The Risk of not Being Secure in a Post Quantum World

Nastja Cepak - Phd Cryptography, Security Officer, CREAplus

Alexandra Günnewig – Head of Product Marketing, UTIMACO

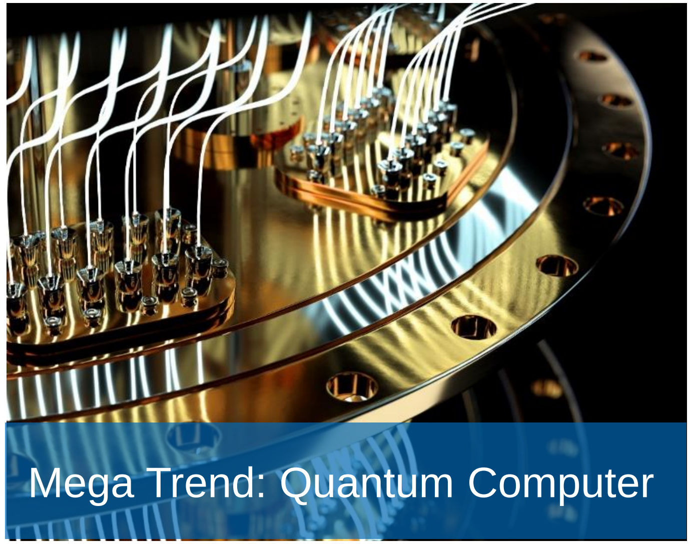
Creating Trust in
the Digital Society

CREAplus

utimaco®

Agenda

CREAplus utimaco®



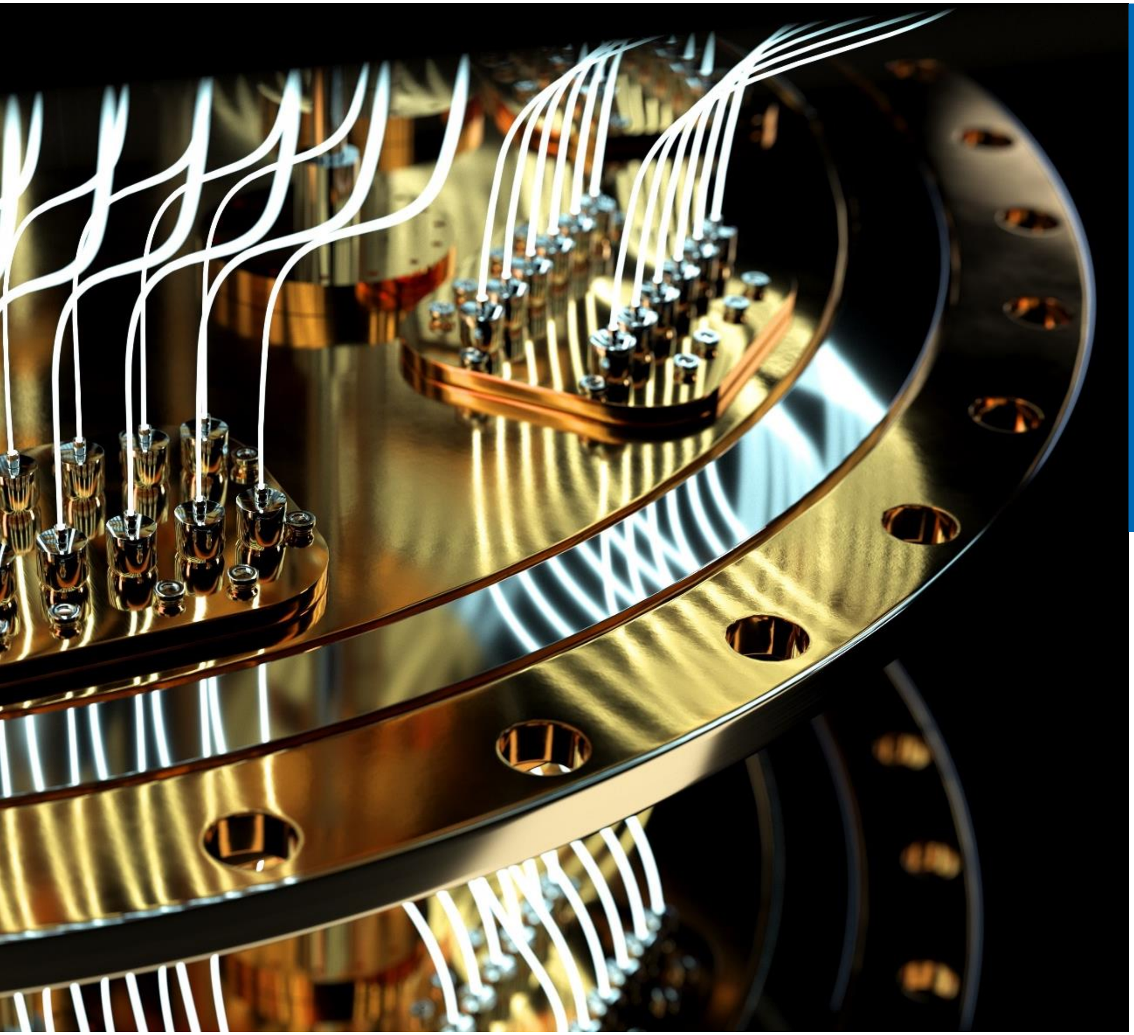
Mega Trend: Quantum Computer

Problem Statement

Utimaco PQ-safe Offering

Q&A

Mega Trend: Quantum Computer



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

What is the Difference?

CREAplus utimaco®

Classical computer

Uses **classical bits**

Possible values are just two:

0 and **1**

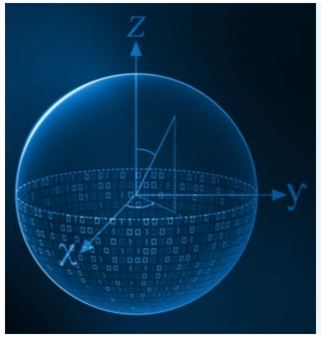
Example: 2 bits can encode 4 values (00, 01, 10, 11)

Computation ends with a **single bit state**

Result is **deterministic**

Quantum computer

Uses **qubits**



Can take values 0, 1, or infinitely many **superpositions** in-between

2 qubits can encode any superposition of the 4 states

Computation ends when we measure the result and the **superpositions collapse**

Result is **probabilistic**

Wonderings Surrounding Quantum

CREAplus utimaco®

Will quantum computers one day **completely replace** the classical computers?

VS.

Probably not

Did we already **achieve quantum supremacy?**

Partially yes

Are quantum computers already **commercially available?**

D:WAVE

QuTech

First models are available

Are quantum computers really going to **devastate our digital security?**

Definitely!

> “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

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	

What does this mean for you?

CREAplus utimaco®

Ask your IT security vendor…

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

… all breakable

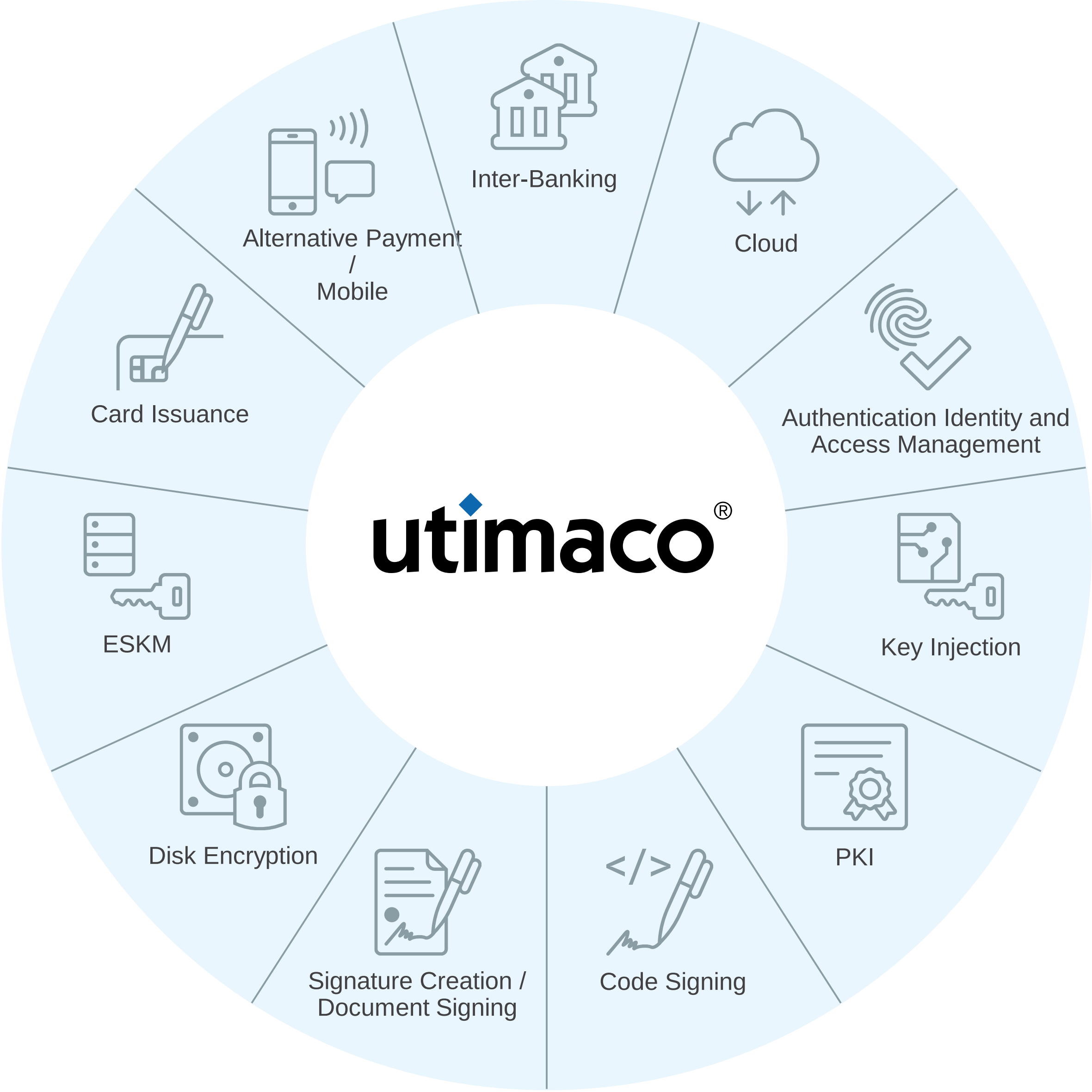
- User authentication
- Device authentication

… mostly breakable

… impersonation attacks

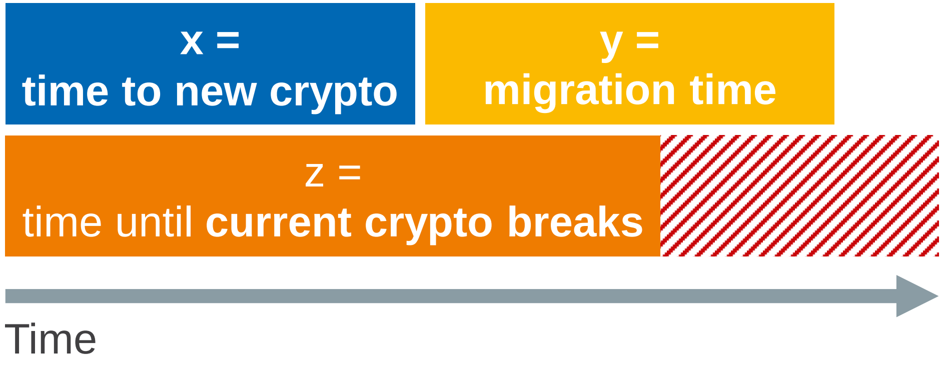
- Integrity and authenticity of contracts, crypto wallets, land records – digital signatures in general etc.

… gone


utimaco®
Inter-Banking
Cloud
Authentication Identity and Access Management
Key Injection
PKI
Code Signing
Signature Creation / Document Signing
Disk Encryption
ESKM
Card Issuance
Alternative Payment / Mobile

How long will it take you to be secure?

Problem Statement – Why should you care … now?



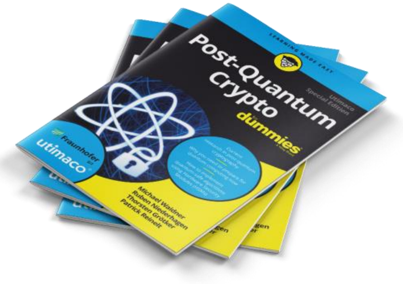
How long is it going to take *you*?

NIST PQC Standardization Process

CREAplus 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

2017
Utimaco integrates New Hope

Nov 30, 2017
82 received

Dec 20, 2017
69 accepted

March, 2018
Utimaco white paper

Apr 2018
1st NIST PQC Standardization Conference

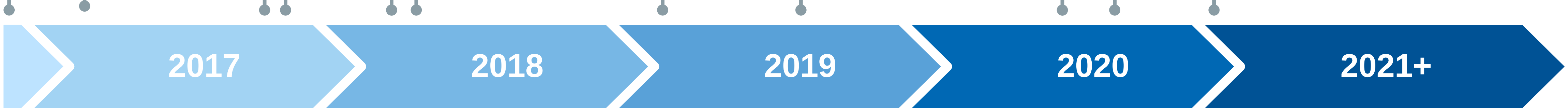
Jan 30, 2019
1st round end,
26 in 2nd round

Aug, 2019
2nd NIST PQC Standardization Conference

July 22, 2020
Finalists

July, 2020
Utimaco launches Q-safe1.0

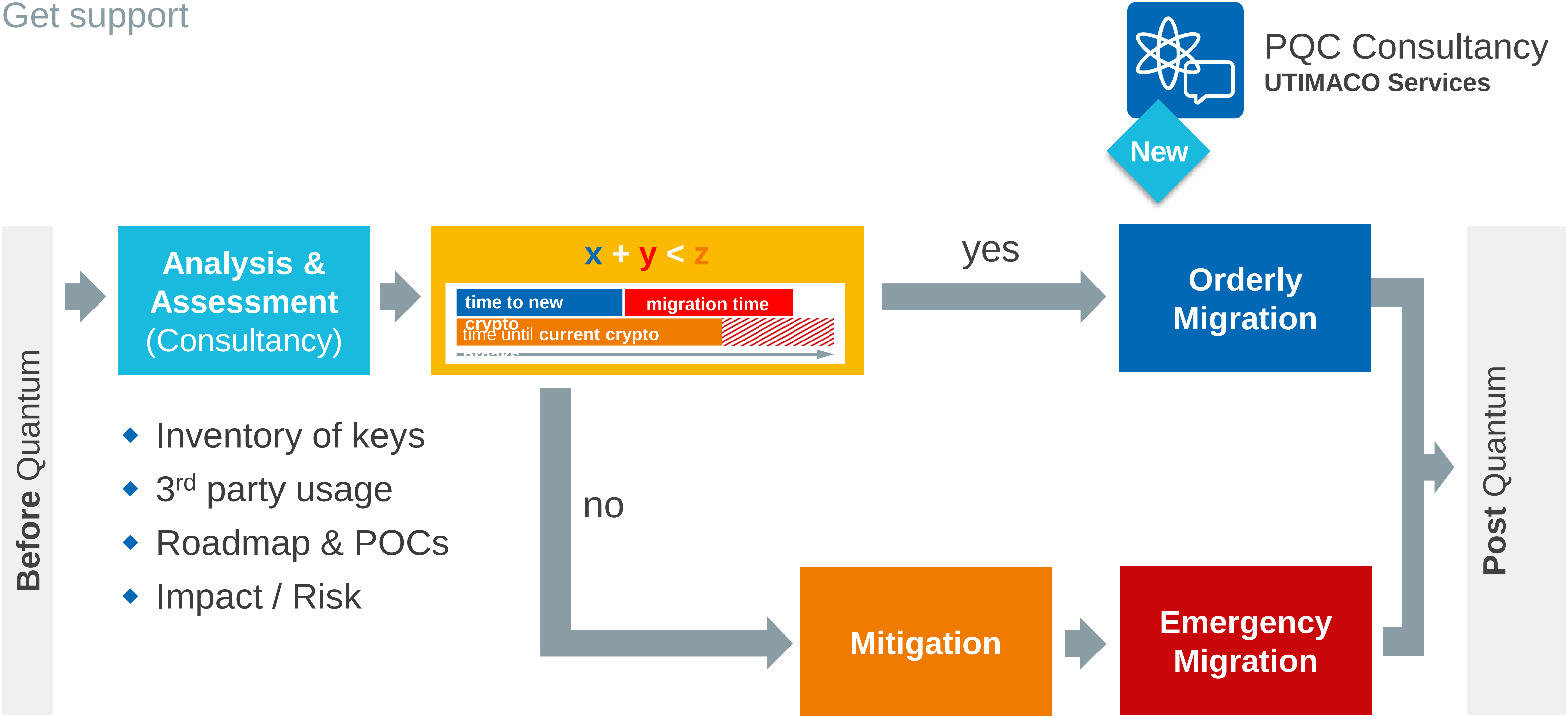
2021+
Draft Standards Available



How to respond to the quantum threat?

CREAplus utimaco®

Get support



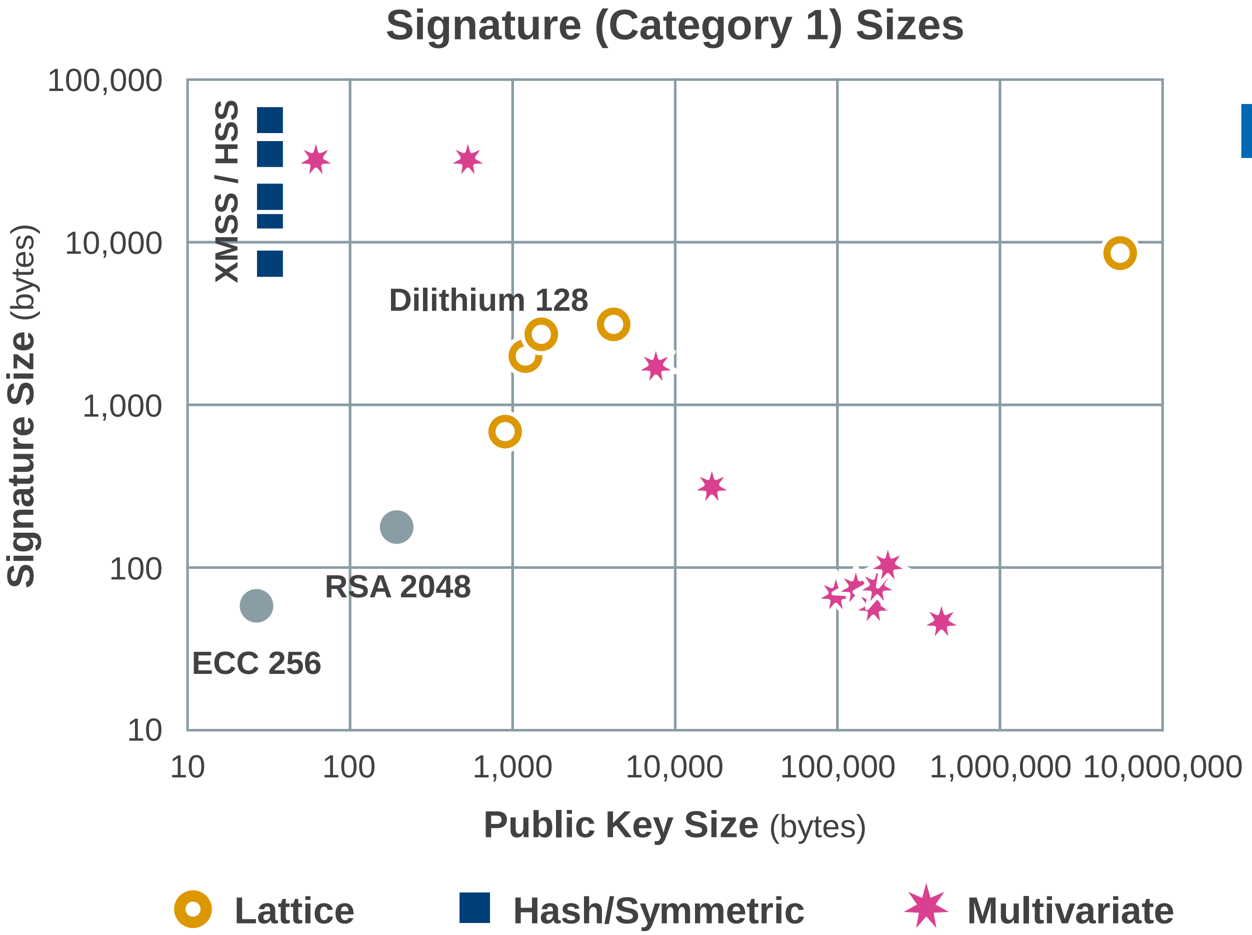
- Inventory of keys
- 3rd party usage
- Roadmap & POCs
- Impact / Risk

* Based on xyz

UTIMACO Q-safe 1.0

CREAplus 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

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	

* Available on project basis

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.

How can we help?

CREAplus utimaco®

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

UTIMACO offers you the knowhow and the tools to

- **assess** which part of your technical infrastructure is at **risk**,
- determine your **PQC roadmap** & identify **critical** paths
- implement the technical **tools** to make your crypto infrastructure quantum secure.

CREA plus

Implementation Tools
UTIMACO Portfolio

PQC Consultancy
UTIMACO Services

UTIMACO Q-safe simulator
(+ SecurityServer Simulator)

Try for FREE!

Need to implement quantum-safe algorithms?

Get in touch and try our Q-safe HSM simulator!

Stay up to date

We inform frequently about Quantum related topics

Follow us

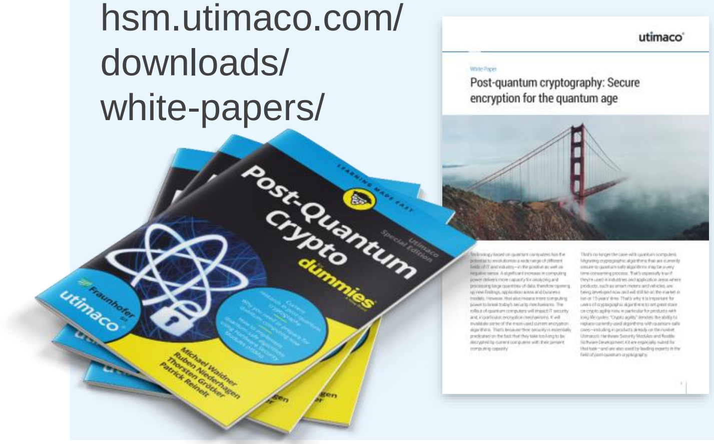
hsm.utimaco.com/blog

UTIMACO Applied Crypto Symposium

- 1st week December
- Michele Mosca – confirmed
- Lily Chen – confirmed

White paper

hsm.utimaco.com/
downloads/
white-papers/


Post-Quantum Crypto
dummies
utimaco
Post-quantum cryptography: Secure encryption for the quantum age

UTIMACO Blog

hsm.utimaco.com/blog

Itan Barmes
Deloitte

Lily Chen
NIST

Michele Mosca
University of Waterloo

Thank you

for your attention!

UTIMACO IS GmbH

Germanusstraße 4
52080 Aachen
Germany

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

utimaco®