Post-Quantum Cryptography & DNSSEC

CENTR workshop| Frankfurt

8 Oct 2024

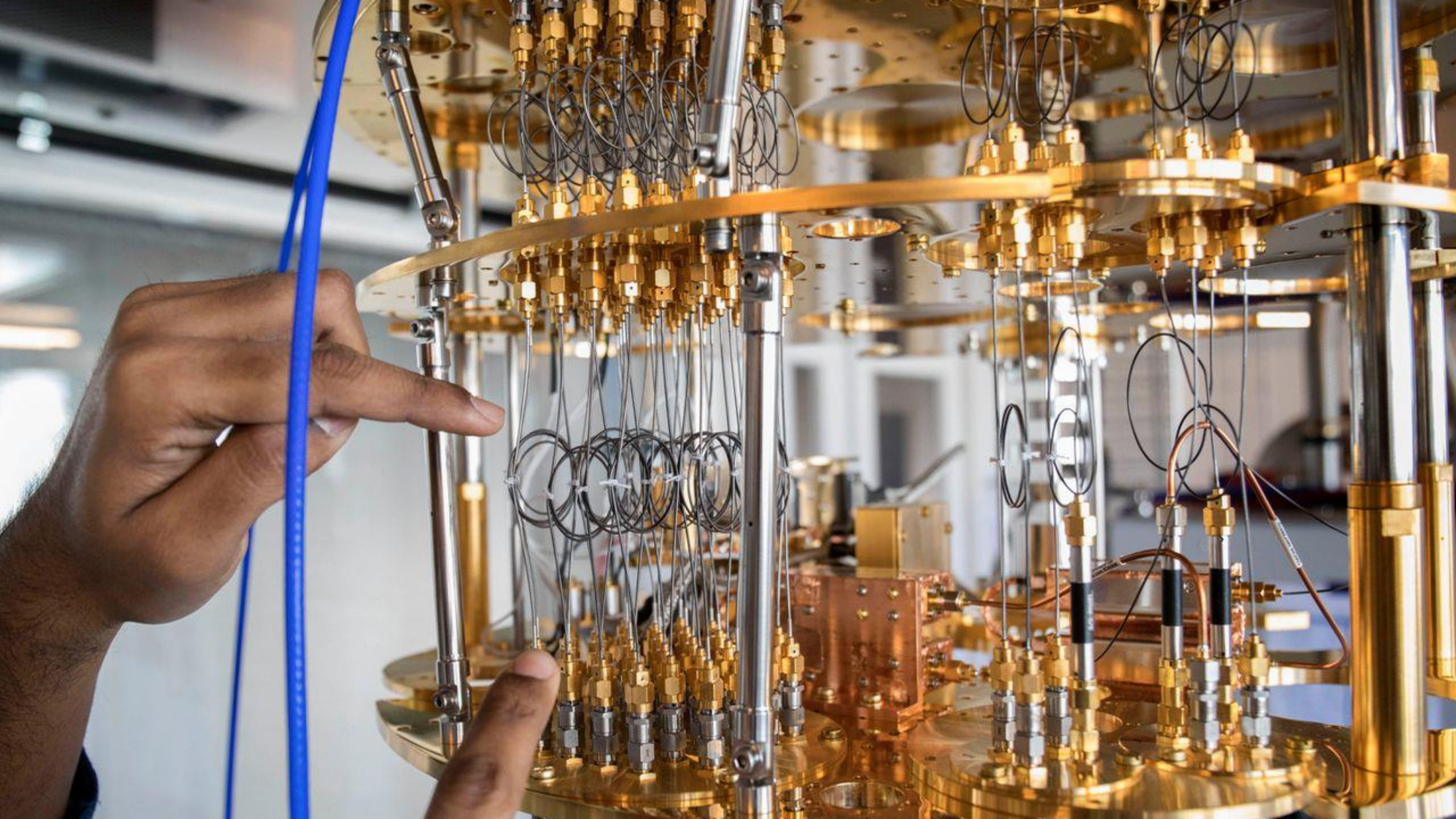
Agenda

1. Introduction to PQC (optional?)

2. PQC measurements for DNSSEC

3. Open discussion

Introduction



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

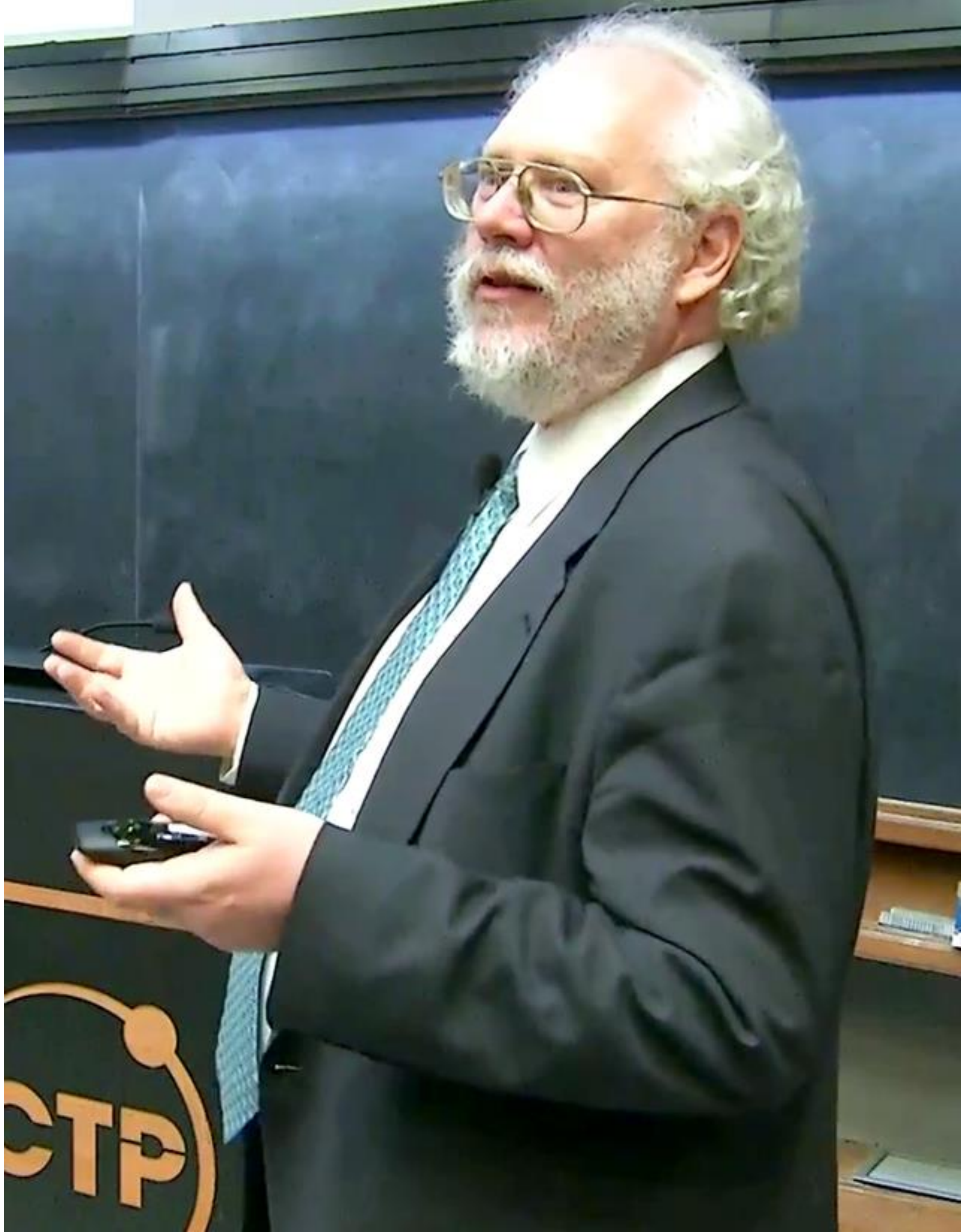
Peter W. Shor†

Abstract

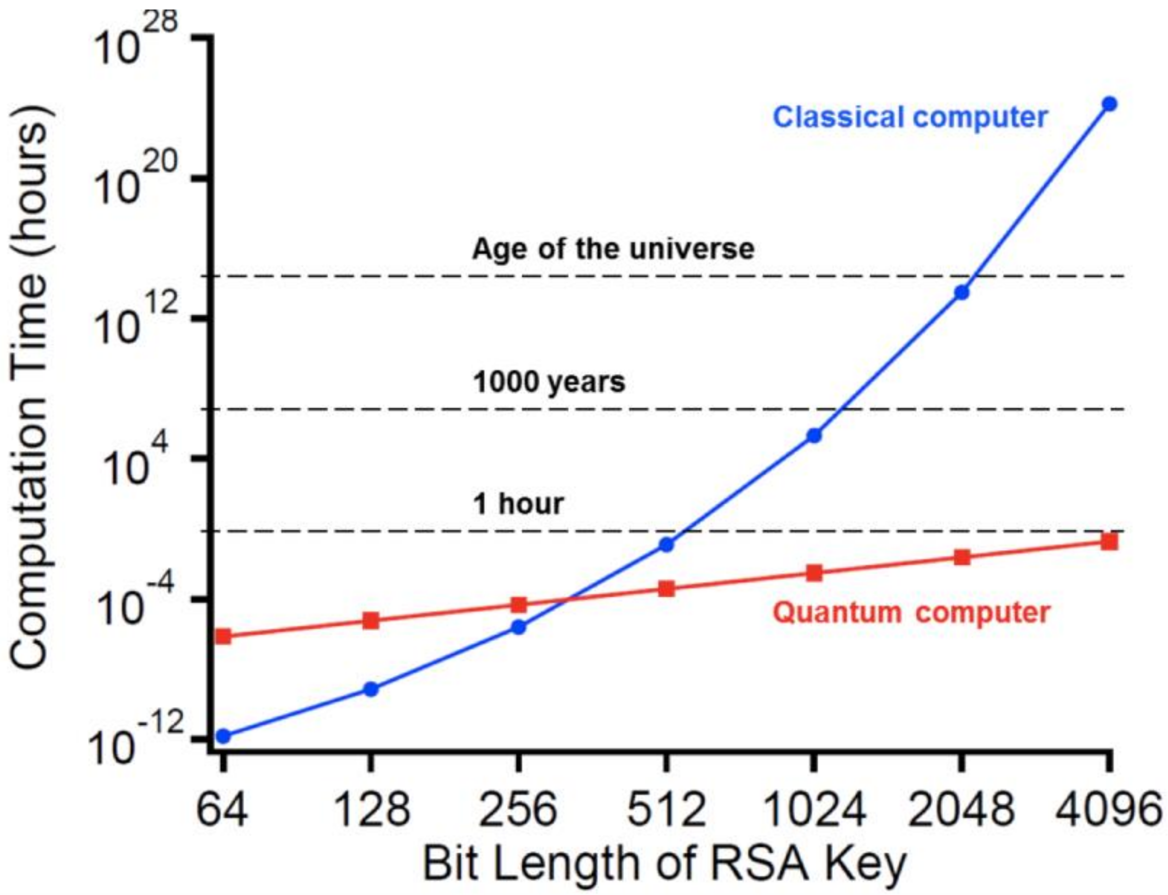
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. 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.

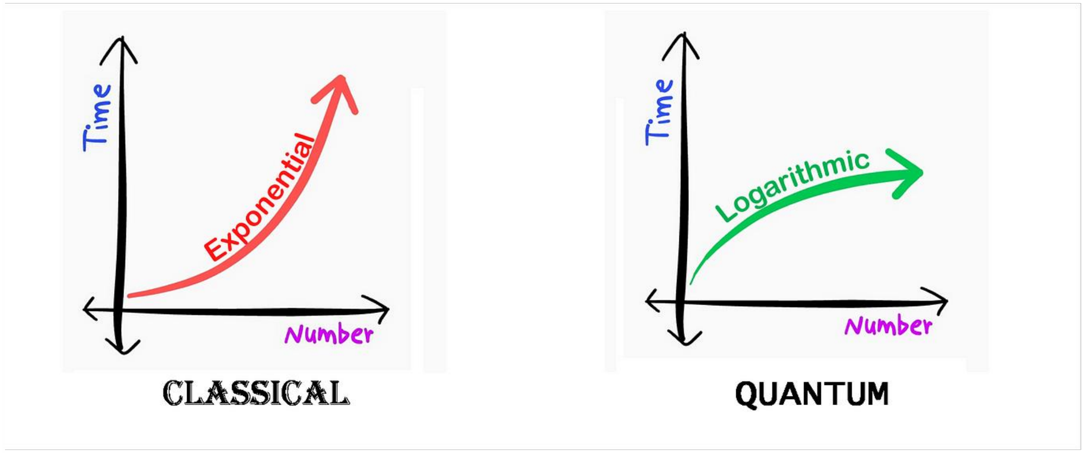
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

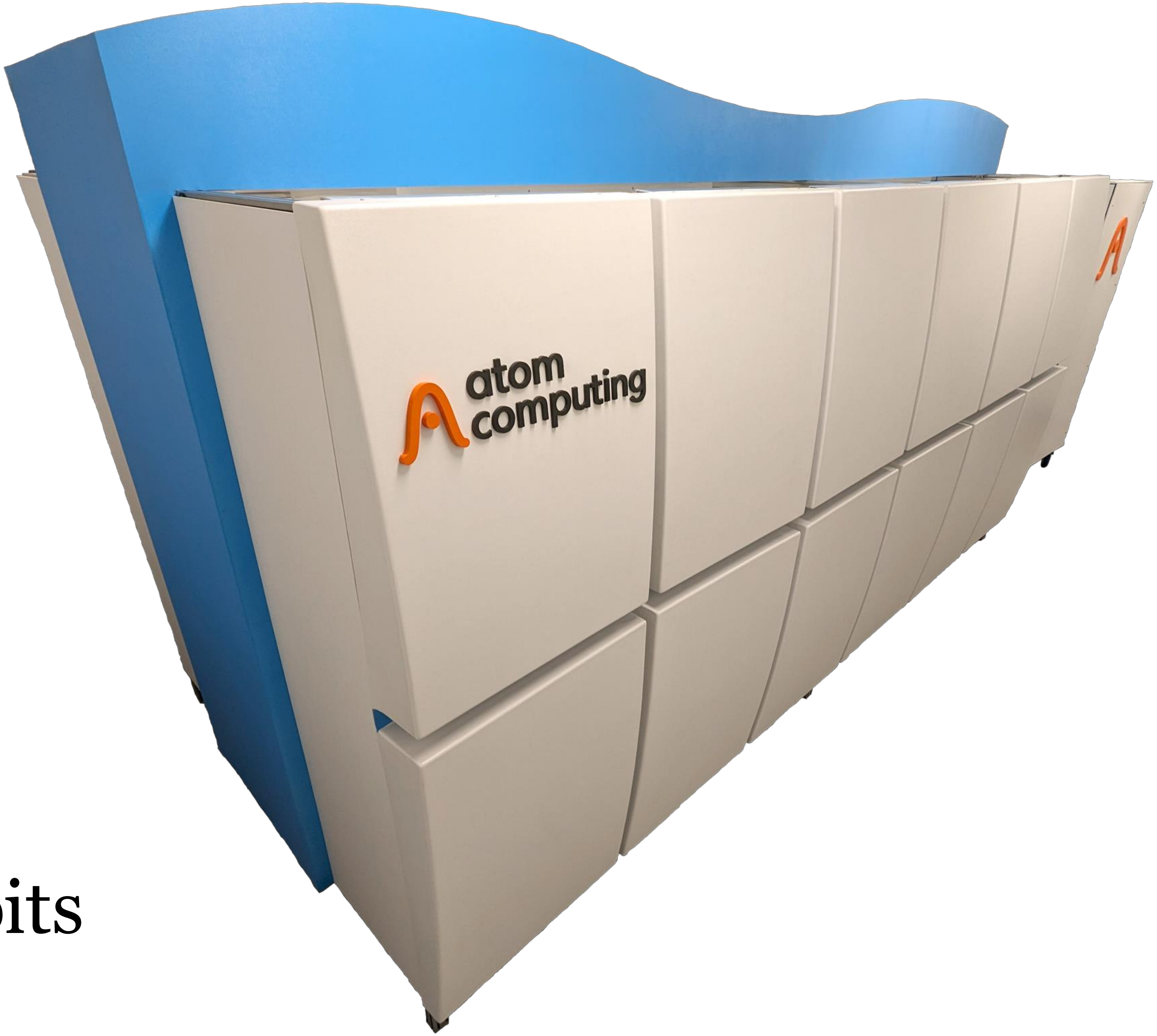
AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10



Quantumcomputers and Cryptographic keys







1180 qubits

Algorithm	Key size	Security	Logical qubits	Physical qubits	Time to break
RSA	1024 bits	80 bits	2.290	~ 2.560.000 bits	3.5 hours
RSA	**2048 bits**	**112 bits**	**4.338**	**~ 6.200.000 bits**	**29 hours**
RSA	4096 bits	128 bits	8.434	~ 14.700.000 bits	10 days
ECC	256 bits	128 bits	2.330	~ 3.210.000 bits	11 hours

Source: National Academies of Sciences, Engineering, and Medicine 2018. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196. Tabel 4.1

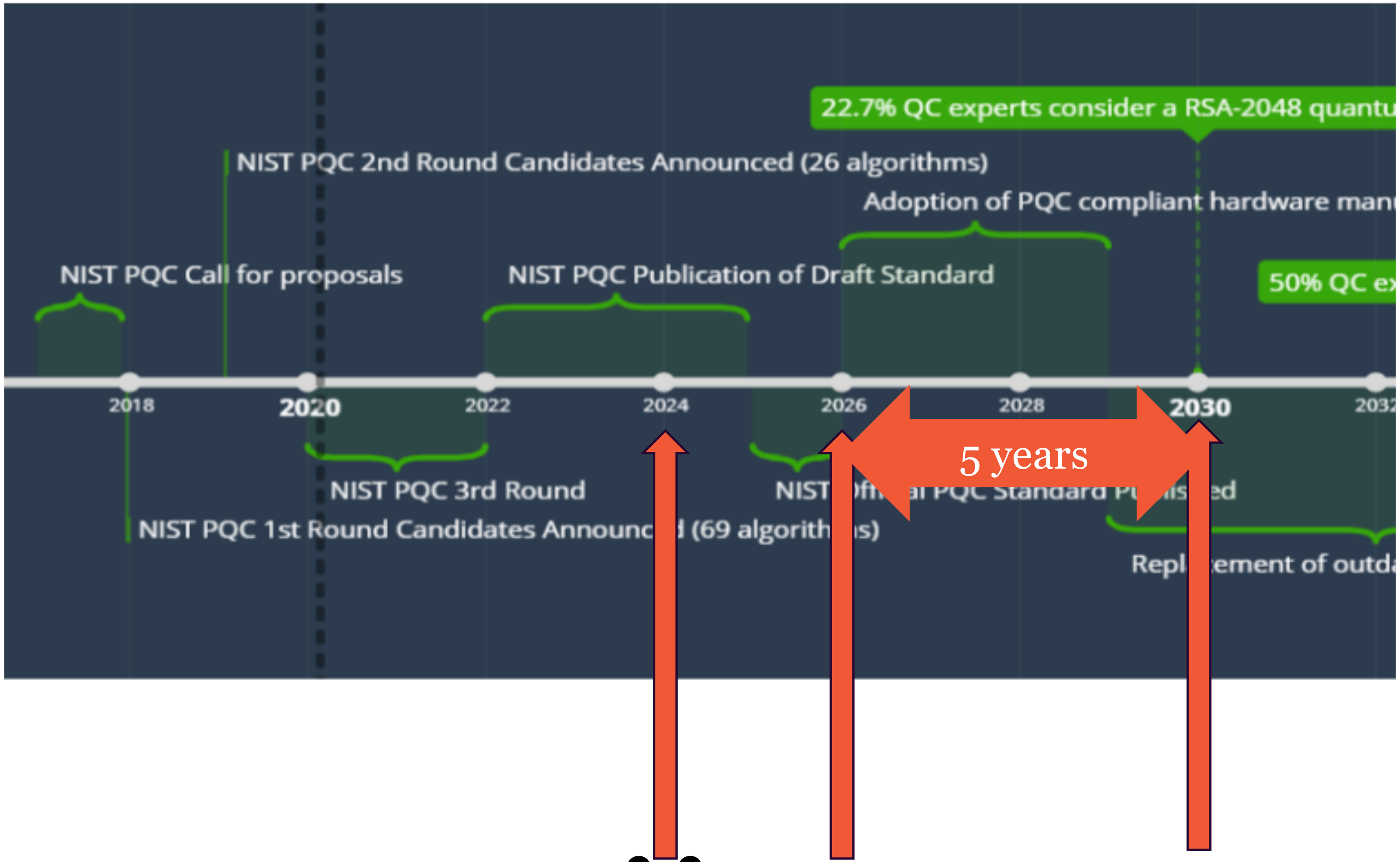
SIDN LABS

DoH, DoT, DNScrypt
https://dns4all.eu/

X25519Kyber768

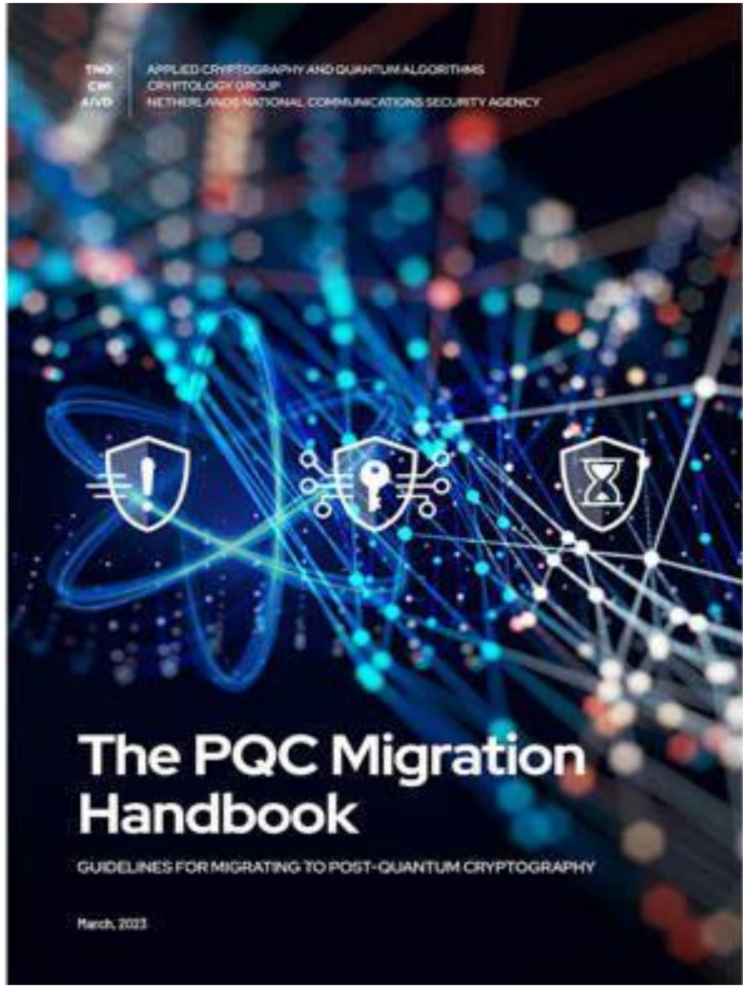
DNSSEC

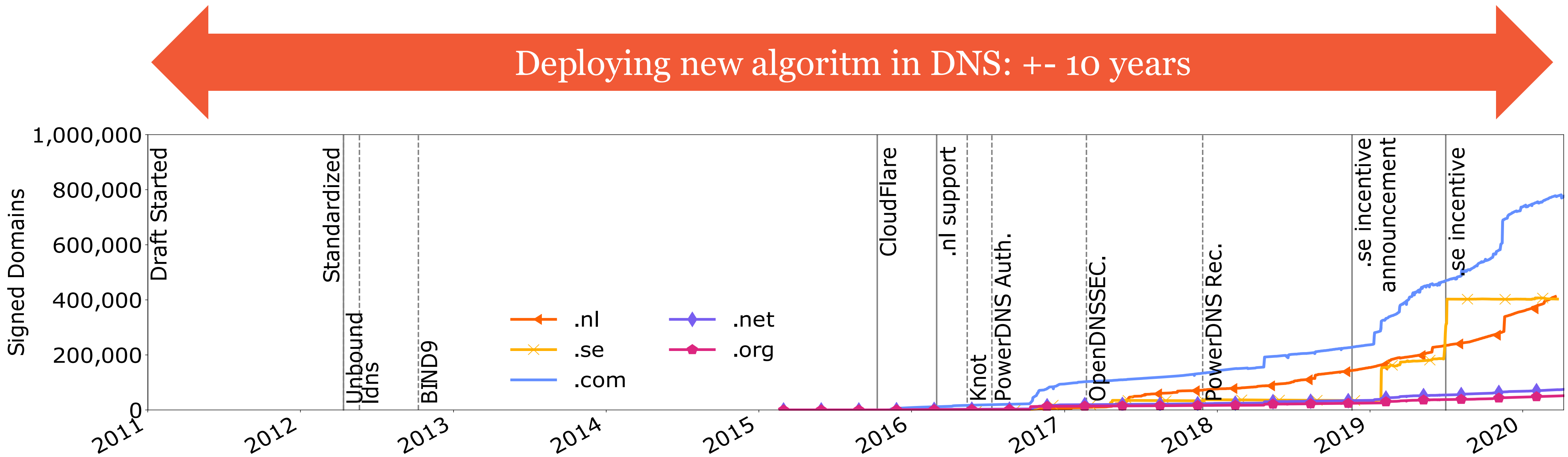
SIDN LABS



Standards for
PQC available

DNSSEC (possibly) vulnerable





Timeline deployment ECDSA256 from
‘*Making DNSSEC Future Proof*’ by dr. Moritz Müller.

SIDN LABS

Prio	Requirement	Good	Accepted Conditionally
#1	Signature Size	$\leq$ 1,232 bytes	—
#2	Validation Speed	$\geq$ 1,000 sig/s	—
#3	Key Size	$\leq$ 64 kilobytes	$>$ 64 kilobytes
#4	Signing Speed	$\geq$ 100 sig/s	—

Table 2: Requirements for quantum-safe algorithms.

M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

SIDN LABS

Jürgen Henn – 11foot8.com


gifbin.com

PQC measurements

Scheme	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig
EdDSA 🧨	Ed25519	Pre-Q	32	64	96
MAYO	two	1	5,488	180	5,668
RSA 🧨	2048	Pre-Q	272	256	528
SNOVA	(24, 5, 16, 4)	1	1,016	248	1,264
SNOVA	(25, 8, 16, 3)	1	2,320	165	2,485
SNOVA	(28, 17, 16, 2)	1	9,842	106	9,948
SQIsign	I	1	64	177	241
VOX	128	1	9,104	102	9,206

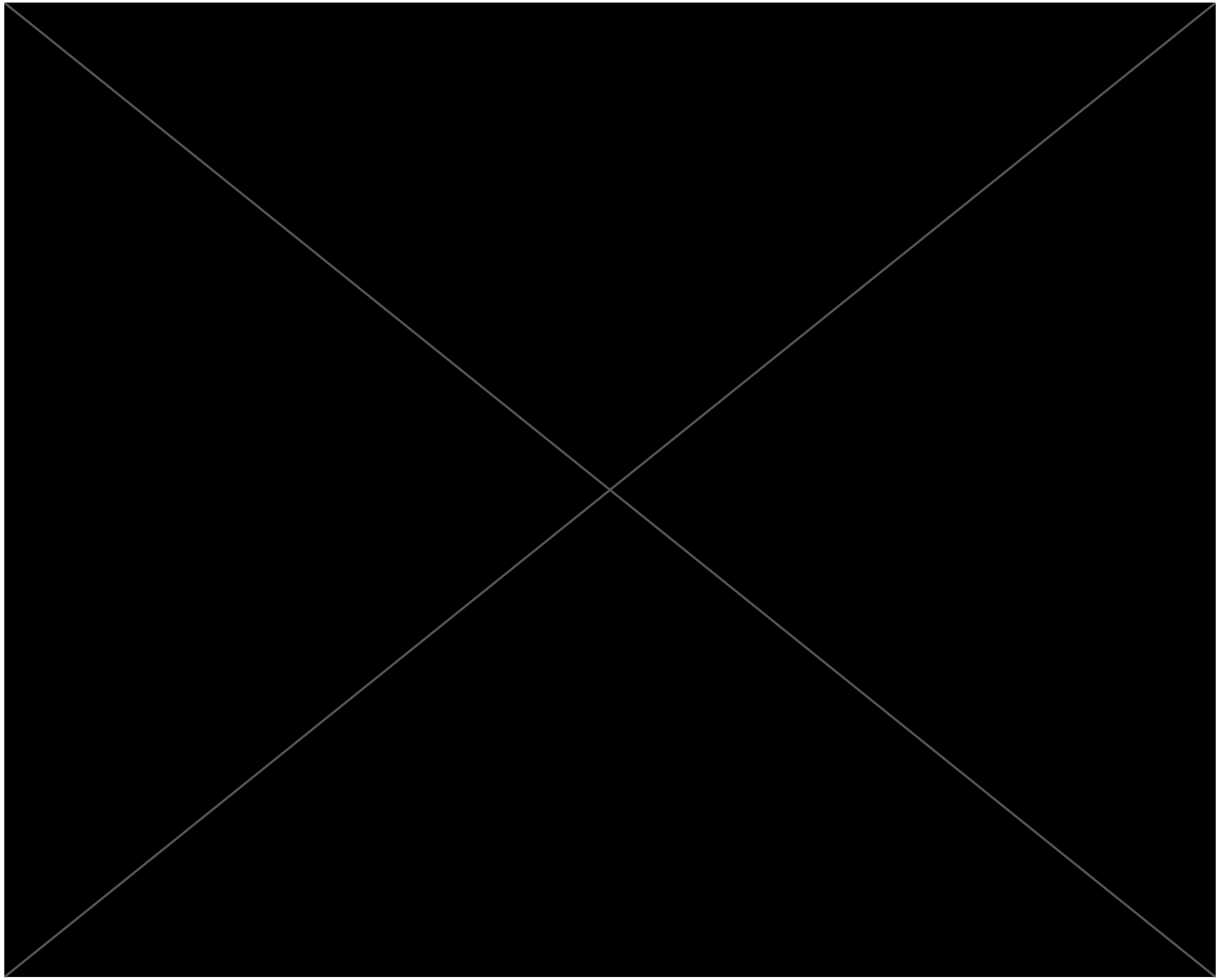
https://pqshield.github.io/nist-sigs-zoo

Scheme	Parameterset	NIST level	Sign (cycles)	Verify (cycles)
EdDSA ⚠️	Ed25519	Pre-Q	42,000	130,000
MAYO	two	1	563,900	91,512
RSA ⚠️	2048	Pre-Q	27,000,000	45,000
SNOVA	(24, 5, 16, 4)	1	19,681,409	8,086,815
SNOVA	(25, 8, 16, 3)	1	12,408,096	3,959,869
SNOVA	(28, 17, 16, 2)	1	10,964,945	3,161,199
SQIsign	I	1	5,669,000,000	108,000,000
VOX	128	1	664,265	168,567

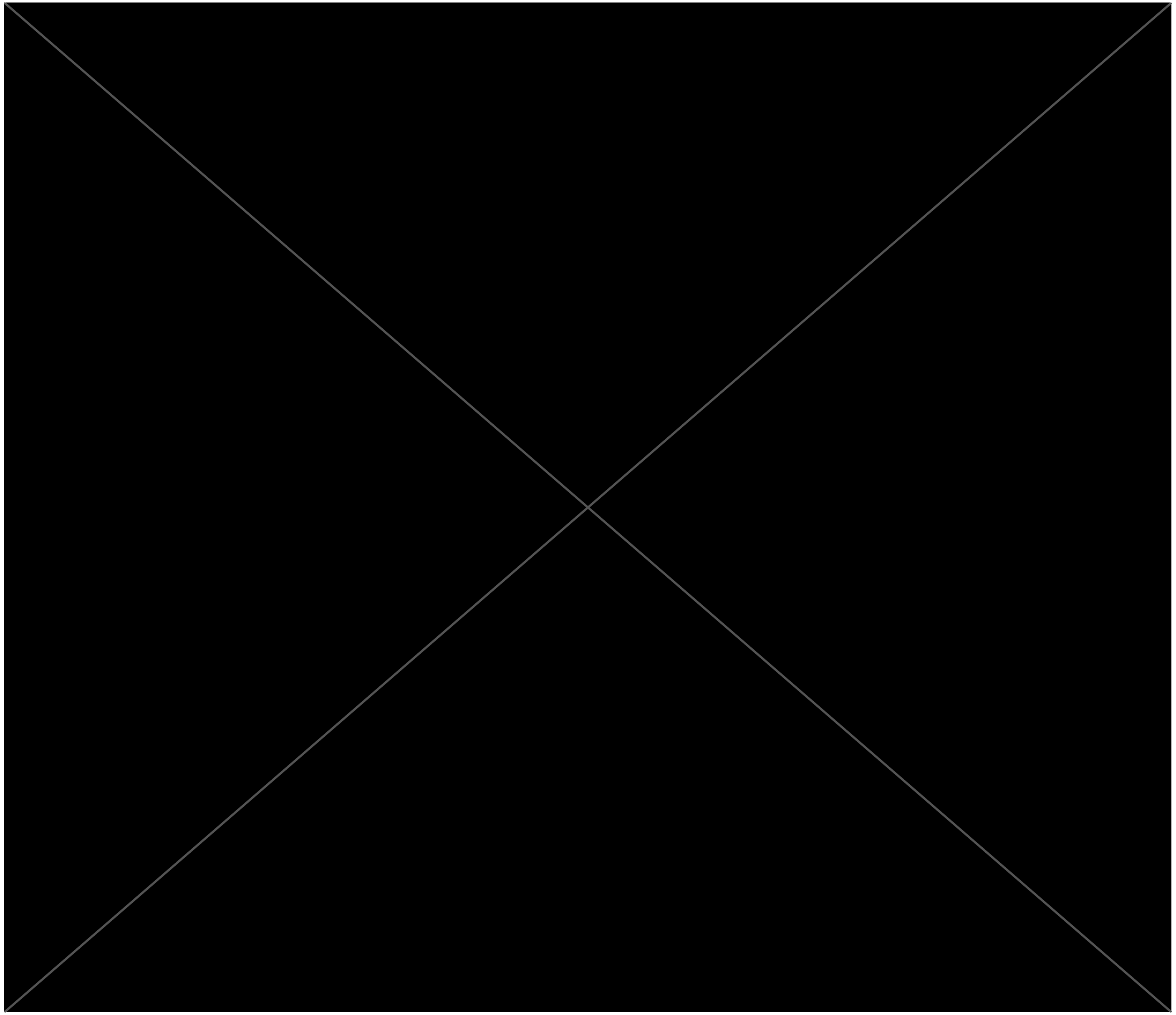
https://pqshield.github.io/nist-sigs-zoo

SIDN LABS

Signing time for entire .nl zone



.nl zone size



Open discussion

SIDN LABS

Open discussion

Some ideas:

1. Signing policies: offline/online
2. Signing policies: interval (e.g., every 30 minutes)
3. Why decide to switch to algo 13 for example? So what needed to switch again to PQC?
4. Sizes/performance back to algo 8 (~ RSA 2048).
   a) Any problems you had with algo 8 in terms of performance?
   b) More TCP?

Open discussion (2)

5. Running PQC testbed yourself

6. Impact van PQC on your services?

Follow us

.nl SIDN.nl

@SIDN

in SIDN

Thank you for your time!

SIDN LABS