Practical implementation of PQC

Why you need to worry now!

Malte Pollmann, Utimaco GmbH, Aachen

utimaco®

About us

Utimaco is an international provider of

» cyber security solutions «

with Headquarters in Aachen & Campbell

66 Mio €
Revenue FY 19/20

300+ highly skilled experts

Worldwide customer and partner network in more than **90** countries

Founded **1964**
Private company

50+ years in IT and
35+ years in IT-Security

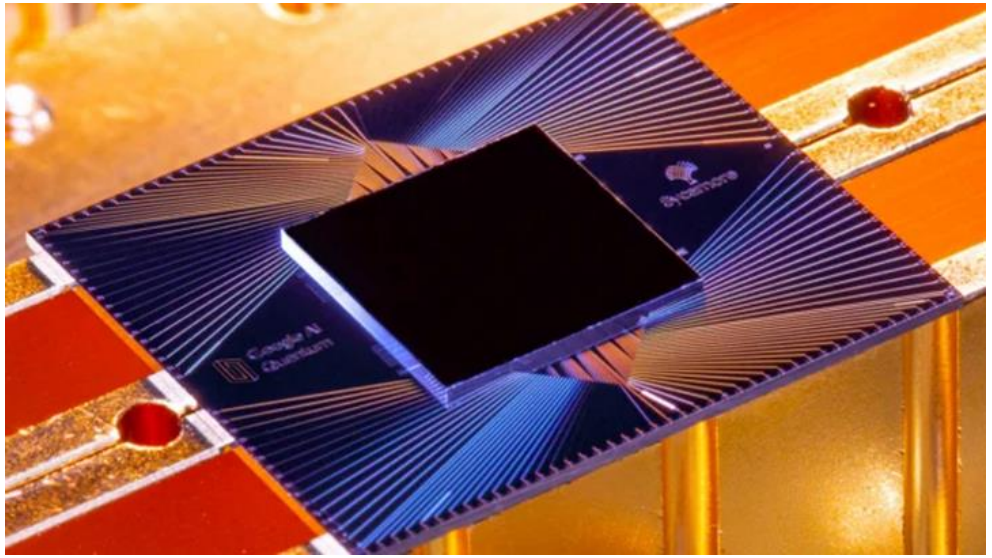
Our Vision

Securing digital values and protecting communication between citizens, devices and global networks

And now a new „Hello World“ moment

Google Sycamore chip – demonstrated „Quantum Supremacy“

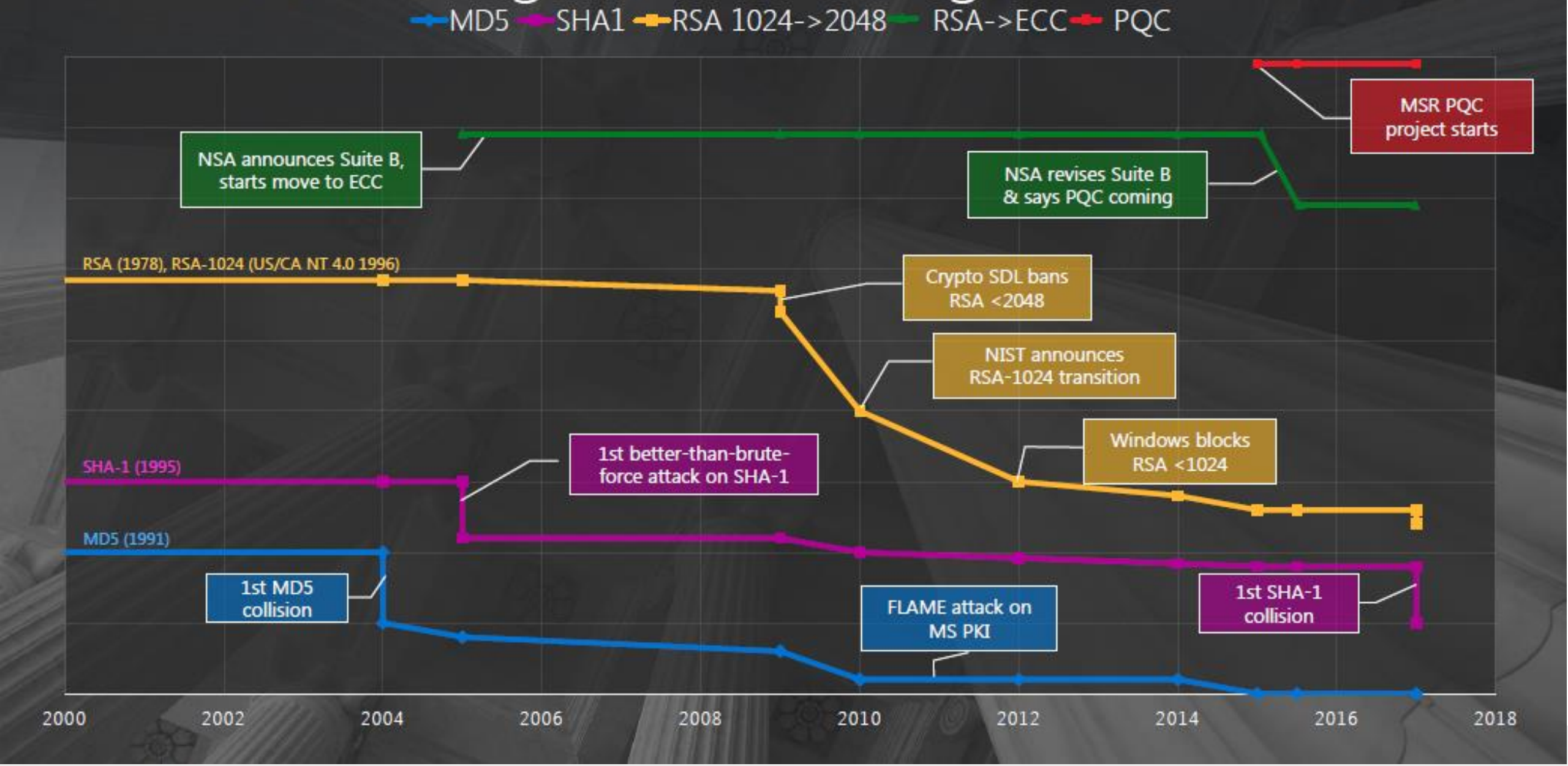
Quantum computers take advantage of quantum physics for solving selected problems that even the **fastest** supercomputers couldn’t solve in a reasonable amount of time today.
This will have an impact on complex search algorithms & data analysis simulations.



Major industry players

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

Relative Algorithms Strength Over Time



Impact of Post-Quantum computing on cryptography

utimaco®

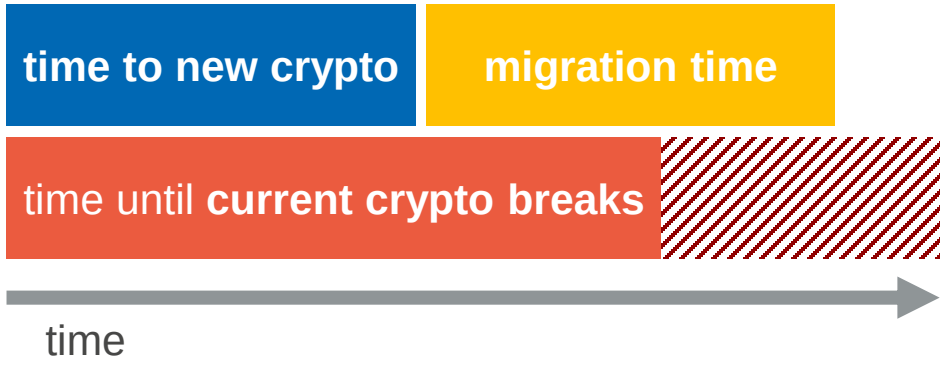
Quantum Computing Algorithms

- Shor's Algorithm breaks **asymmetric crypto**
  - Breaks RSA by quickly factorizing 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
  - Reduces cryptographic strength of symmetric encryption and hashing by 50%

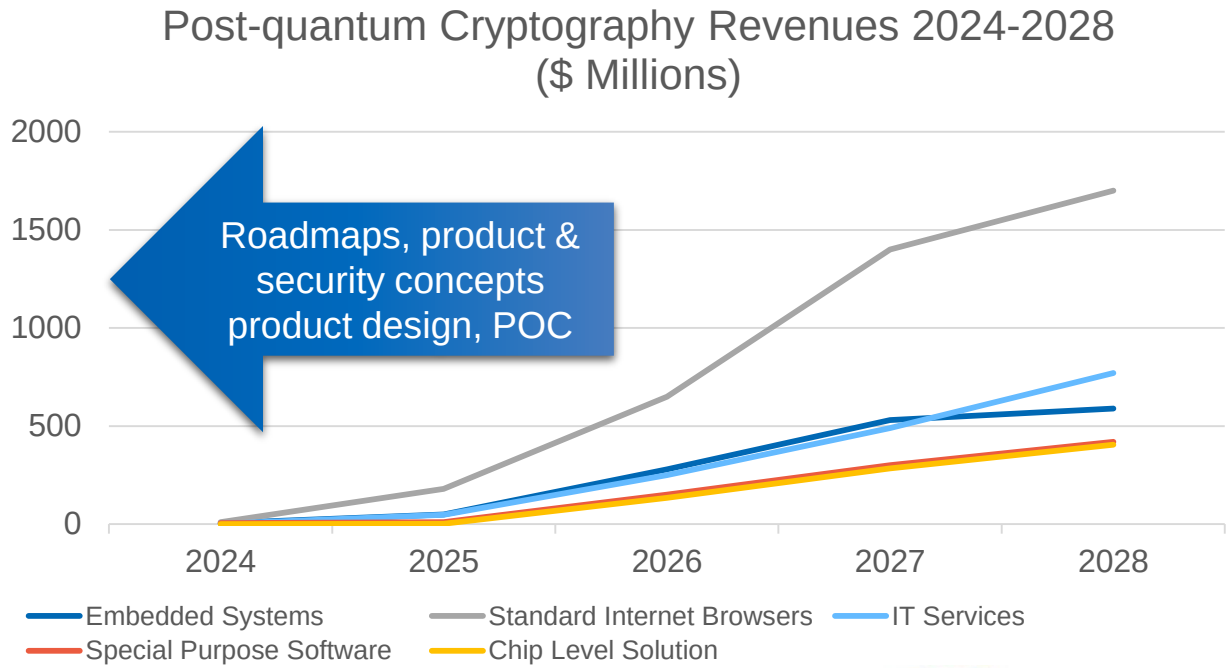
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

Post-Quantum Cryptography

Do we need to worry 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



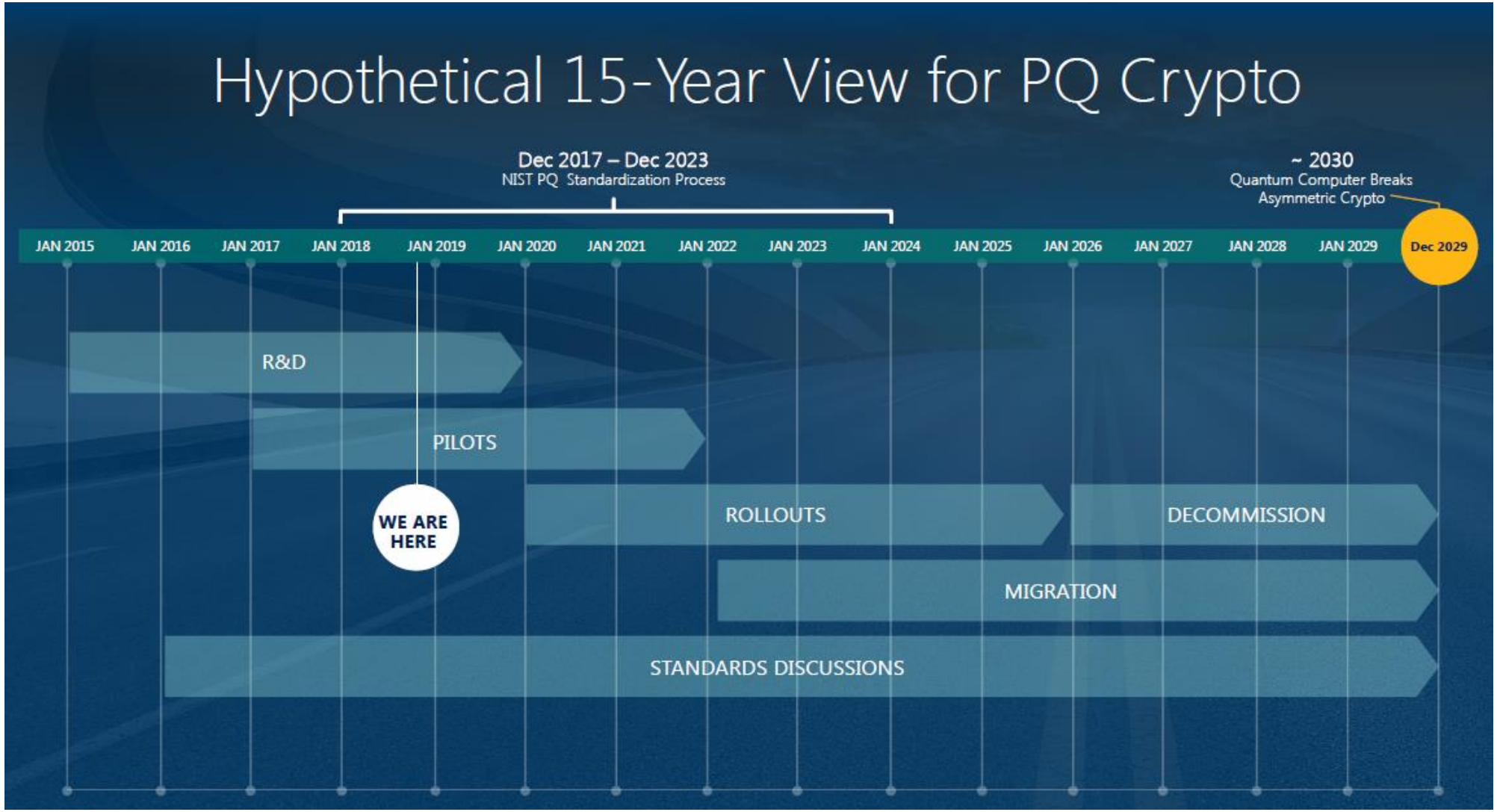
Depends on*:
- *security shelf-life* (*x* years)
- *migration time (y years)*
- *collapse time (z years)*

"Theorem": If *x* + *y* > *z*, then worry!

What is ‘z’?

- **M. Mosca** [Oxford, 1996]: *“20 qubits in 20 years”*
- **Microsoft Research** [October 2015]: *”Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer* **within a decade**”*.*
- **M. Mosca**([NIST,April 2015], [ISACA**,** September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*
- **M. Mosca**[London, September 2017]*: “1/6 chance within 10 years”*
- **Simon Benjamin** [London, September 2017]: *Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 years”*

Timeline for real-life implementations



DoD PKI MIGRATION EXAMPLE

There's more than
4.5 million active users
in the DoD identity
management system.

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

ISARA

Utimaco Post-Quantum timeline

#1 choice of PQC experts: building thought leadership & an ecosystem

2017
1st Applied Crypto Symposium – Microsoft announces availability of Picnic

2017
Publication of 1st white paper: New Hope implementation

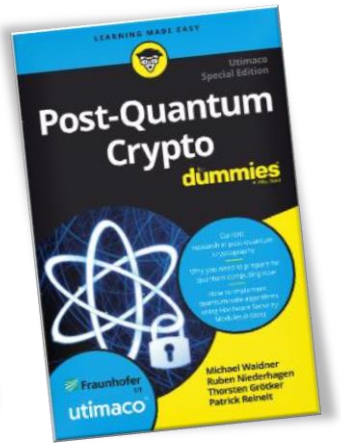
2018
RSA: Publication of PQC for Dummies

2018
2nd & 3rd Applied Crypto Symposium

Feb 2019
1st implementation of digital certificates using Picnic & publication of 6 blog posts

May 2019
LibOQS porting to CryptoServer – **setting standards** via open source

June 2019
Start of productization: Qsafe



Webinar with Brian LaMaccia

May 2019

Brian LaMacchia, Distinguished Engineer, Microsoft

Microsoft

utimaco® WEBINAR

Practical implementations can start already

Free PQC enabled HSM simulator

- **Fully functional software simulator** for Windows and Linux
  - HSM administration, user authentication, key management, cryptography, etc.
- Ideal for
  - Proof of concepts to evaluate impact of new algorithms on your infrastructure & products
  - Dry-run before setup of production HSM

Available **for free** on the Utimaco website

Open Quantum Safe Project

- The **Open Quantum Safe (OQS) project** has the goal of developing and prototyping quantum-resistant cryptography.
- **LIBOQS** is an open source **C library for quantum-resistant cryptographic algorithms**.
- LIBOQS provides:
  - a common API for post-quantum key encapsulation mechanisms and digital signature schemes
  - a collection of open source implementations of post-quantum cryptography algorithms
  - a test harness and benchmarking routines
- The OQS project also provides prototype integrations into application-level protocols to enable testing of quantum-resistant cryptography.
- More information on OQS can be found on our website: https://openquantumsafe.org/

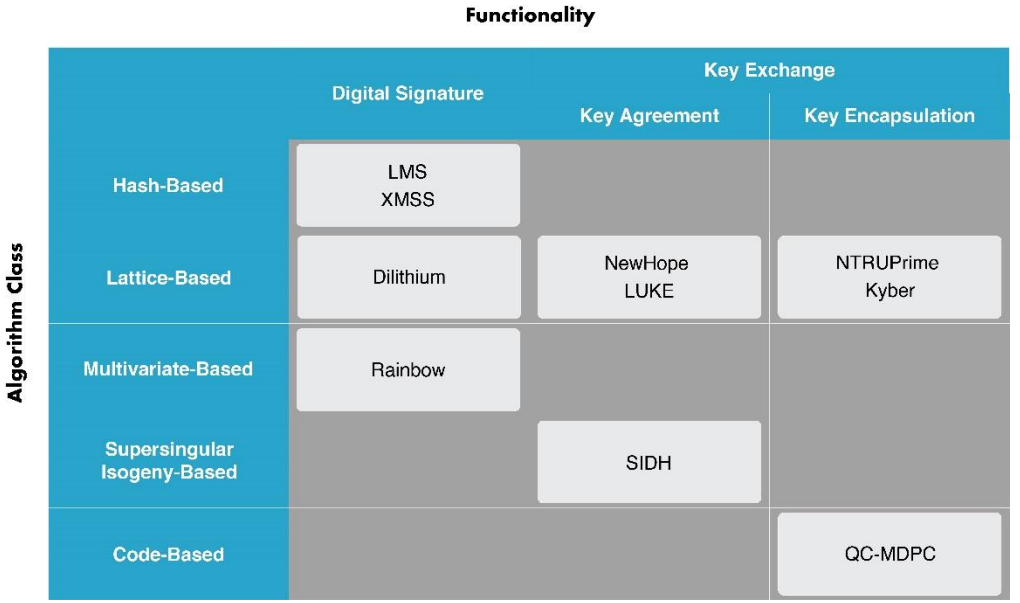
- https://github.com/open-quantum-safe/liboqs

Roadmap – Post Quantum Cryptography

PQC Building Blocks Available Today

- Prototyping, POC, performance optimization
  - PICNIC [https://microsoft.github.io/Picnic/]
    HSM firmware module code: https://microsoft.github.io/Picnic/picnic_hsm_demo.zip
  - SIDH performance improvements [LGE]
  - Efficient Implementation of Lattice-based Cryptography [RWTH Aachen]
  - WIP

- Partner Products
  - Isara Radiate suite
    - Version 1.4 updated to support HSM implementations of LMS and XMSS (stateful hash-based signature schemes)



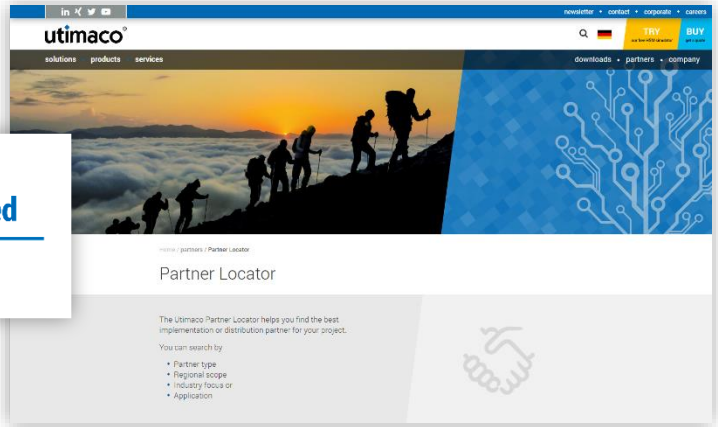
Roadmap – Post Quantum Cryptography

SecurityServer 4.40

- Adaptions in base firmware modules
  - Working with lighthouse customers and **partners**
  - E.g. account for larger key sizes (key.db)
- Hybrid schemes
  - **Examples** (SDKs)
  - Key exchange: New Hope -> Secure Messaging
  - Hash-based signature: XMSS/LMS -> firmware module signing
- PQC firmware libraries
  - **Partners**
  - Cooperation w/ academia
  - Utimaco

PQCRYPTO
ICT-645622

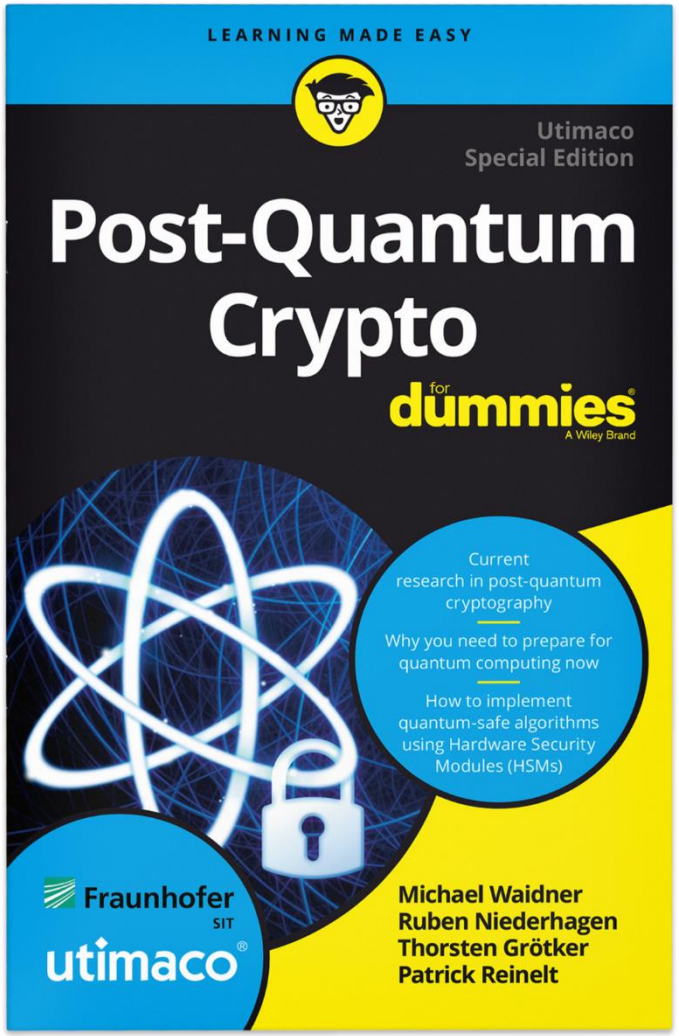
utimaco certified
Partner Program

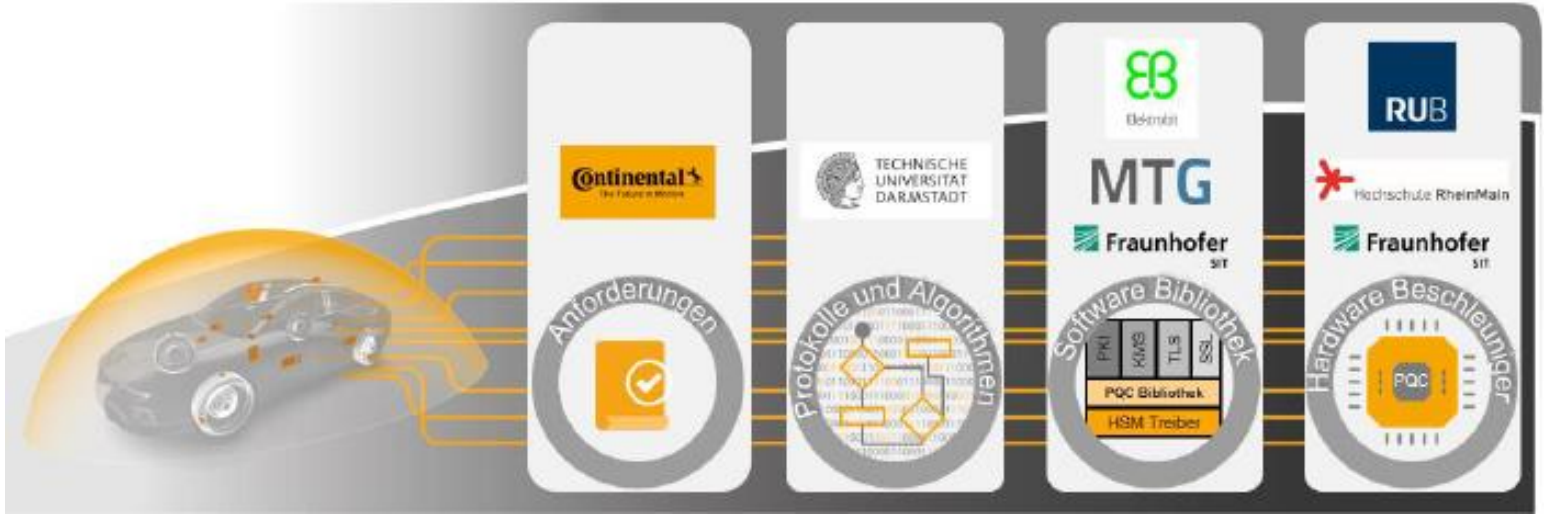


https://hsm.utimaco.com/partners/partner-locator

Education & Quantum RISC project

Industry leaders in post-quantum crypto work with Utimaco HSMs





➔ APIs for PQC algorithms

Education & Quantum RISC project

Industry leaders in post-quantum crypto work with Utimaco HSMs

Goal:

- Research on the use of PQC methods on resource-restricted embedded systems, e.g. RISC-V
- PQC-based applications for embedded systems (e.g. OTA).Challenge
- Selection of PQC procedures and protocols, as well as the secure implementation of these procedures in an efficient software hardware co-design on a cost-effective hardware platform

Results:

- Enhanced PQC-Algorithms.
- Design of PQC-based protocols.
- Secure and efficient implementations.
- Hardware-Software Co-Design.
- Proof of concept (hardware and software) in form of a demonstrator

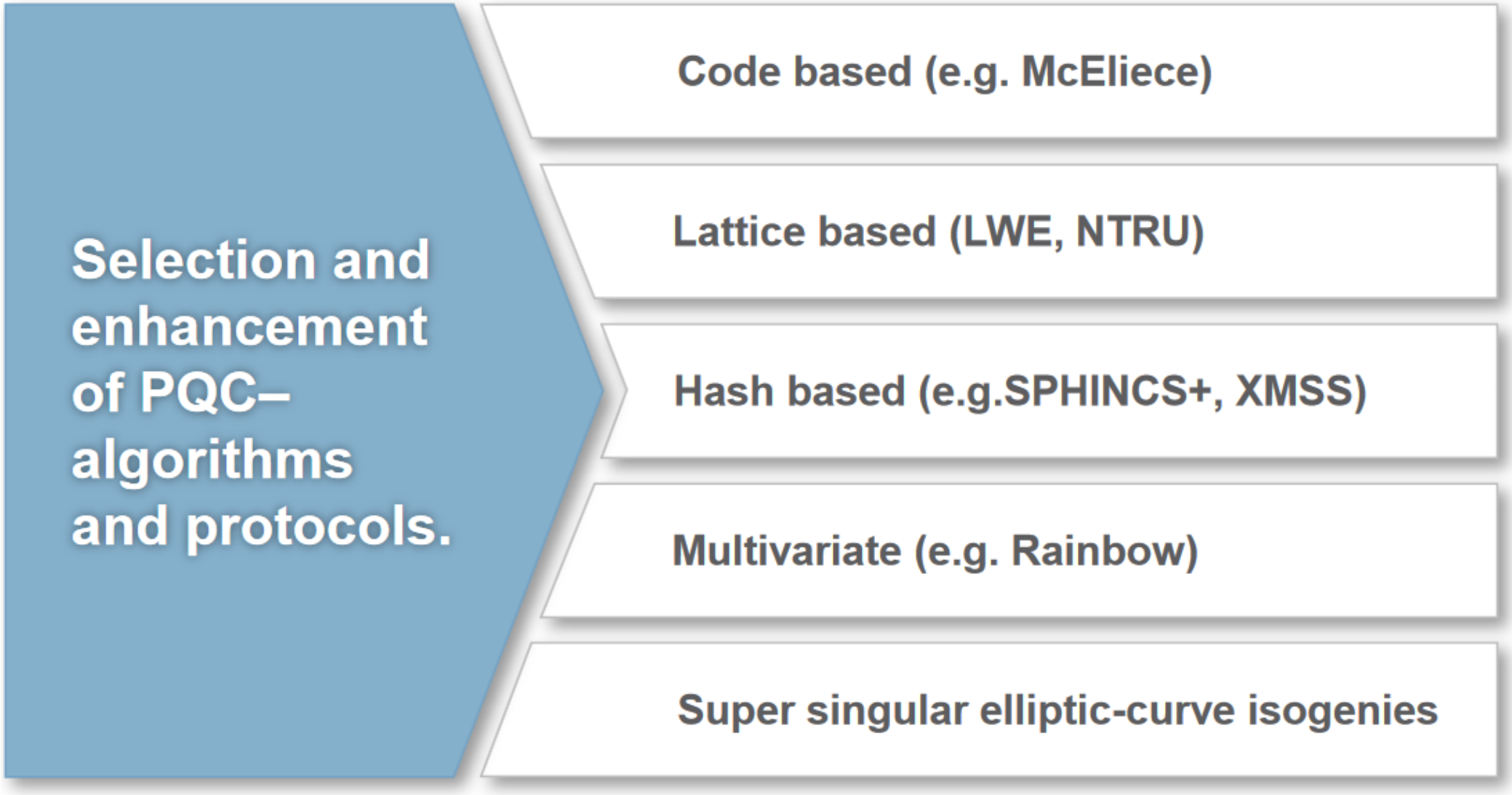
Quantum RISC – Next steps

➔ PQC migration to Utimaco HSM

➔ Crypto agility

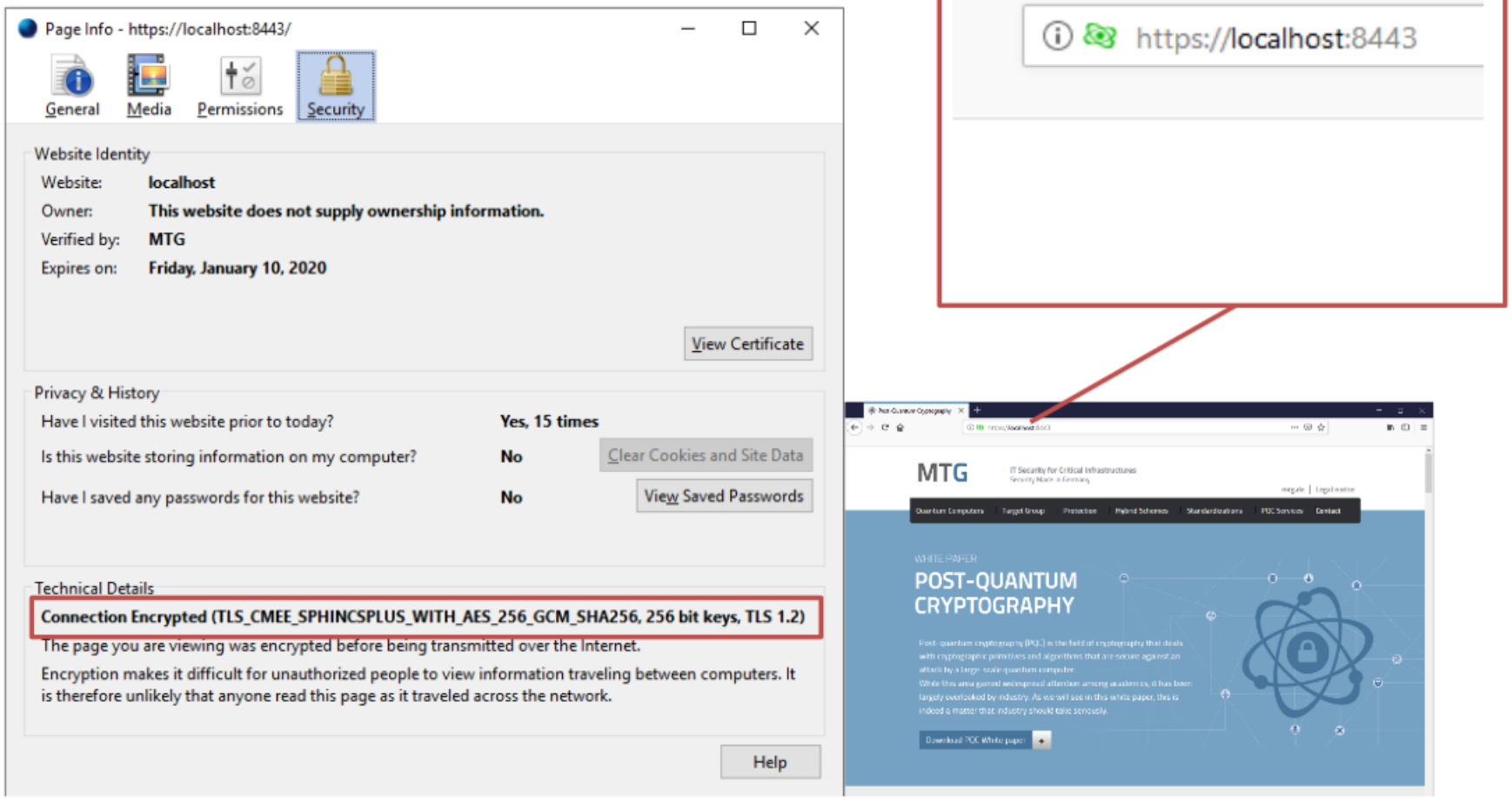
https://cloakable.irdeto.com/2018/06/21/cryptographic-agility/

Quantum RISC – Next steps



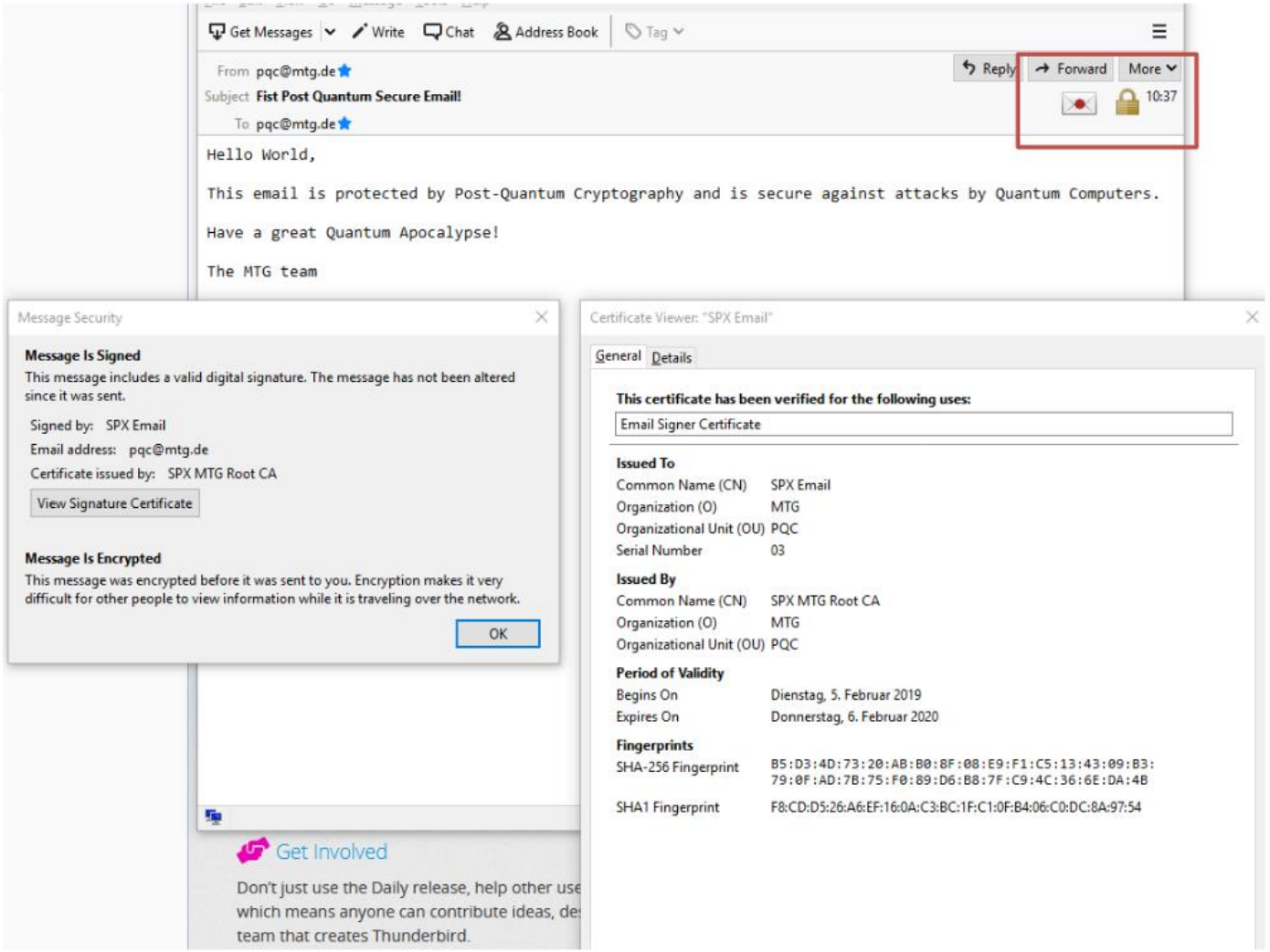
Quantum RISC – other practical implementations

Use Case: POC Web Browser & Web Server



Quantum RISC – other practical implementations

Use Case: PQC Email Client



Why Utimaco HSMs?

PQC: an SDK is a must-have

The **CryptoServer Software Development Kit (SDK)**
is the professional development environment for all Utimaco Hardware Security Modules.

Cost-effective development

It allows integrators and end-users to create specific applications, e.g. proprietary or PQC algorithms, custom key derivation procedures or complex protocols that run in the tamper-proof environment of the HSM.

- **Fast:**
  - Provides full access to the Utimaco base firmware, so custom firmware modules can be developed in a very short time frame.
- **Cost efficient, simple & easy to use**
  - **Simple pricing**: No additional license fees for runtime environments or per delivered application
  - **Minimal training**: use of standard programming languages & common development environments
  - **Efficient testing** & debugging
  - **Good documentation:** complete description of internal programming interfaces (API) allows for maximum utilization of base firmware modules

Thanks for your attention

Malte Pollmann

Managing Director & Chief Strategy Officer

malte.pollmann@utimaco.com

Utimaco GmbH

Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696-0
Web www.utimaco.com
E-Mail info@utimaco.com