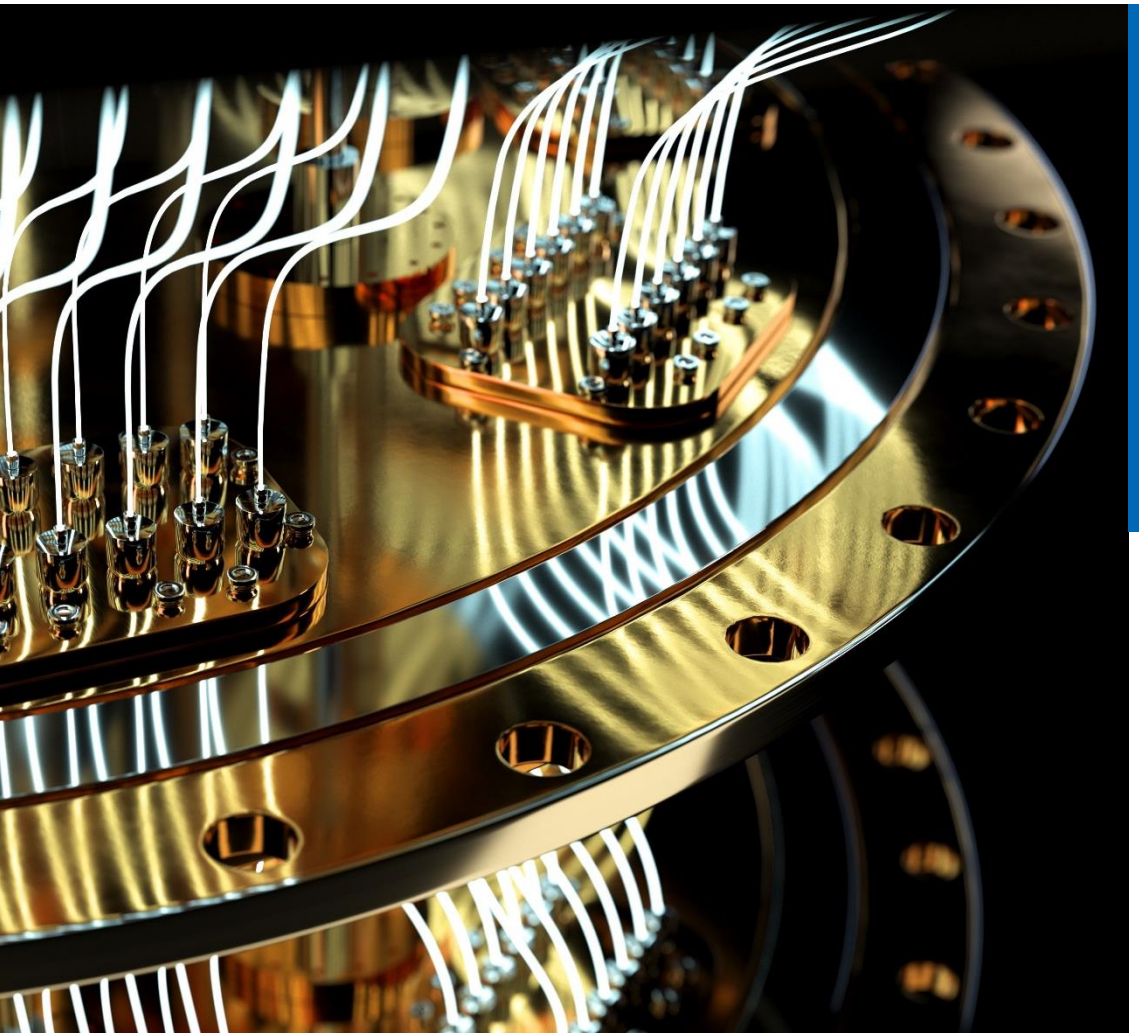

Q-safe Offering & Positioning


Q&A

Mega Trend: Quantum Computer

utimaco®

Q-safe 1.0 Launch



Quantum computers take advantage of quantum physics for solving selected problems that even the **fastest** supercomputers couldn't solve in a reasonable amount of time today.

This will have an impact on complex search algorithms & data analysis simulations.

Major industry players

D-Wave The Quantum Computing Company™ · Google · Honeywell · IBM · intel · Microsoft · rigetti


Quantum Computing will decimate the security infrastructure of the digital economy
Dr. Michele Mosca
Founder of the Institute for Quantum Computing, University of Waterloo

Mega Trend: Quantum Computer

utimaco®

Problem Statement

- Shor's Algorithm **breaks asymmetric crypto**
  - Breaks **RSA** by quickly factoring large numbers
  - Breaks **Elliptic Curve** Cryptography and **Diffie-Hellman** by solving the discrete log problem
- Grover's Algorithm **weakens symmetric crypto**
  - Square-root speedup on search algorithms
  - **Weakens** symmetric encryption and hashing **by 50%**

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

Mega Trend: Quantum Computer

utimaco®

Problem Statement – In practice

- TLS key agreement
- IPSec key agreement
- SSH key agreement

… all breakable

- User authentication
- Device authentication

… mostly breakable

… impersonation attacks

- Integrity and authenticity of contracts, crypto wallets, land records – digital signatures in general etc.

… gone

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

Mega Trend: Quantum Computer

utimaco®

Problem Statement – To whom is this relevant?

Critical Infrastructure Sectors

- Energy & Water
- Health
- Transport
- Financial
- ICT
- Food
- Public & Legal Order & Safety
- Government & Military

Driver for enterprise: Risk & Cost

Customer wants to protect existing products / processes from being broken

Driver for solution provider: Innovation & Growth

Customer / IT solution provider wants to offer PQC enabled or enabling new product generations

NIST PQC Standardization Process

utimaco®

Progress in development and standardization of PQC

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Dec 20, 2016
Federal Register Notice calling for PQC submissions

Nov 30, 2017
82 received

Dec 20, 2017
69 accepted

Apr 2018
1st NIST PQC Standardization Conference

Jan 30, 2019
1st round end, 26 in 2nd round

Aug, 2019
2nd NIST PQC Standardization Conference

Q2-Q3, 2020
1st selection(s)

2021+
Draft Standards Available

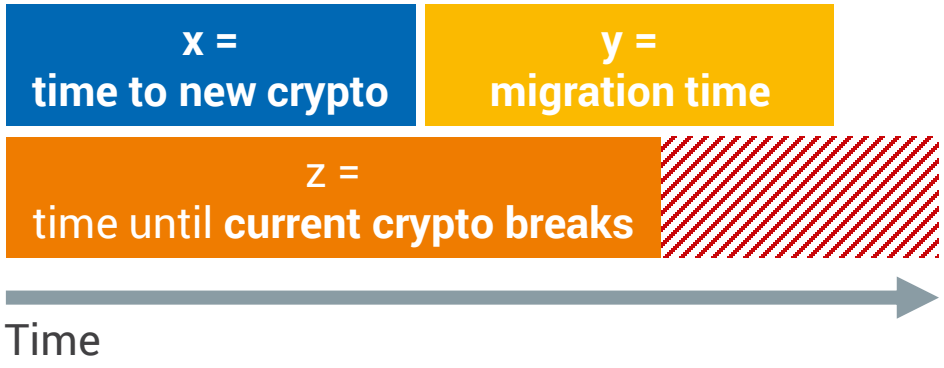
2017 → 2018 → 2019 → 2020 → 2021+

The PQC market is **expected to take off 2025** (limited by NIST approval of new algorithms) – but **innovation and risk assessment initiatives MUST start earlier**.

The risk of not being secured by Post Quantum Cryptography

utimaco®

Problem Statement – Why should you care … now?



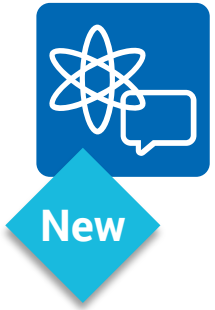
Especially organizations with the need to **secure products and infrastructures over long periods of time** (automotive, government, energy, manufacturing) have already started with road mapping, PoCs & implementations.

PQC products are **expected to take off 2025** (limited by NIST approval of new algorithms) – but **innovation and risk assessment initiatives MUST start earlier**.

How to respond to the quantum threat?

utimaco®

Get support



PQC Consultancy
UTIMACO Services

Before Quantum

Analysis & Assessment (Consultancy)

- Inventory of keys
- 3rd party usage
- Roadmap & POCs
- Crypto agility
- Impact / Risk

x + y < z

time to new crypto | migration time

time until **current crypto breaks**

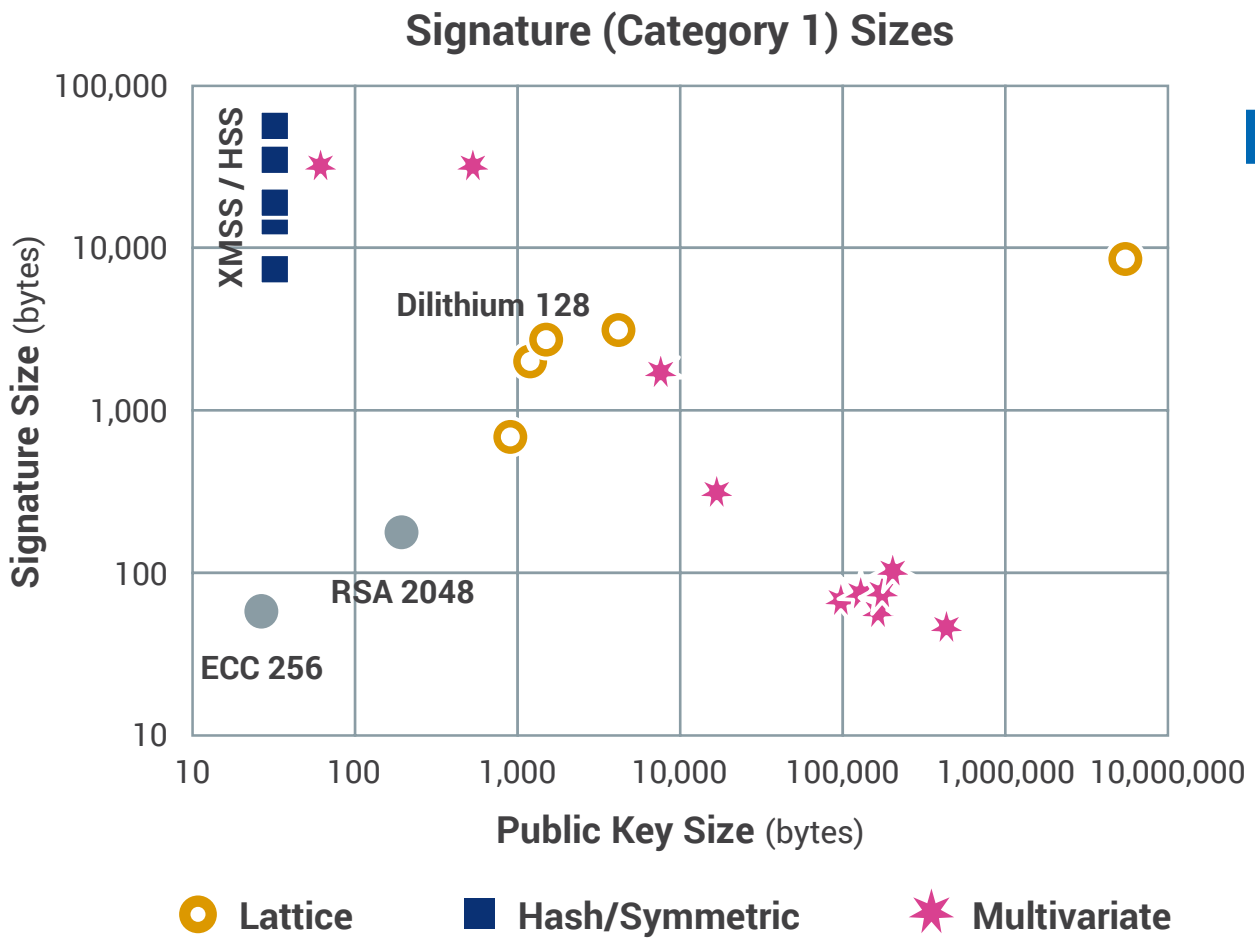
yes → **Orderly Migration**

no → **Mitigation** → **Emergency Migration**

Post Quantum

utimaco®

Get support



https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf

Challenges

- Increased complexity: Choose **the right algorithm**
  - Key size
  - Storage space required
  - Speed of execution

- Identify the impact on your business
- Start ***now*** to prepare for migration !
- Learn about the impact of the new algorithms on your infrastructure

PQC Consultancy
UTIMACO Services

UTIMACO Q-safe 1.0

utimaco®

Get the tools

Quantum-Safe Cryptography	Digital Signature	Public-Key Encryption	Key Agreement
Hash-based Signatures (**XMSS**, **HSS**, …)	X		
Lattices (**Dilithium**, **Kyber**, NewHope, Frodo, …)	X	X	X
Error Correcting Codes (Classic McEliece, …)	X	X	
Elliptic Curve Isogenies (SIKE)	X	X	X
Multivariate (Rainbow, …)	X	X	

Q-safe is the only commercially available HSM extension in the market today, that allows you to run quantum-safe algorithms within the secure perimeter of an HSM.

UTIMACO Q-safe 1.0

utimaco®

Q-safe Offering – What's in?

Which algorithm?	Why this one?
Hash-based Signature Schemes	
XMSS (eXtended Merkle Signature Scheme) **XMSS-MT** (XMSS Multi Tree)	◆ Recognized as quantum-safe ◆ Approved by German BSI (Federal Office for Information Security) ◆ Advanced standardization
HSS (Hierarchical Signature Scheme)	◆ Recognized as quantum-safe ◆ Advanced standardization
Lattice-based schemes	
Dilithium-128 (signature scheme)	◆ Several requests from customers & solution vendors
Kyber-768, **Kyber-1024** (key encapsulation)	◆ Several requests from customers & solution vendors
Coming with Q-safe 1.1 in Q3	
HSS-MT (HSS Multi Tree), **Dilithium-90**, **Kyber-512**	◆ Completing algorithm options / key sizes

UTIMACO Q-safe 1.0

utimaco®

Q-safe Offering – What's in it?

- **Firmware Module** implementing PQC algorithms
  - Extension for SecurityServer Se-Series Gen2 and CSe-Series
  - Retro-fittable to installed base
    - *Minimum requirement: SecurityServer 4.31.0*
  - For Windows and Linux simulator
- **PKCS#11** Vendor Defined Mechanisms for
  - Key generation
  - Signature creation / verification
  - Key Derivation
- Tool for **Key Export / Import**
- **Documentation**
- **Sample Code** for each supported algorithm

UTIMACO
Q-safe 1.0

Is your business secured against quantum attacks?

utimaco®

3 UTIMACO PQC building blocks: Knowhow & network, consultancy, tools

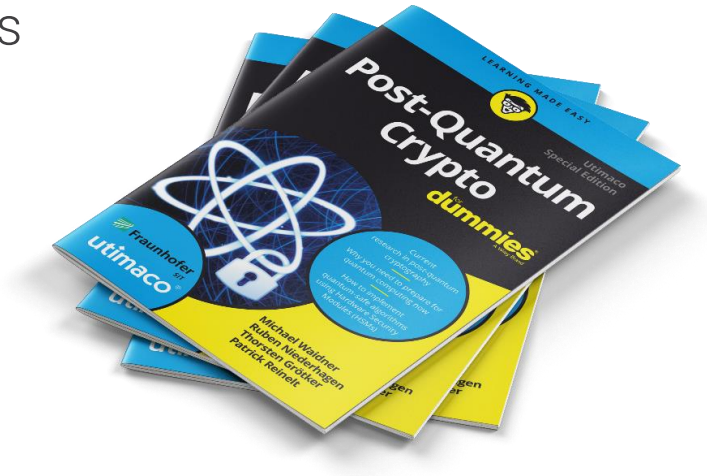
UTIMACO offers you the knowhow & network, the consultancy and the tools to

- **assess** which part of your **technical infrastructure** is prone to PQC risk,
- **determine** your **PQC roadmap** & identify critical paths (in cooperation with partners)
- **implement** the technical tools for proof of concept setups to make your crypto infrastructure and thus the future of your business quantum secure.

Implementation Tools
UTIMACO Portfolio

PQC Consultancy
UTIMACO Services

Knowhow & Network
u.Trust Program



u.trust
by Utimaco

Thank you

for your attention!

UTIMACO GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com