

TeleTrust-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 18.06.2019

Real World Post Quantum Cryptography in Public Key Infrastructures

Stathis Deligeorgopoulos, MTG AG



- MTG, which was founded in 1995, is a high tech software company based in the Rhein-Main region (Darmstadt, Germany) – the Germany IT security cluster.
- MTG is a leading expert for encryption technologies in Germany. MTG's IT security solutions effectively secure critical infrastructures and the Internet of Things (IoT).
- MTG offers security products and services, such as PKI, Key Management System, and HSM integration with best practice traditional and Post-Quantum Cryptography.



**Integrate
Post-Quantum
Cryptography now!**

Schrödingers Cat



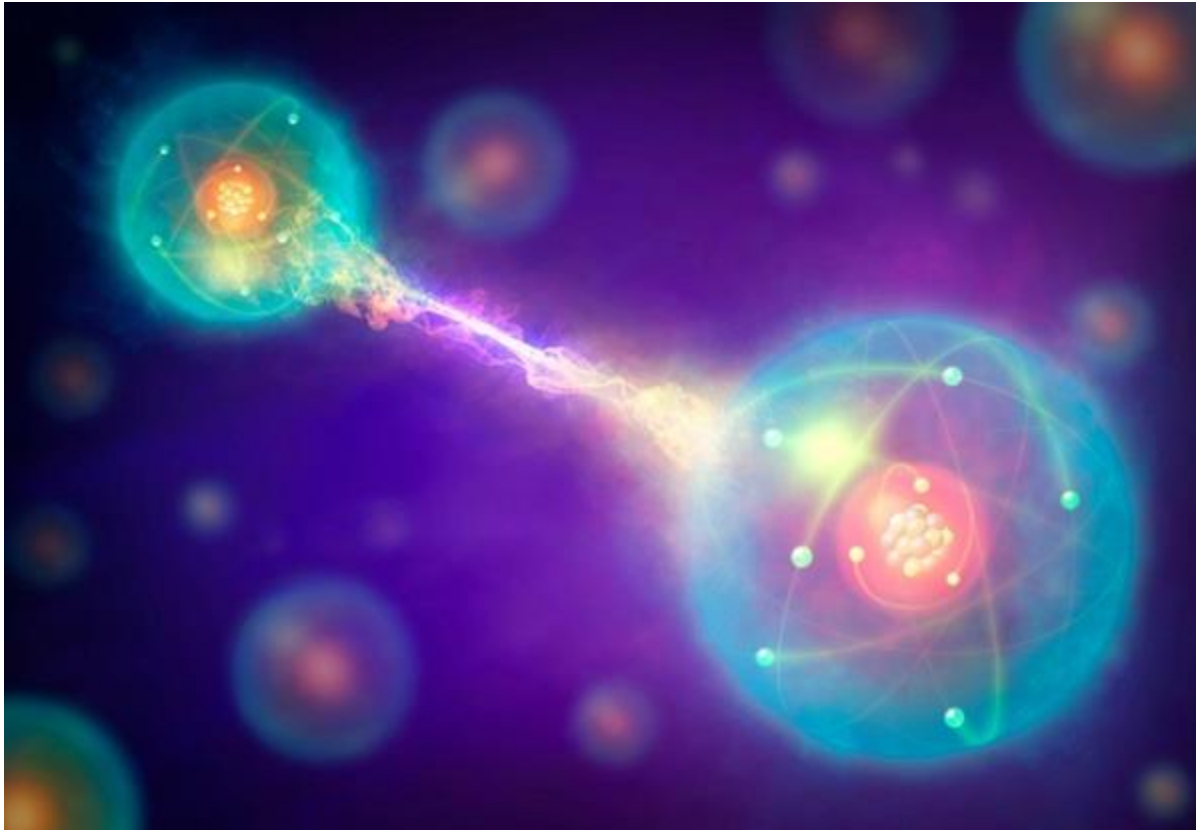
<http://www.einfachtierisch.de>

Quantum Superposition



<https://brilliant.org/courses/quantum-computing/>

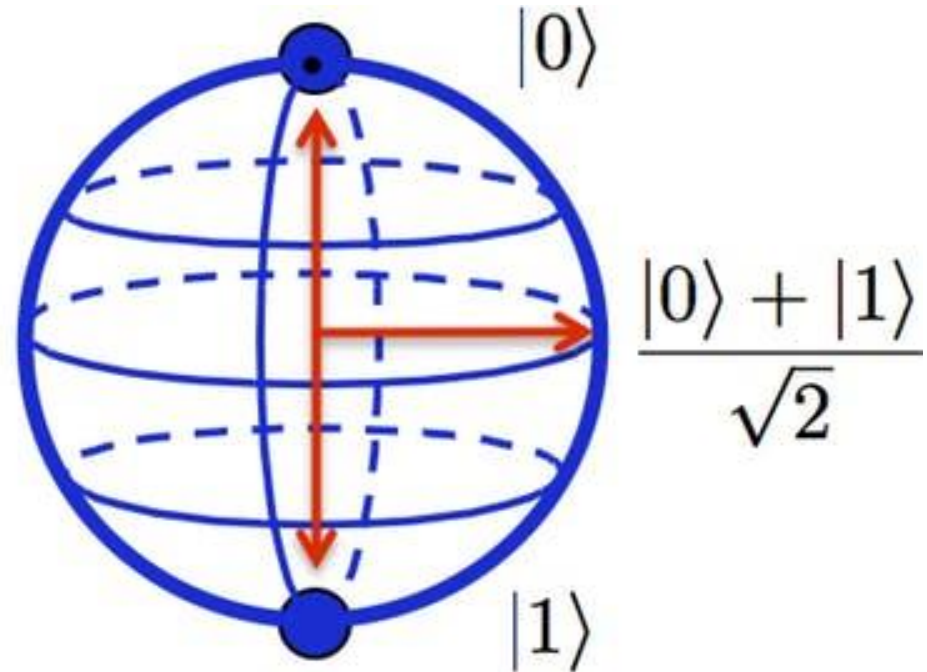
Quantum Entanglement



<http://www.astronomy.com/news/2018/08/distant-quasars-confirm-quantum-entanglement>

● 0

● 1

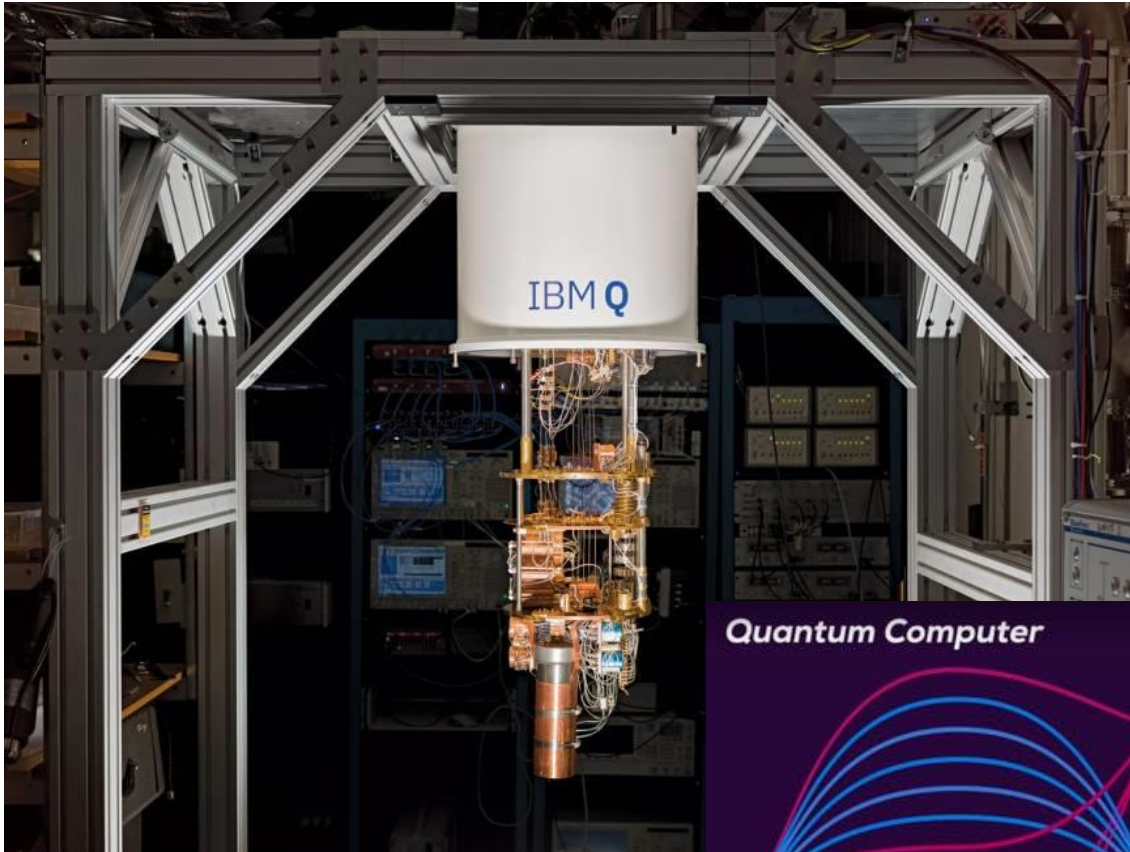


Classical Bit

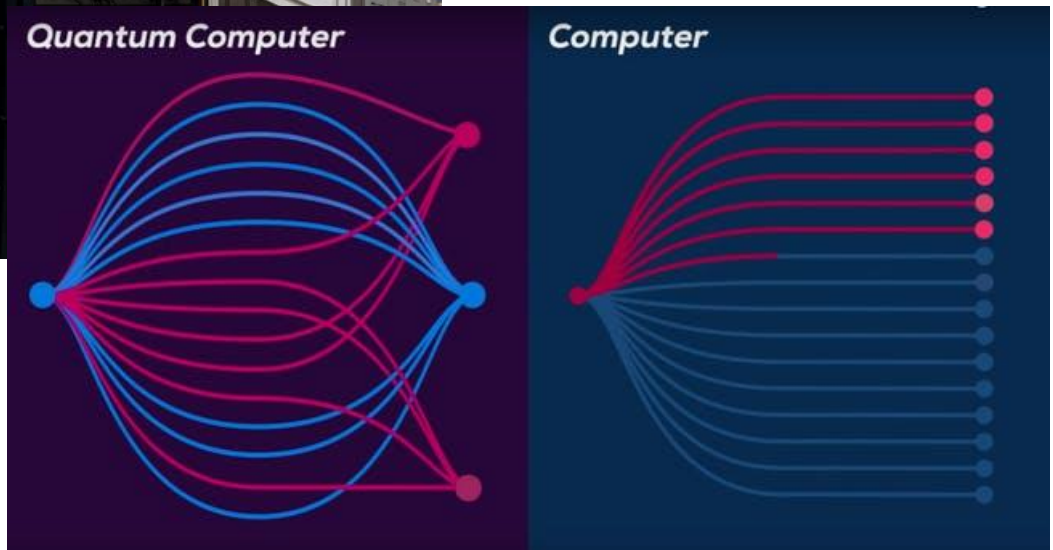
Qubit

<https://www.inverse.com/article/38860-quantum-computers-are-almost-here>

- A quantum bit (qubit) can exist in multiple states simultaneously!
- The number of states potentially grows with the number of qubits (2^N , N = number of Qubits)
- Example: A system with 16 qubits can be in $2^{16} = 65,536$ states at once



<https://www.japantimes.co.jp/news/2017/06/16/business/tech/quantum-computing-machines-tomorrow/>



<https://www.inverse.com/article/38860-quantum-computers-are-almost-here>



Pictures: [Unsplash](#)



GOVERNMENT

e.g. Support deep
cryptoanalysis of
critical data



PHARMACEUTICAL

e.g. Develop new drugs
and treatments



MANUFACTURING & INDUSTRIAL

e.g. Develop new
materials and processes



TELECOMMUNICATIONS

e.g. Enable secure communications
across networks



TRAVEL & TRANSPORTATION

e.g. Design new vehicles and
transport systems



FINANCIAL SERVICES

e.g. Predict market
trends and risks

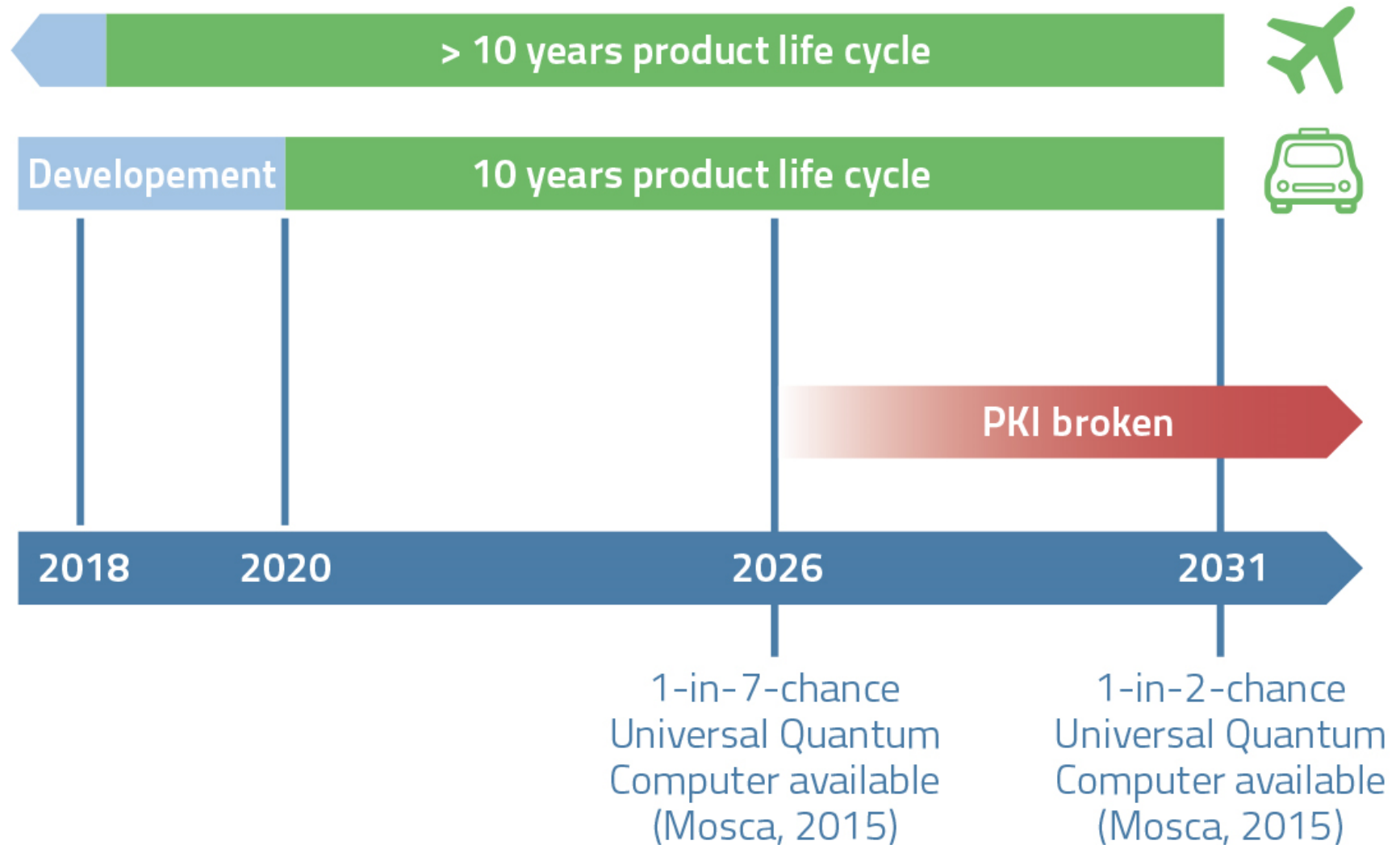
<https://www.ibm.com/thought-leadership/technology-market-research/quantum-computing-report.html>

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

Resource Estimates for Shor's Algorithm

Algorithm	#Qubits
RSA 1024	2050
RSA 2048	4098
ECC 256	2330
ECC 521	4719

Quelle: Roetteler, Martin et al. "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms." ASIACRYPT (2017).

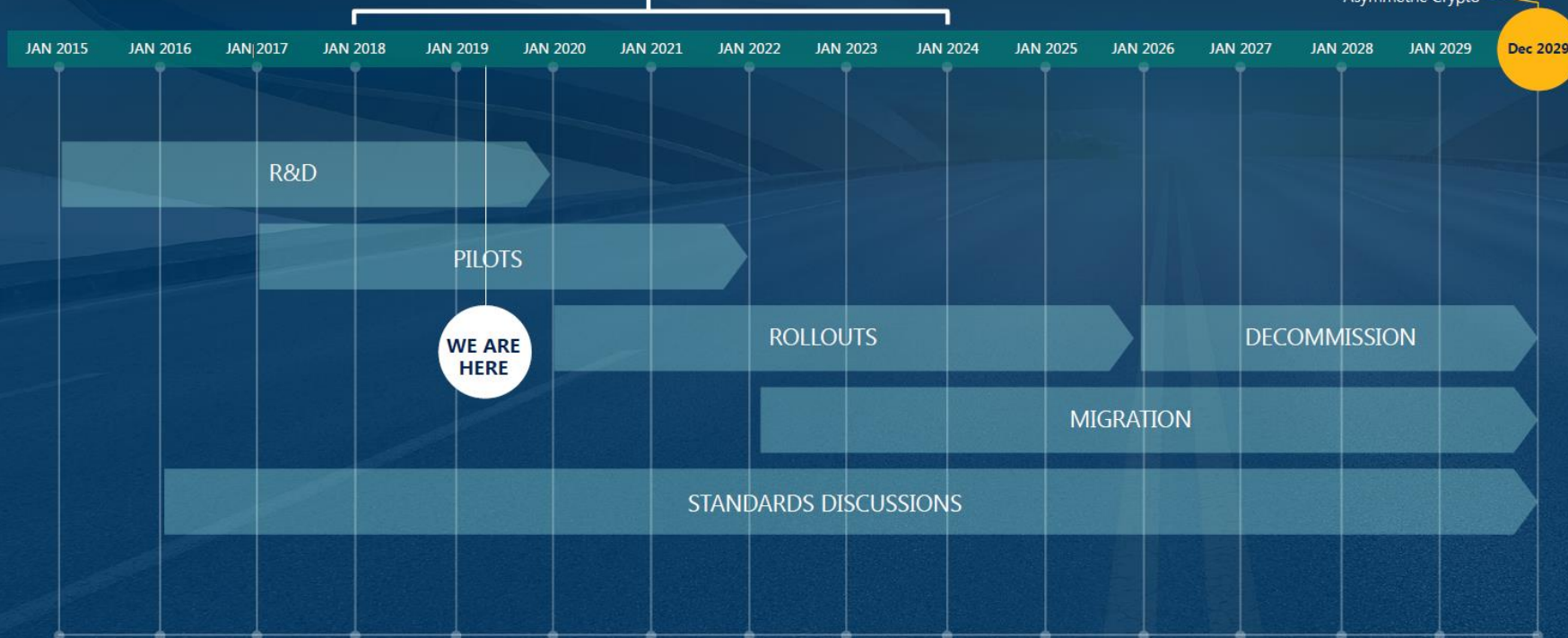


- NIST Post-Quantum Standardization Project
 - Goal: find algorithms based on different mathematical problems that are not vulnerable to known quantum attacks
 - Started on Nov 30, 2017 → finish in 2023
 - ~ 70 submissions from around the world
 - Primitives used:
 - code-based
 - lattice-based
 - hash-based
 - Multivariate
 - super singular elliptic-curve isogenies
 - NIST & crypto community now engaged in cryptanalysis
 - NIST expected to pick multiple “winning” algorithms
-
- Current Status: Round 2
 - 17 key encipherment (encryption) algorithms
 - 9 digital signature algorithms

Hypothetical 15-Year View for PQ Crypto

Dec 2017 – Dec 2023
NIST PQ Standardization Process

~ 2030
Quantum Computer Breaks
Asymmetric Crypto



https://hsm.utimaco.com/wp-content/uploads/2019/05/20190516-Utimaco-webinar-Post-Quantum-Cryptography_The-Perspective-of-Brian-LaMacchia_Microsoft-slides.pdf

„The ability for an IT system to gracefully and securely exchange crypto primitives, with minimum down-time, no migration periods, and complete visibility on used primitives.“

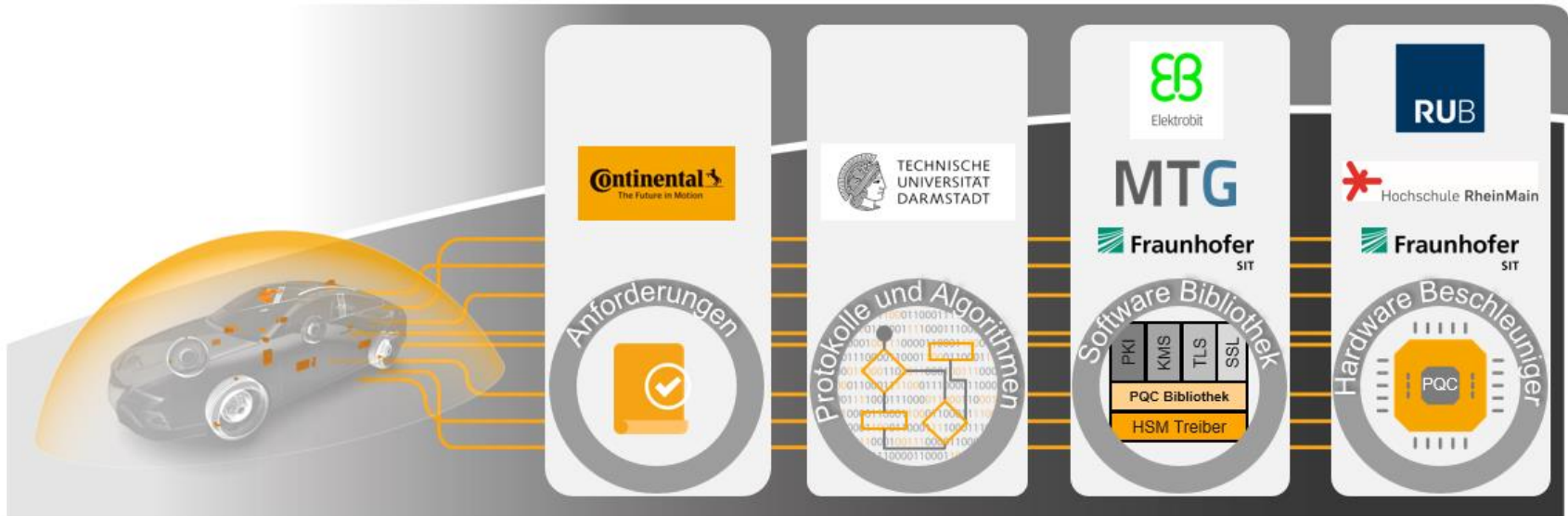


<https://cloakable.irdeto.com/2018/06/21/cryptographic-agility/>

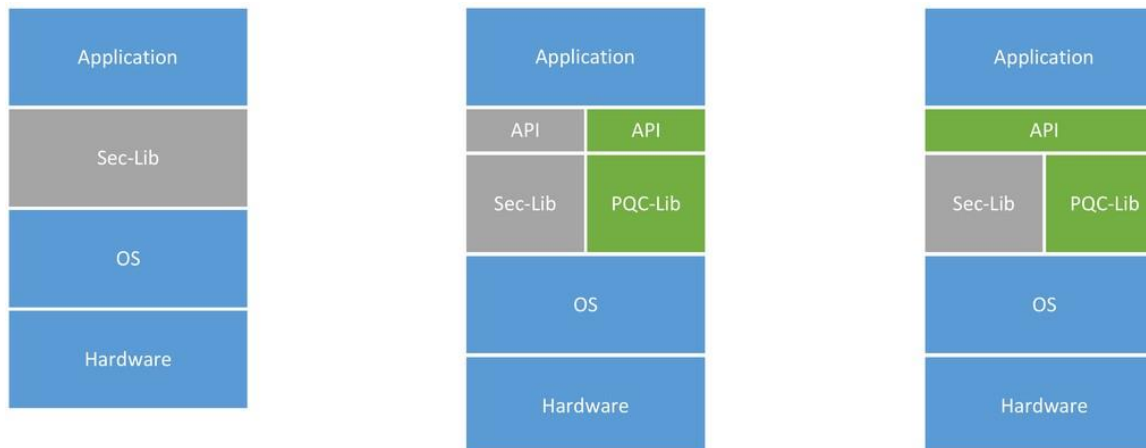
Why?

- Different PQC algorithms for different use cases
- Algorithms can be proven insecure
- New more effective/secure algorithms can be developed

QuantumRISC



Use-A-PQCLib



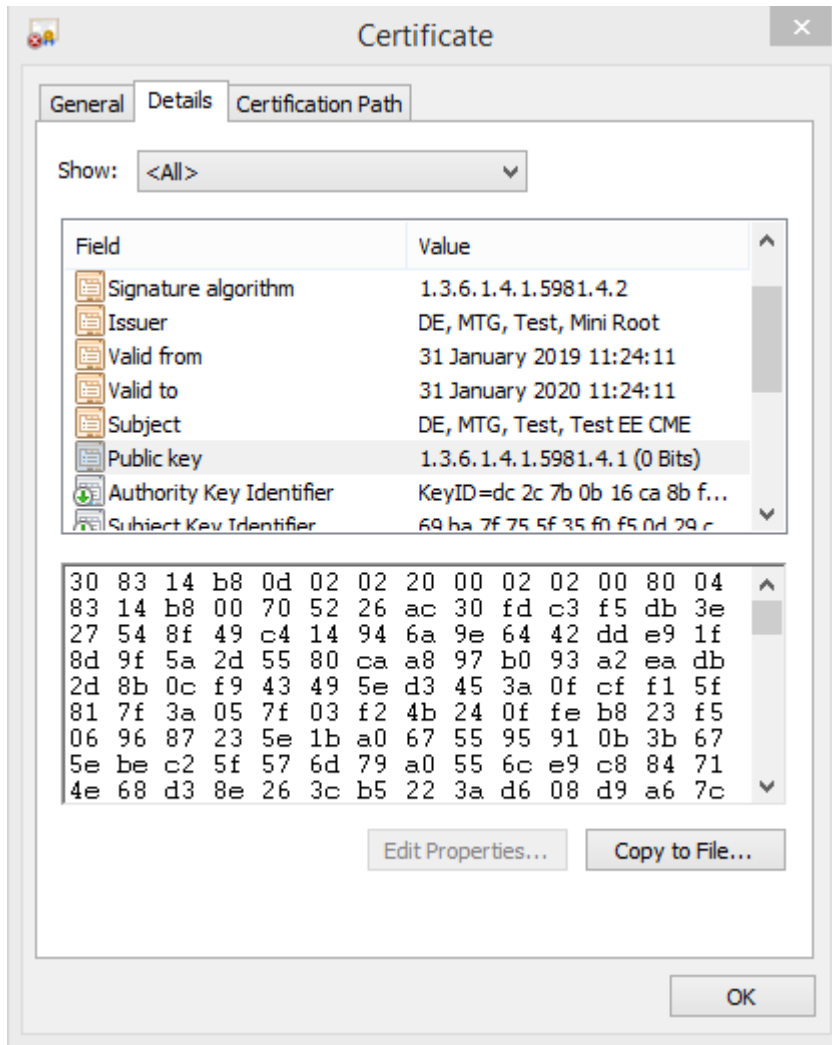
h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES



**Integrate
Post-Quantum
Cryptography now!**

Real World PQC Applications



- Classic McEliece Public Key
- Sphinx Plus Signature
- No standardized OIDs
- No standardized ASN1 Structures
- Most applications cannot handle:
 - Large key sizes (1,4 MB)
 - Large signature sizes (50 KB)

- No standardized PQC Algorithms
- No standardized encoding for keys and algorithm parameters
- Large key sizes (1,4 MB)
- Large signature sizes (50 KB)
- Keys and Certificates stored in databases...
- Existing software written with no flexibility in mind
- Restrictions through variable types...
- Communication overhead for large keys and certificates
- The whole system needs to use PQC (Webserver, Web browser, HSM, etc.)
- Many existing tools and solutions decide to wait for standards...



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](#)

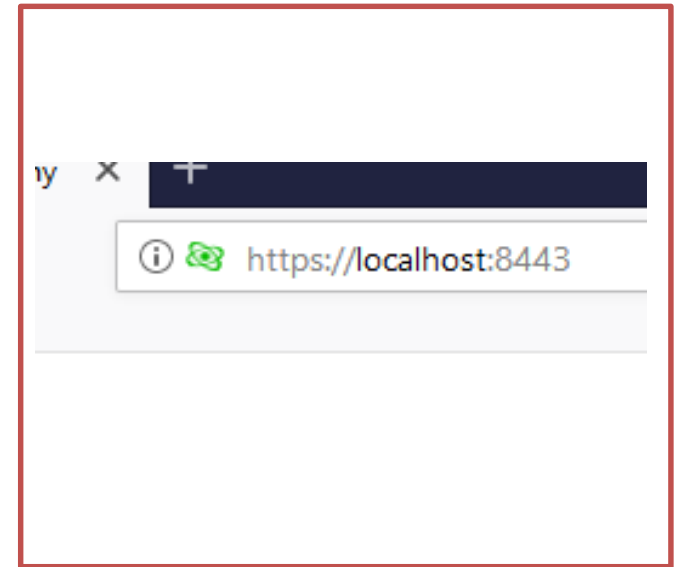
Technical Details

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](#)



Post-Quantum Cryptography X

MTG IT Security for Critical Infrastructures
Security Made in Germany

Quantum Computers Target Group Protection Hybrid Schemes Standardizations 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](#)



Get Messages Write Chat Address Book Tag

From pqc@mtg.de
Subject **Fist Post Quantum Secure Email!**
To pqc@mtg.de

Reply Forward More 10:37

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

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 Details

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:80:8F:08:E9:F1:C5:13:43:09:B3:79:0F:AD:7B:75:F0:89:D6:B8:7F: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

[Get Involved](#)

Don't just use the Daily release, help other use which means anyone can contribute ideas, dev team that creates Thunderbird.

- PQC transition must start today!
- There are new challenges and requirements!
- Most of today's IT infrastructures and systems are able to use PQC!
- What role could the European Bridge CA play in the adaptation of PQC?

Contact

Stathis Deligeorgopoulos

sdeligeorgopoulos@mtg.de

+ 49 6151 8000 40

