



Practical implementation of PQC

Why you need to worry now!

Malte Pollmann, Utimaco GmbH, Aachen

utimaco[®]

Utimaco is an international provider of
» **cyber security solutions** «
with Headquarters in Aachen & Campbell



66 Mio €
Revenue FY 19/20



300+ highly skilled experts



Founded **1964**
Private company



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

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



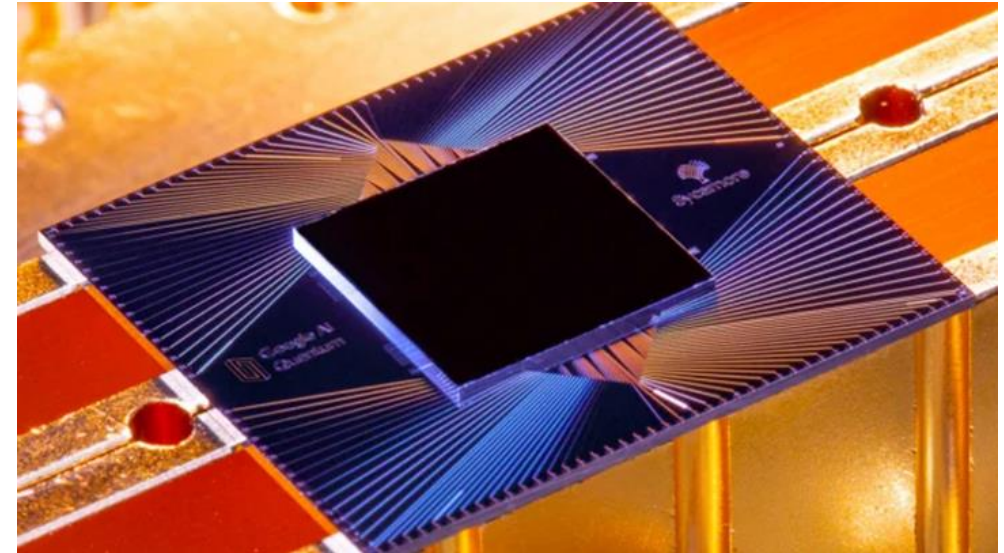
Securing digital values
and protecting
communication
between citizens,
devices and global
networks



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.

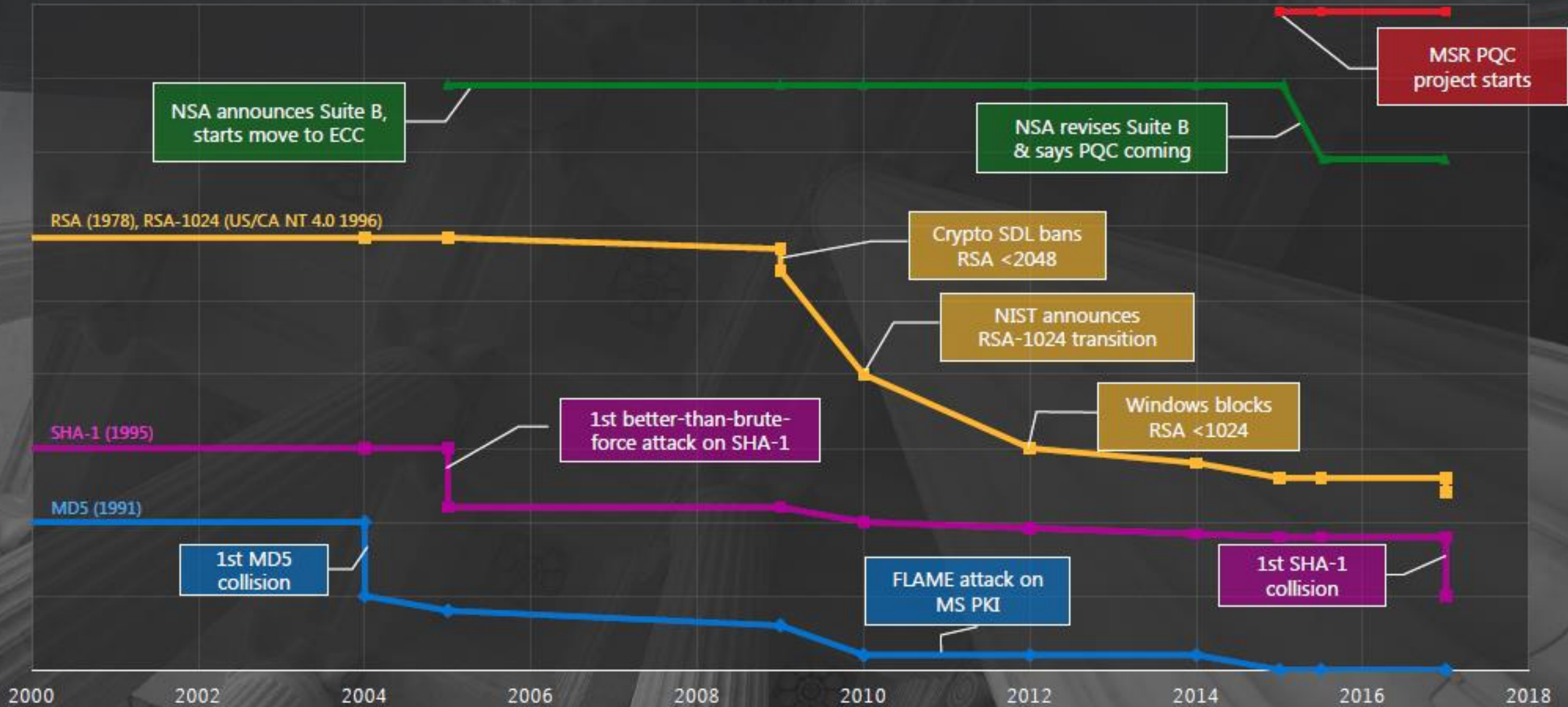


Major industry players



Relative Algorithms Strength Over Time

— MD5 — SHA1 — RSA 1024->2048 — RSA->ECC — PQC



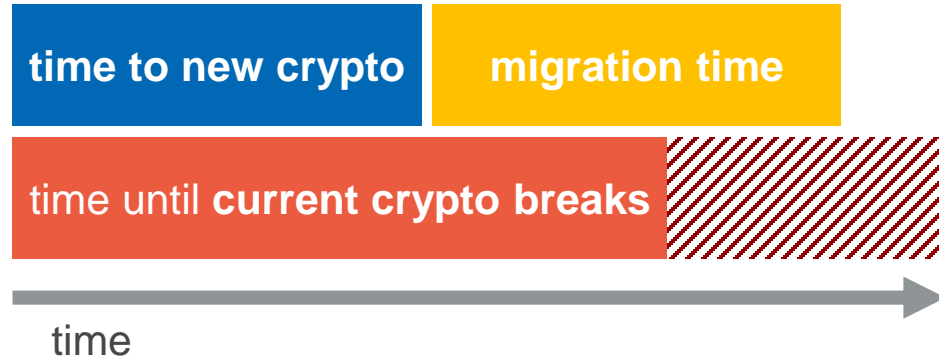
Quantum Computing Algorithms

- **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	



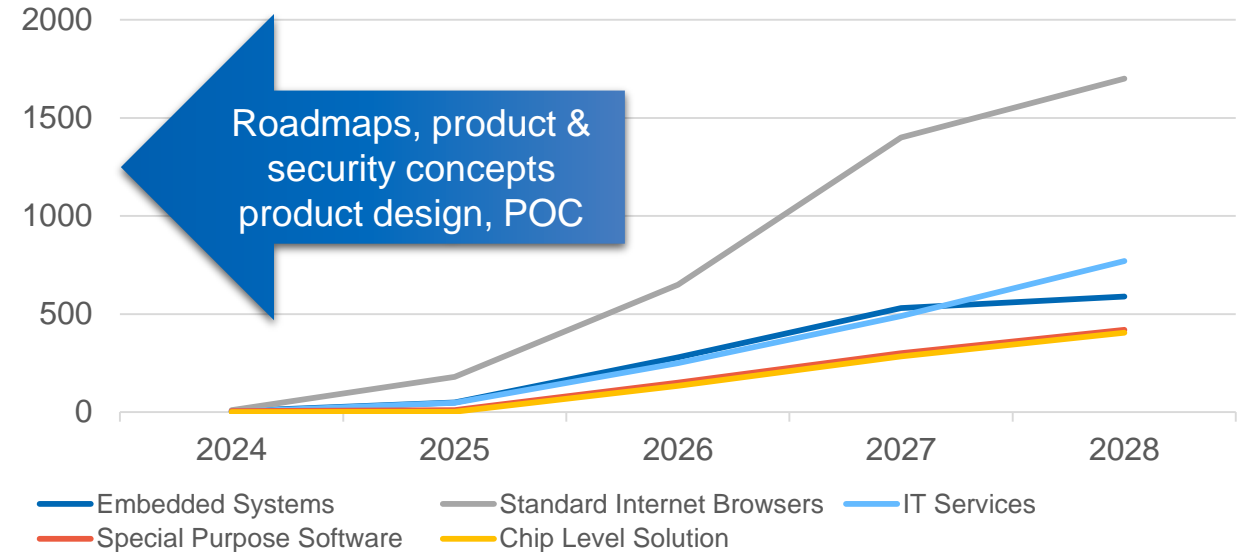
Do we need to worry now?



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



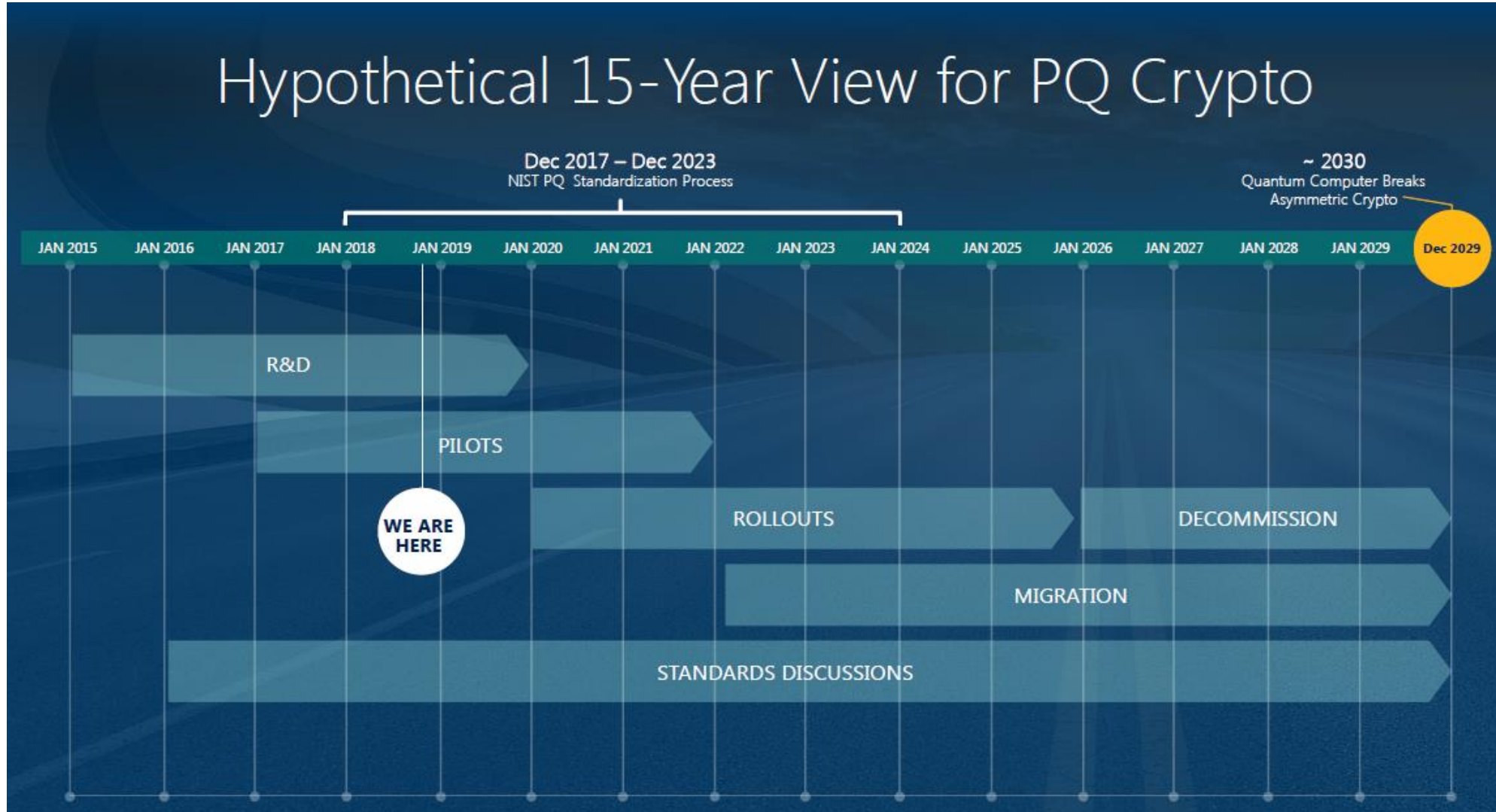
Post-quantum Cryptography Revenues 2024-2028 (\$ Millions)



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

“Theorem”: If $x + y > z$, then worry!

- **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, 1/2 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”*



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.

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

2017

Publication of 1st white paper: New Hope implementation

2017

1st Applied Crypto Symposium – Microsoft announces availability of Picnic

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

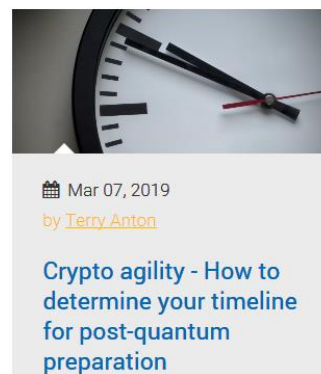
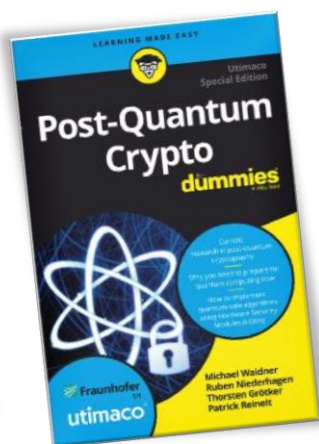
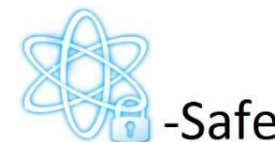


May 2019

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

June 2019

Start of production: Qsafe



Webinar with Brian LaMaccia
May 2019



Brian LaMaccia,
Distinguished Engineer, Microsoft



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



The banner features a blue background with a yellow diagonal stripe in the top right corner. On the left, there is a white icon of an atom with a padlock, and a white rocket with an orange nose cone is launching upwards. The text on the banner reads: "Need to implement quantum-safe algorithms? Get in touch and try our Q-safe HSM simulator!" and "Try for FREE!"

Available
for free
on the Utimaco
website

- 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>



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

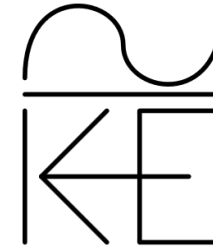
- Partner Products

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

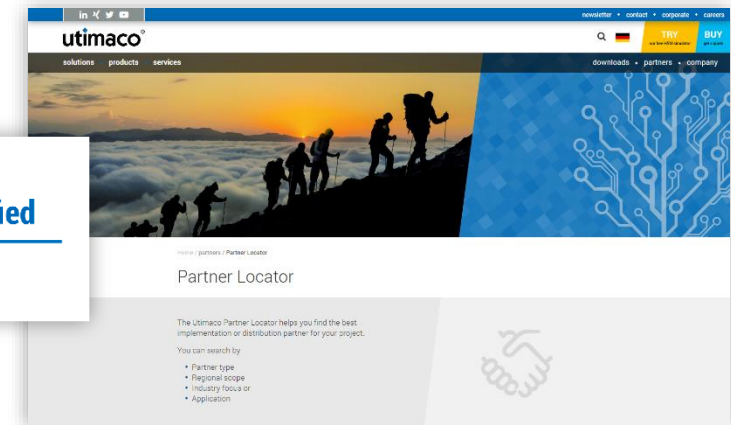
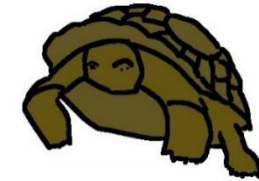
Algorithm Class	Functionality		
	Digital Signature	Key Exchange	
		Key Agreement	Key Encapsulation
Hash-Based	LMS XMSS		
Lattice-Based	Dilithium	NewHope LUKE	NTRUPrime Kyber
Multivariate-Based	Rainbow		
Supersingular Isogeny-Based		SIDH	
Code-Based			QC-MDPC

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

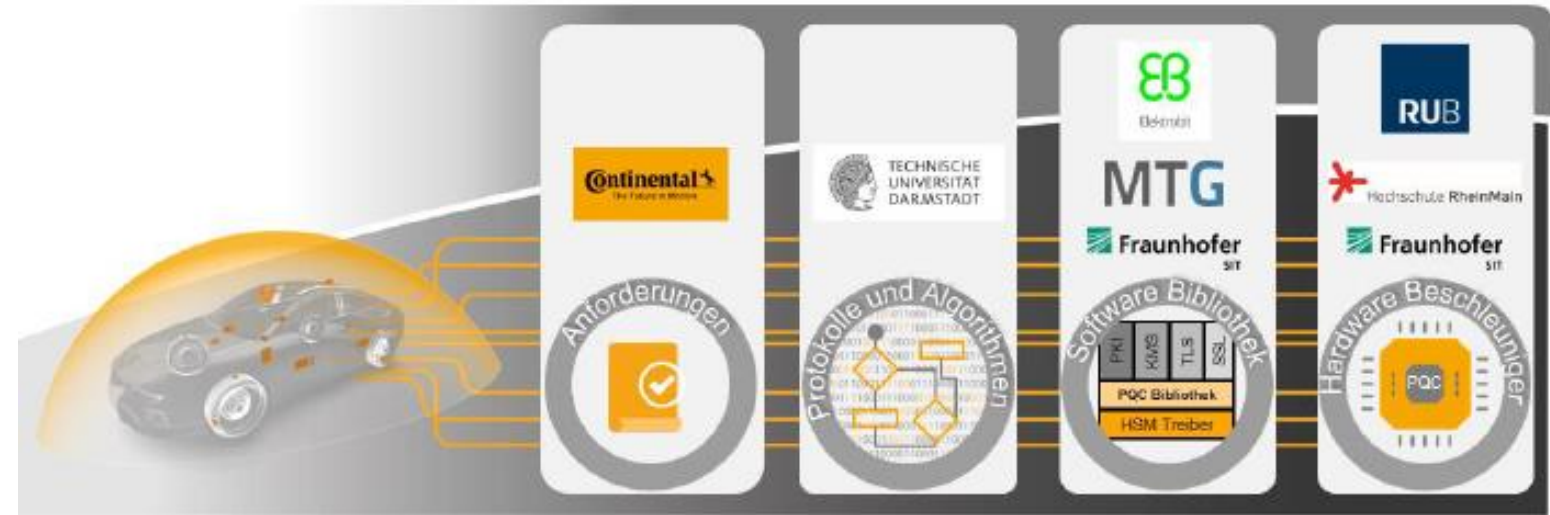
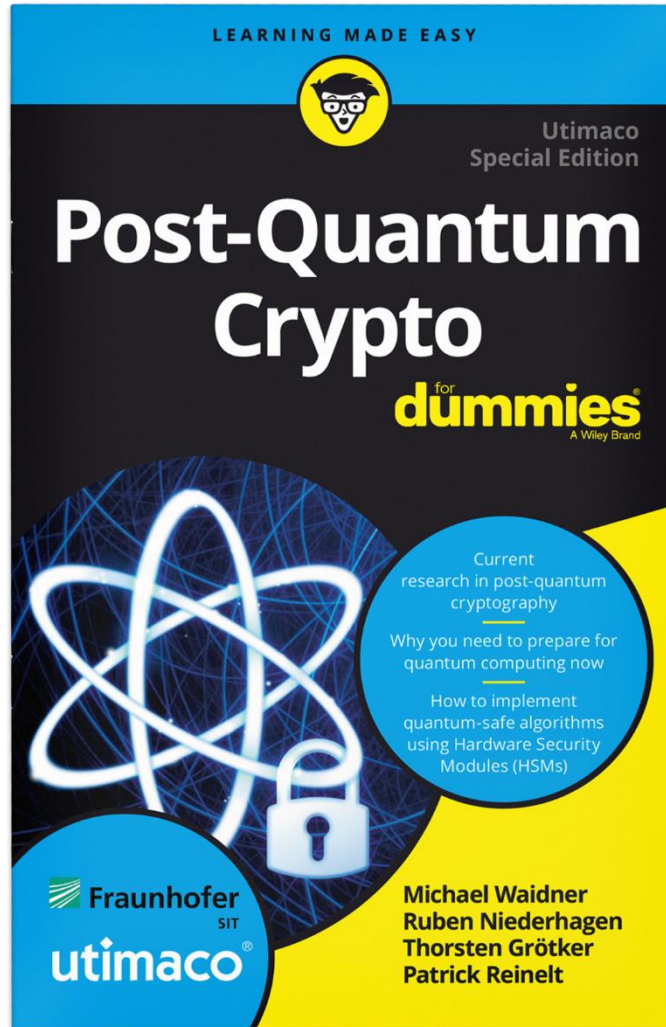


**PQCRYPTO
ICT-645622**



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

Industry leaders in post-quantum crypto work with Utimaco HSMs



→ APIs for PQC algorithms



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

Continental Over-The-Air Updates



→ PQC migration to Utimaco HSM



→ Crypto agility



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

**Selection and
enhancement
of PQC–
algorithms
and protocols.**

Code based (e.g. McEliece)

Lattice based (LWE, NTRU)

Hash based (e.g. SPHINCS+, XMSS)

Multivariate (e.g. Rainbow)

Super singular elliptic-curve isogenies

Use Case: PQC Web Browser & Web Server



Page Info - https://localhost:8443/

General Media Permissions Security

Website Identity

Website: localhost
Owner: This website does not supply ownership information.
Verified by: MTG
Expires on: Friday, January 10, 2020

View Certificate

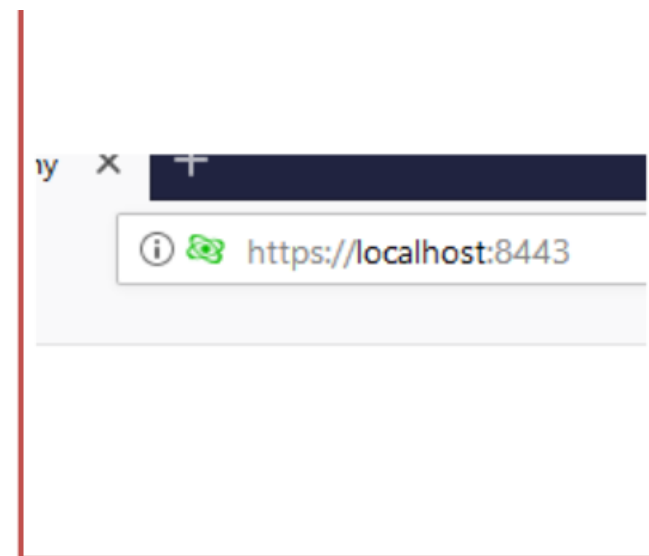
Privacy & History

Have I visited this website prior to today? Yes, 15 times
Is this website storing information on my computer? No Clear Cookies and Site Data
Have I saved any passwords for this website? No View Saved Passwords

Technical Details

Connection Encrypted (TLS_CAMEL_SPHINCSPLUS_WITH_AES_256_GCM_SHA256, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Help



Non-Quantum Cryptography

MTG IT Security for Critical Infrastructures
Security Made a Priority

Quantum Computers Target Group Protection Hybrid Schemes Standards and PQC Services Contact

WHITE PAPER
POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography (PQC) is the field of cryptography that deals with cryptographic primitives and algorithms that are secure against an attack by a large-scale quantum computer. While this area gained widespread attention among academics, it has been largely overlooked by industry. As we will see in this white paper, this is indeed a matter that industry should take seriously.

Download PQC White paper

Use Case: PQC Email Client

The screenshot displays a Thunderbird email client interface. The main window shows an email from `pqc@mtg.de` with the subject "Fist Post Quantum Secure Email". The email body contains the text: "Hello World, This email is protected by Post-Quantum Cryptography and is secure against attacks by Quantum Computers. Have a great Quantum Apocalypse! The MTG team". A red box highlights the "Forward" button and a lock icon in the top right corner of the email header.

Two dialog boxes are overlaid on the email content:

- Message Security**:
 - Message Is Signed**: This message includes a valid digital signature. The message has not been altered since it was sent.
 - Signed by: SPX Email
 - Email address: `pqc@mtg.de`
 - Certificate issued by: SPX MTG Root CA
 - [View Signature Certificate](#)
 - Message Is Encrypted**: This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.
- Certificate Viewer: "SPX Email"**:
 - General** tab selected.
 - This certificate has been verified for the following uses:**
 - Email Signer Certificate
 - Issued To**:
 - Common Name (CN): SPX Email
 - Organization (O): MTG
 - Organizational Unit (OU): PQC
 - Serial Number: 03
 - Issued By**:
 - Common Name (CN): SPX MTG Root CA
 - Organization (O): MTG
 - Organizational Unit (OU): PQC
 - Period of Validity**:
 - Begins On: Dienstag, 5. Februar 2019
 - Expires On: Donnerstag, 6. Februar 2020
 - Fingerprints**:
 - SHA-256 Fingerprint: B5:D3:4D:73:20:AB:B0:8F:08:E9:F1:C5:13:43:09:B3:79:0F:AD:7B:75:F0:89:D6:BB:7F:C9:4C:36:6E:DA:4B
 - SHA1 Fingerprint: F8:CD:D5:26:A6:EF:16:0A:C3:BC:1F:C1:0F:B4:06:C0:DC:8A:97:54

At the bottom of the email client, there is a "Get Involved" link and a message: "Don't just use the Daily release, help other use which means anyone can contribute ideas, de team that creates Thunderbird."

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

utimaco[®]