MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

Forschung am MPI-SP und ein kleiner Blick auf die Migration zur Post-Quanten Kryptographie

Peter Schwabe

26. September, 2024

MPI-SP: Basic Facts

Founded	2019
Location	Bochum
Mission	Our mission is to design, build, and analyze security and privacy technologies from foundations, through systems, to society
Intersectional	Operates under CPT and GSH sections
Faculty	6 Directors and 12 independent Research Group Leaders

MPI-SP: Basic Facts

Founded	2019
Location	Bochum
Mission	Our mission is to design, build, and analyze security and privacy technologies from foundations, through systems, to society
Intersectional	Operates under CPT and GSH sections
Faculty	6 Directors and 12 independent Research Group Leaders

MPI-SP Faculty

DIRECTORS

Gilles Barthe

Christof Paar

Peter Schwabe

Meeyoung Cha

Research Group Leaders

Asia Biega

Marcel Böhme

Catalin Hritcu

Yixin Zou

Jana Hofmann

Junior RGLs

Clara Schneidewind

Abraham Mhaidli

MPI-SP’s current research

- Data Science and AI
- Trustworthy Systems
- Formal Methods and Verification
- Privacy and Data Protection
- Societal Impacts of Technology
- Cryptography

MPI-SP's current research

Data Science and AI

- Cross-disciplinary partnerships
- Tackle, e.g., misinformation, bias, fraud, poverty, and disaster damage

Formal Methods and Verification

Societal Impacts of Technology

Trustworthy Systems

Privacy and Data Protection

Cryptography

MPI-SP's current research

Data Science and AI

Formal Methods and Verification

- Mathematical guarantees for properties of programs
- Secure compilation, smart contracts, . . .

Societal Impacts of Technology

Trustworthy Systems

Privacy and Data Protection

Cryptography

MPI-SP’s current research

Data Science and AI

Formal Methods and Verification

Societal Impacts of Technology

- Study impacts of socio-technical systems on individuals, organizations, and societies
- Uncover and mitigate harms of technology

Trustworthy Systems

Privacy and Data Protection

Cryptography

MPI-SP’s current research

Data Science and AI

Formal Methods and Verification

Societal Impacts of Technology

Trustworthy Systems

- Examine the security of existing technologies
- Design and build secure computer systems

Privacy and Data Protection

Cryptography

MPI-SP's current research

Data Science and AI

Formal Methods and Verification

Societal Impacts of Technology

Trustworthy Systems

Privacy and Data Protection

- Computationally operationalize principles of data protection
- Embed end-users' privacy needs in the development of systems

Cryptography

MPI-SP's current research

Data Science and AI

Formal Methods and Verification

Societal Impacts of Technology

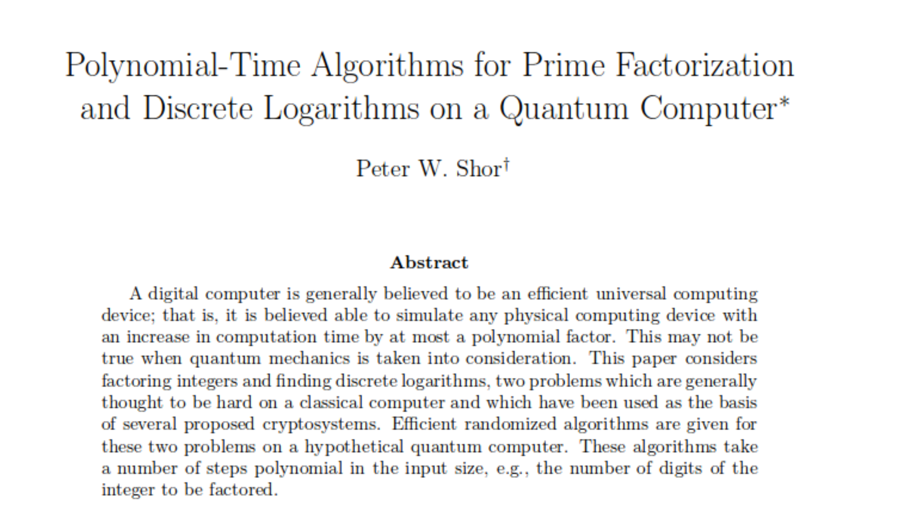
Trustworthy Systems

Privacy and Data Protection

Cryptography

- High-assurance cryptography
- Post-quantum cryptography

[A small demo]

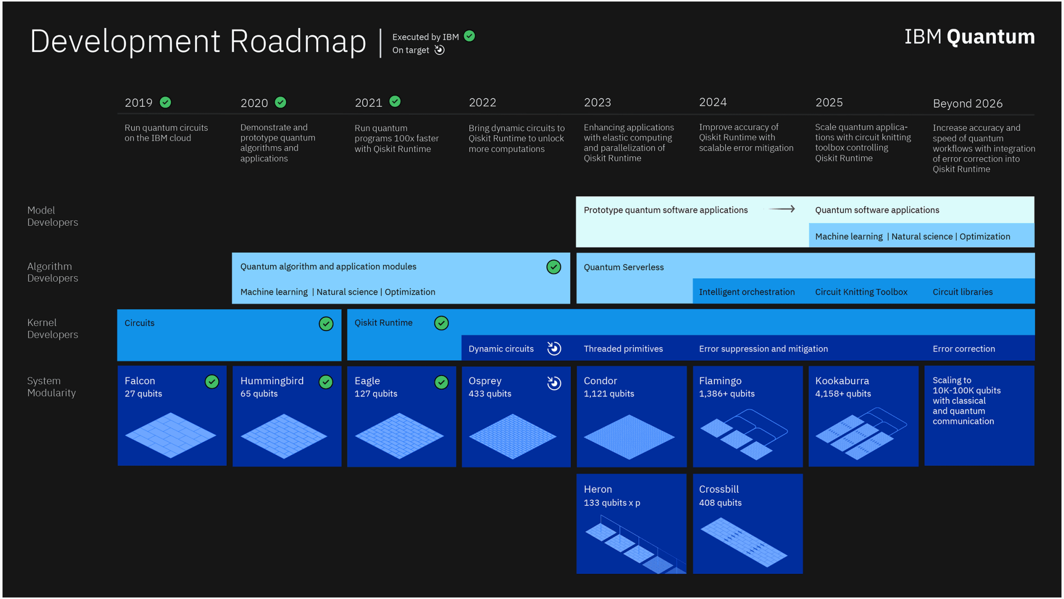


Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.



Development Roadmap | Executed by IBM ✓ On target ↻

IBM **Quantum**

	2019 ✓	2020 ✓	2021 ✓	2022	2023	2024	2025	Beyond 2026
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum software applications →		Quantum software applications Machine learning | Natural science | Optimization	
Algorithm Developers		Quantum algorithm and application modules ✓ Machine learning | Natural science | Optimization			Quantum Serverless	Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits ✓		Qiskit Runtime ✓	Dynamic circuits ↻	Threaded primitives	Error suppression and mitigation		Error correction
System Modularity	Falcon ✓ 27 qubits	Hummingbird ✓ 65 qubits	Eagle ✓ 127 qubits	Osprey ↻ 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron 133 qubits x p	Crossbill 408 qubits		

See **https://www.ibm.com/quantum/blog/ibm-quantum-roadmap-2025**

Post-quantum crypto

Definition

Post-quantum crypto is (asymmetric) crypto that resists attacks using classical *and quantum* computers.

Post-quantum crypto

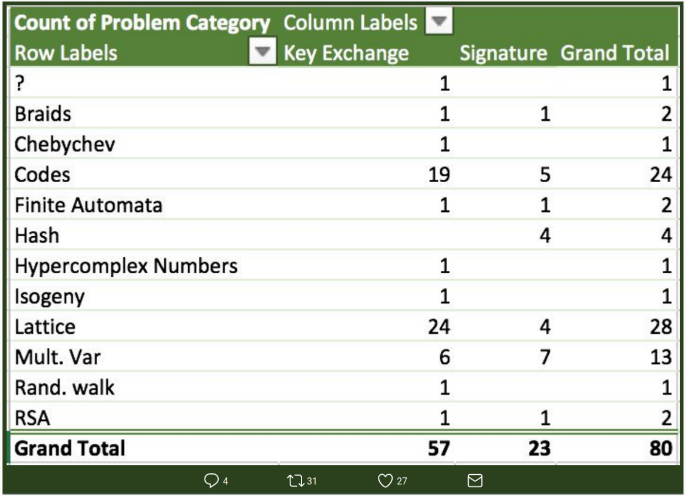
Definition

Post-quantum crypto is (asymmetric) crypto that resists attacks using classical *and quantum* computers.

5 main directions

- Lattice-based crypto (PKE and Sigs)
- Code-based crypto (mainly PKE)
- Multivariate-based crypto (mainly Sigs)
- Hash-based signatures (only Sigs)
- Isogeny-based crypto (it's complicated. . .)

NIST PQC – how it started (Nov. 2017)

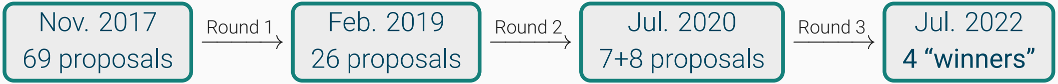


Count of Problem Category	Column Labels		
Row Labels	Key Exchange	Signature	Grand Total
?	1		1
Braids	1	1	2
Chebychev	1		1
Codes	19	5	24
Finite Automata	1	1	2
Hash		4	4
Hypercomplex Numbers	1		1
Isogeny	1		1
Lattice	24	4	28
Mult. Var	6	7	13
Rand. walk	1		1
RSA	1	1	2
Grand Total	**57**	**23**	**80**

Overview tweeted by Jacob Alperin-Sheriff on Dec 4, 2017.

NIST PQC – how it went

NIST PQC



Nov. 2017
69 proposals

Round 1

Feb. 2019
26 proposals

Round 2

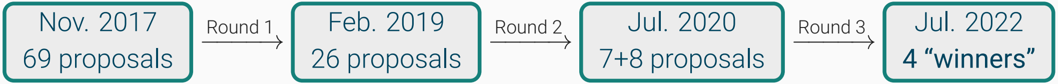
Jul. 2020
7+8 proposals

Round 3

Jul. 2022
4 “winners”

NIST PQC – how it went

NIST PQC



Nov. 2017
69 proposals

Round 1

Feb. 2019
26 proposals

Round 2

Jul. 2020
7+8 proposals

Round 3

Jul. 2022
4 “winners”

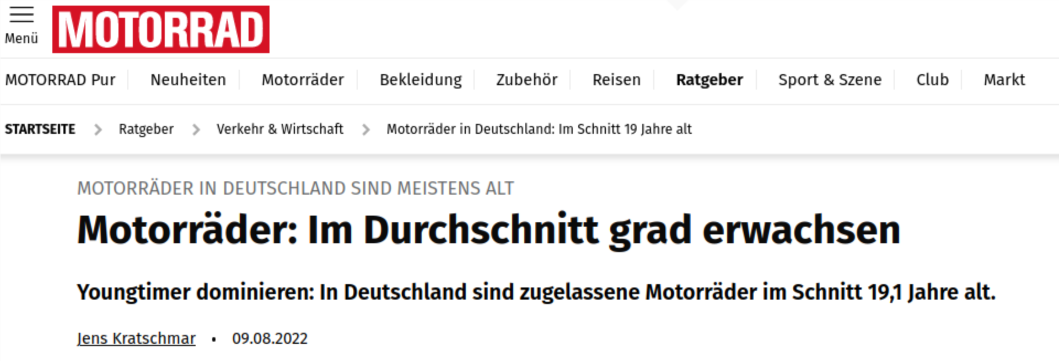
> *“The public-key encryption and key-establishment algorithm that will be standardized is* ***CRYSTALS-KYBER****. The digital signatures that will be standardized are CRYSTALS-Dilithium, FALCON, and SPHINCS*$^+$*. While there are multiple signature algorithms selected, NIST recommends* ***CRYSTALS-Dilithium*** *as the primary algorithm to be implemented”*
>
> —NIST IR 8413-upd1

Should you care now?

“Store now, decrypt later”

https://en.wikipedia.org/wiki/Utah_Data_Center#/media/File:EFF_photograph_of_NSA's_Utah_Data_Center.jpg

Should you care now? (part II)



MOTORRÄDER IN DEUTSCHLAND SIND MEISTENS ALT

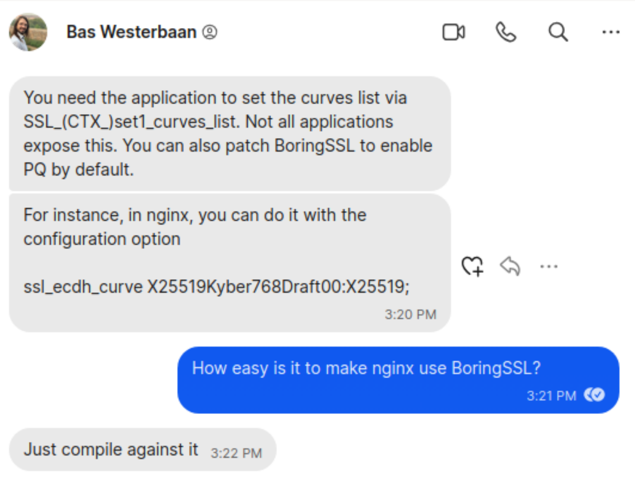
Motorräder: Im Durchschnitt grad erwachsen

Youngtimer dominieren: In Deutschland sind zugelassene Motorräder im Schnitt 19,1 Jahre alt.

Jens Kratschmar • 09.08.2022

[Back to our demo]

Start “playing” with PQC



Bas Westerbaan

You need the application to set the curves list via SSL_(CTX_)set1_curves_list. Not all applications expose this. You can also patch BoringSSL to enable PQ by default.

For instance, in nginx, you can do it with the configuration option

ssl_ecdh_curve X25519Kyber768Draft00:X25519;

3:20 PM

How easy is it to make nginx use BoringSSL?

3:21 PM

Just compile against it 3:22 PM

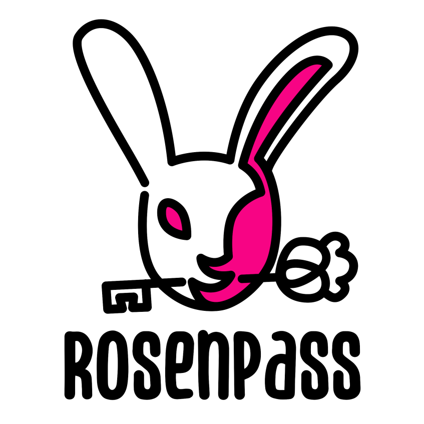
Start “playing” with PQC

Alternative: Use post-quantum Caddy:

https://gist.github.com/bwesterb/2f7bfa7ae689de0d242b56ea3ecac424

See also https://blog.cloudflare.com/pq-2024/

Start “playing” with PQC



Post-quantum VPN on top of WireGuard

https://rosenpass.eu