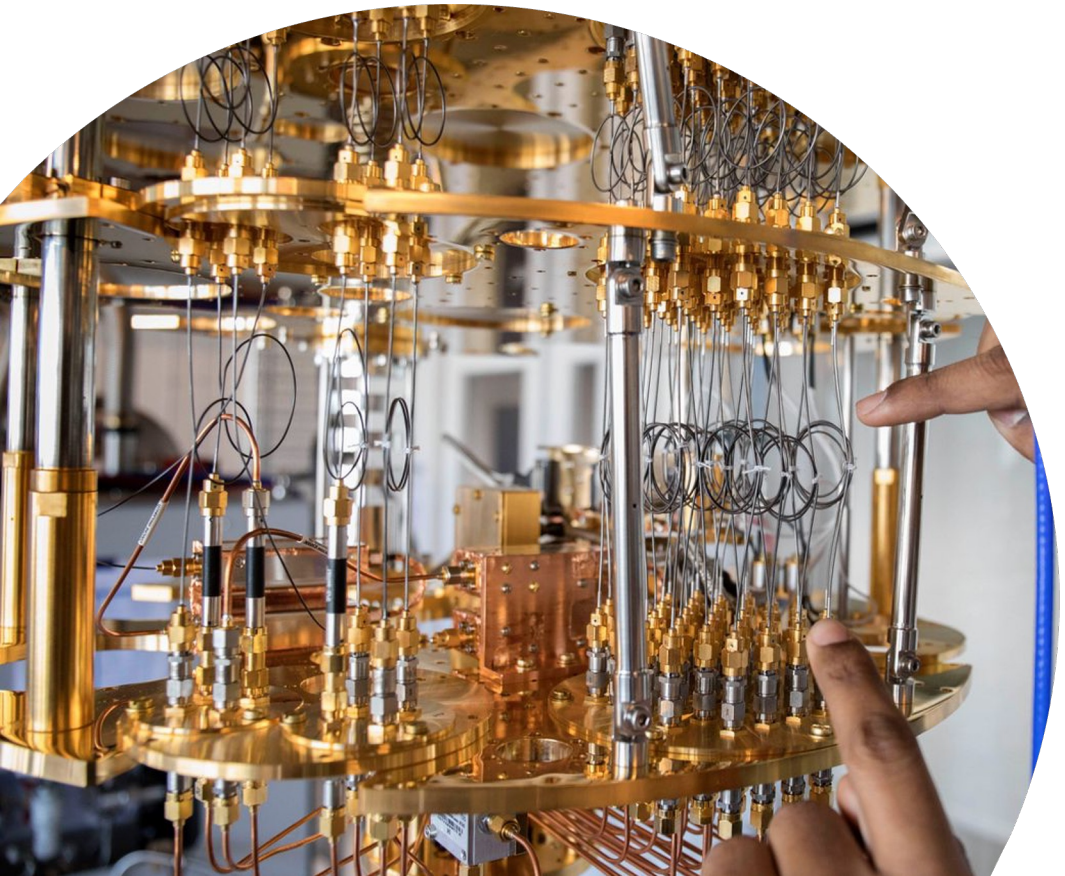
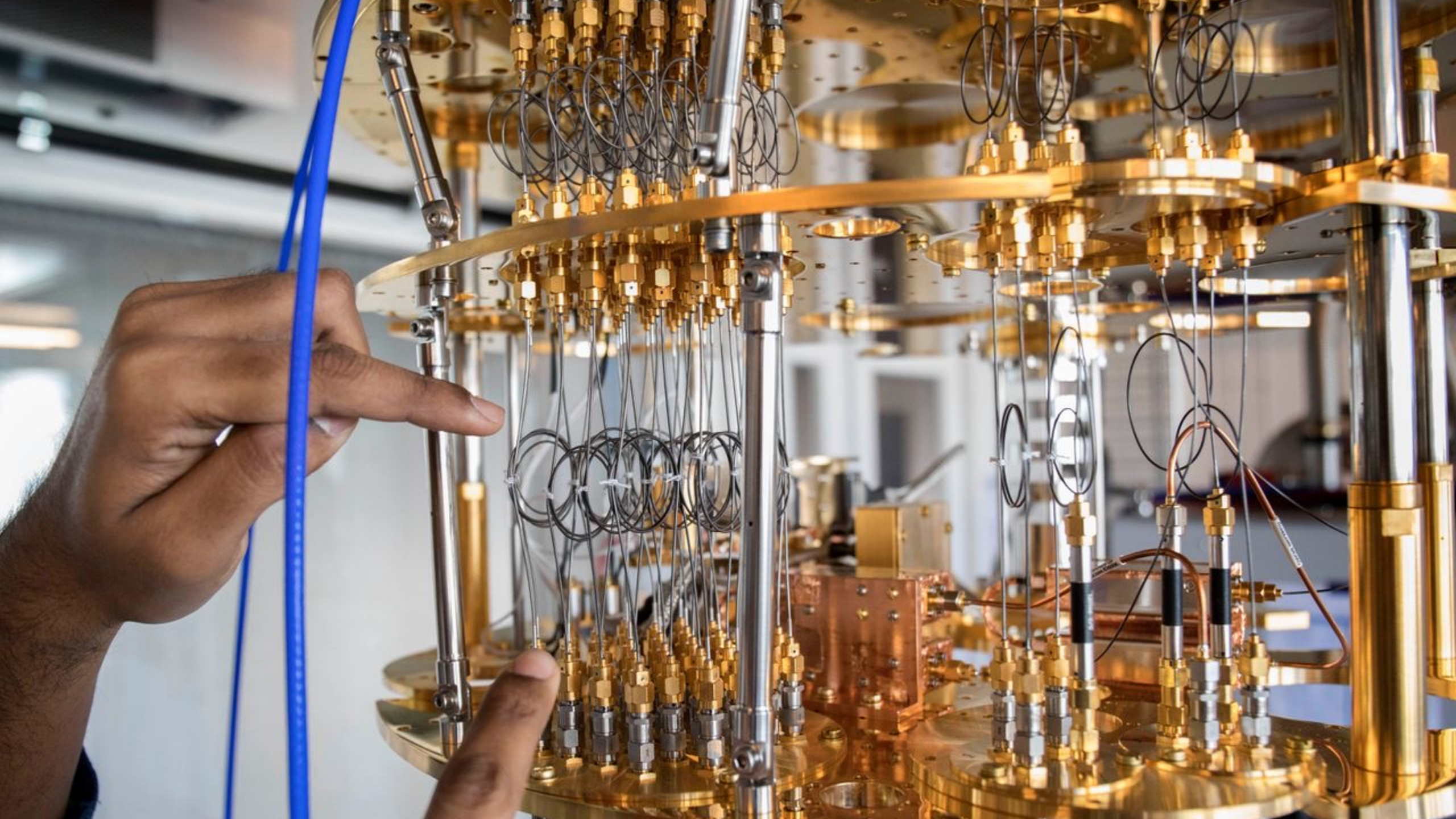


Een testbed om post-kwantumalgoritmes voor DNS te evalueren

Elmer Lastdrager

16 mei 2024


KWANTUM
KWANTUM
MUTMAWKI
MUTMAWKI



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

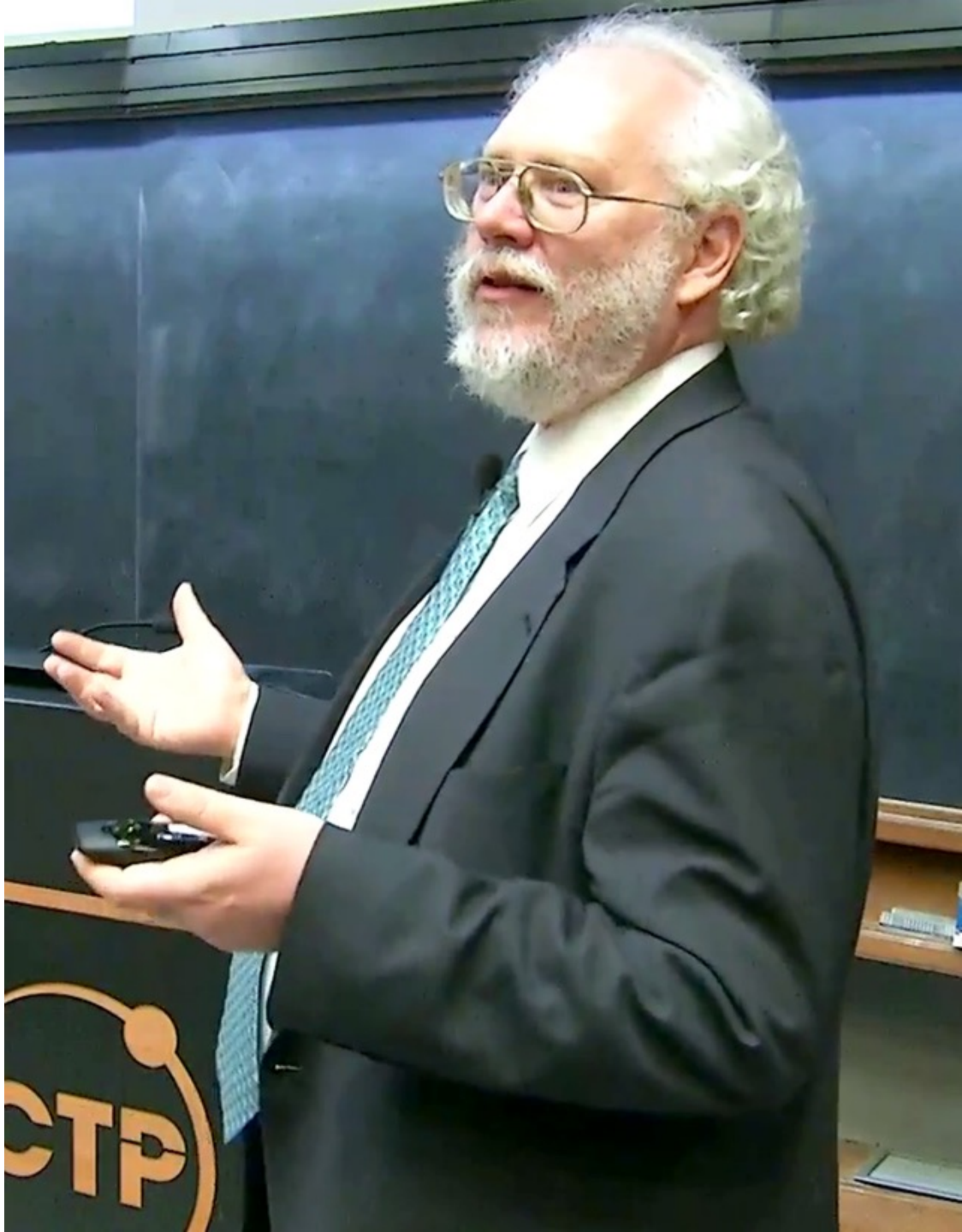
Peter W. Shor†

Abstract

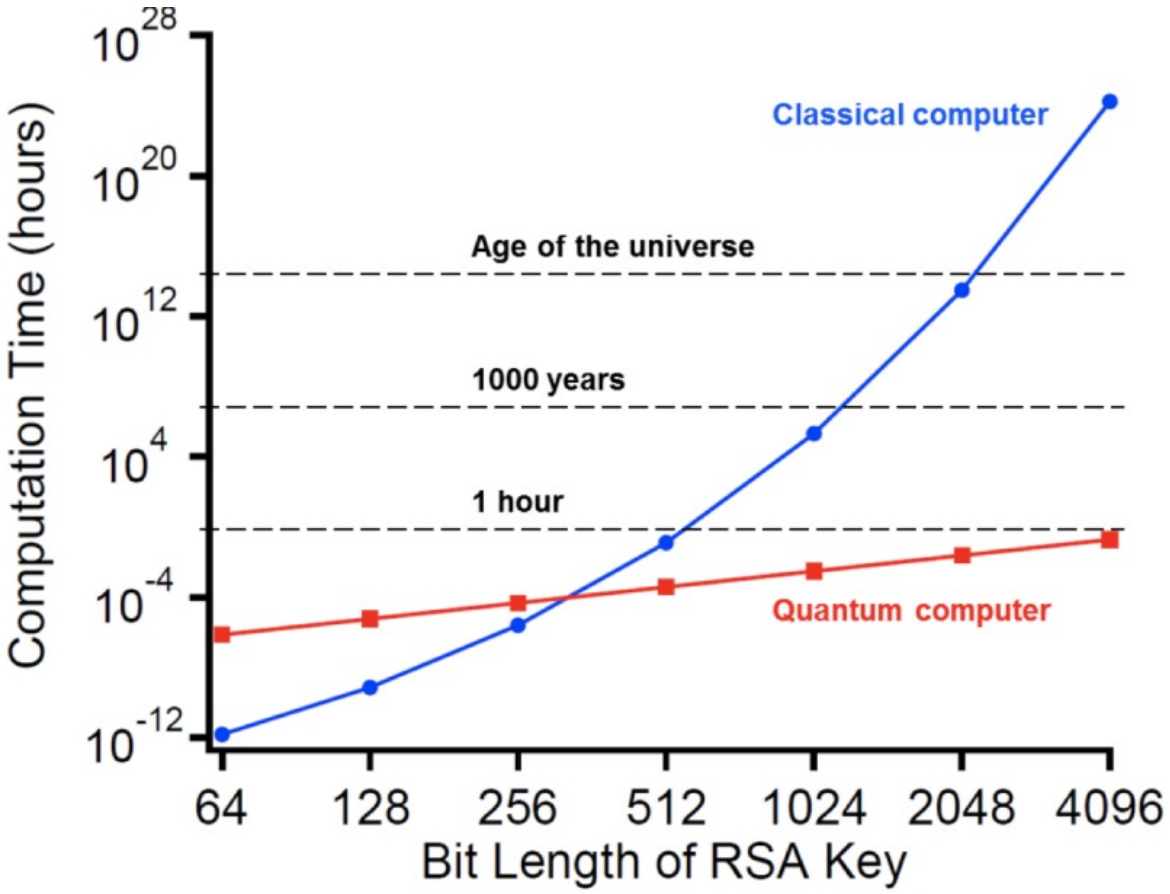
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration.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

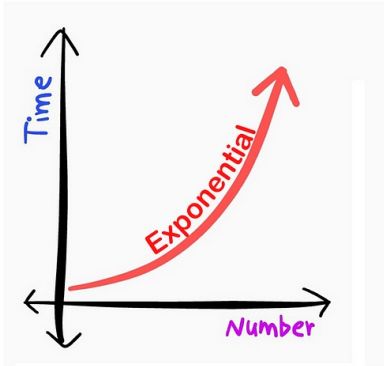
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

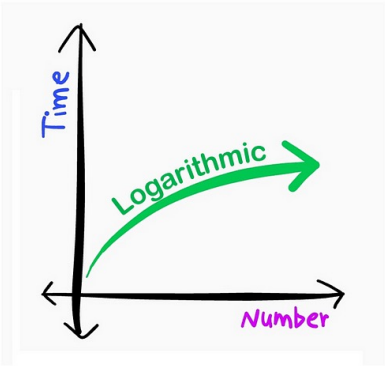
AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10



Kwantumcomputers en cryptografische sleutels







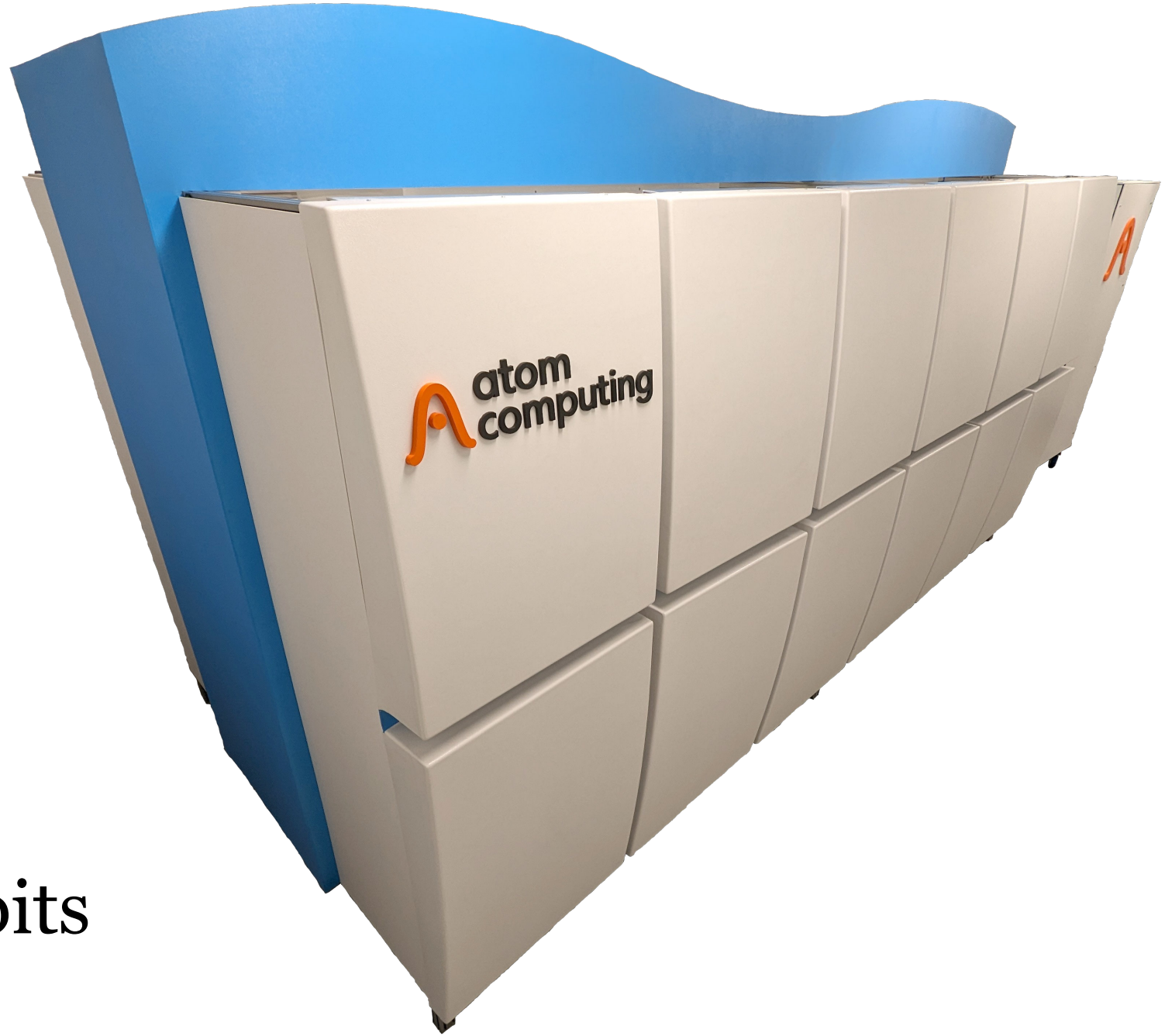
deVolkskrant

TECHNOLOGIE

De quantumcomputer zou alle digitale geheimen kunnen kraken. Hoe is dat te voorkomen?

Nog dit decennium is de quantumcomputer er, volgens sommige experts. Die zou de cyberbeveiliging kunnen kraken die nu wordt gebruikt voor alles van staats- en bankgeheimen tot chatgesprekken. Hoe maak je de versleuteling 'quantumveilig'? Daar wordt hard aan gewerkt.

Frank Rensen 1 december 2023, 10:30



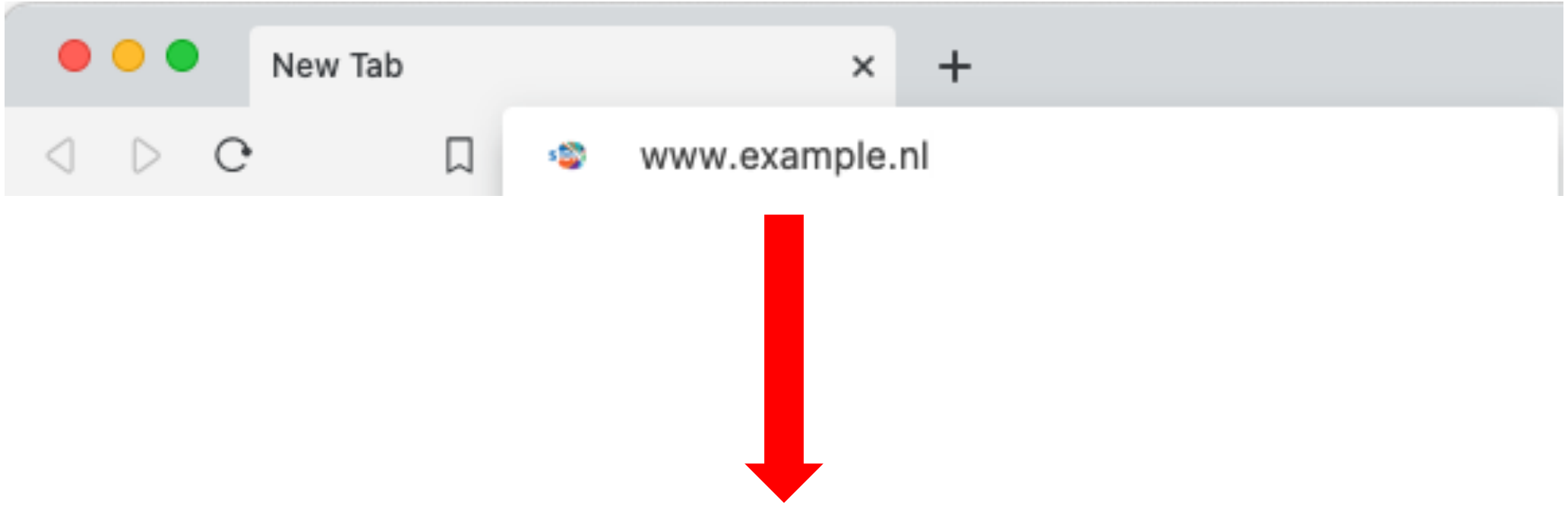
1180 qubits

Algoritme	Key size	Security	Logische qubits	Fysieke qubits	Time to break
RSA	1024 bits	80 bits	2.290	~ 2.560.000 bits	3.5 uur
RSA	**2048 bits**	**112 bits**	**4.338**	**~ 6.200.000 bits**	**29 uur**
RSA	4096 bits	128 bits	8.434	~ 14.700.000 bits	10 dagen
ECC	256 bits	128 bits	2.330	~ 3.210.000 bits	11 uur

Bron: 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

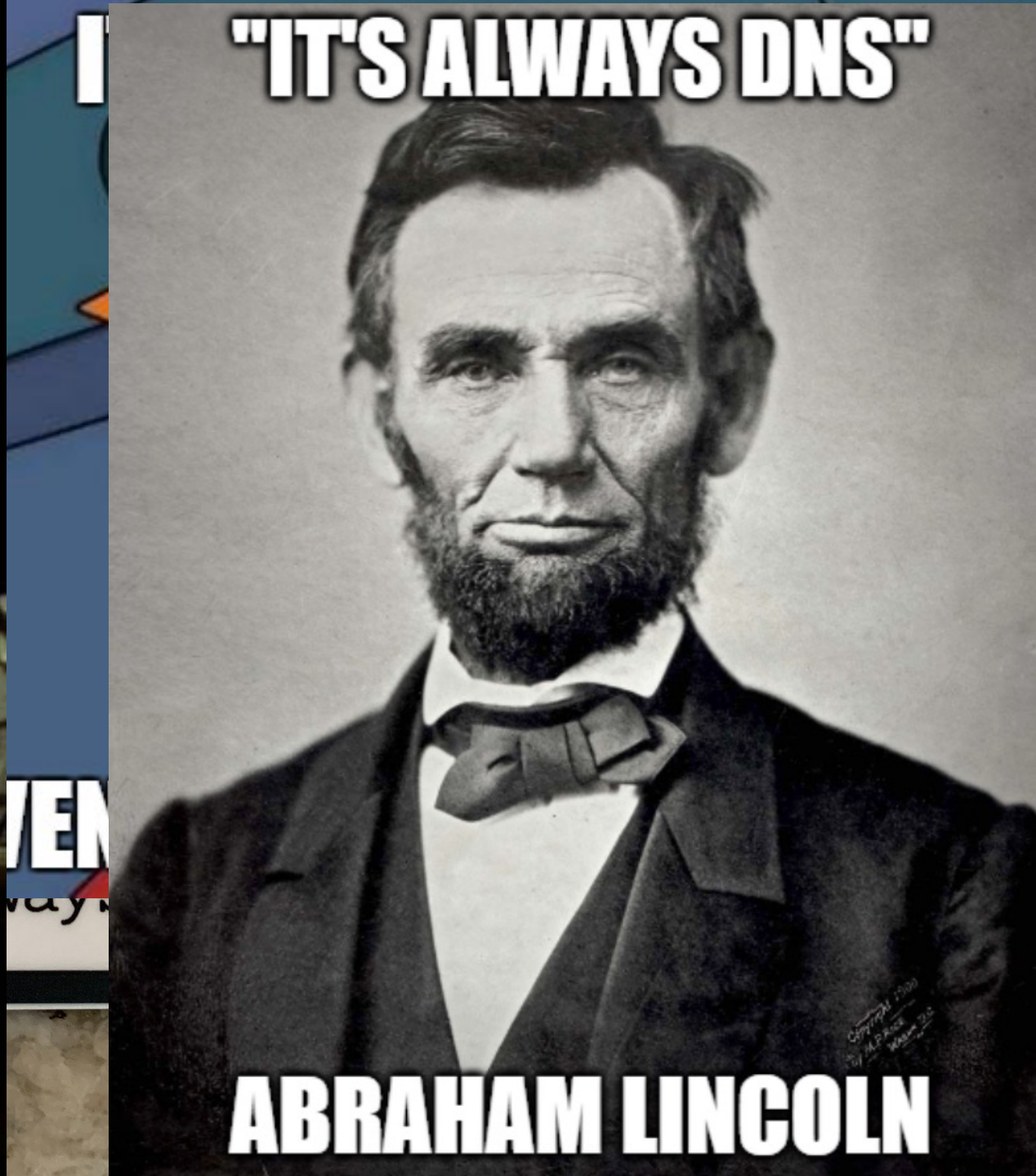
SIDN LABS

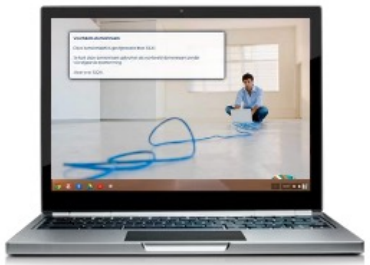

SIDN
IDN



2a00:d78:0:712:94:198:159:35


Why is it when something happens, it's always you three?
DNS
BGP
DHCP

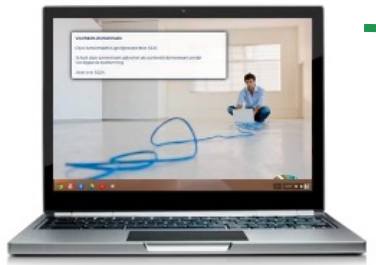

"IT'S ALWAYS DNS"
ABRAHAM LINCOLN



Gebruiker

Resolver

Authoritatieve nameservers



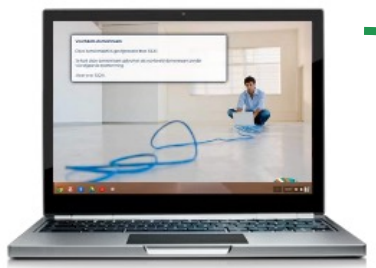
Gebruiker

Where can I find www.example.nl ?

???

Resolver

Authoritatieve nameservers



Gebruiker

Where can I find
www.example.nl ?

???

Resolver

Where can I find
www.example.nl ?

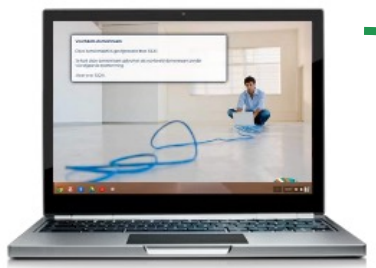
Ask nl

.

nl

example.nl

Authoritatieve
nameservers



Where can I find
www.example.nl ?

???

Where can I find
www.example.nl ?

Ask example.nl

.

nl

example.nl

Where can I find
www.example.nl ?

???

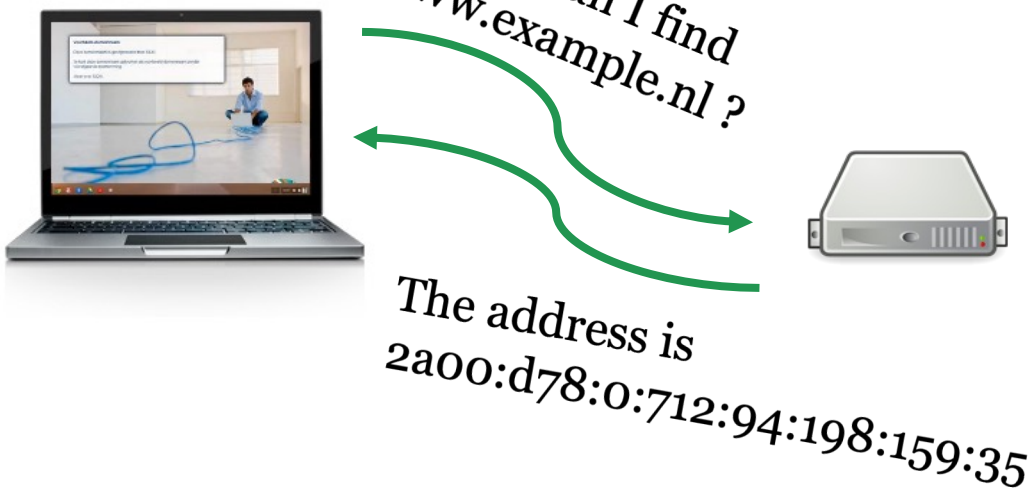
Where can I find
www.example.nl ?

The address is
2a00:d78:0:712:94:198:159:35

.

nl

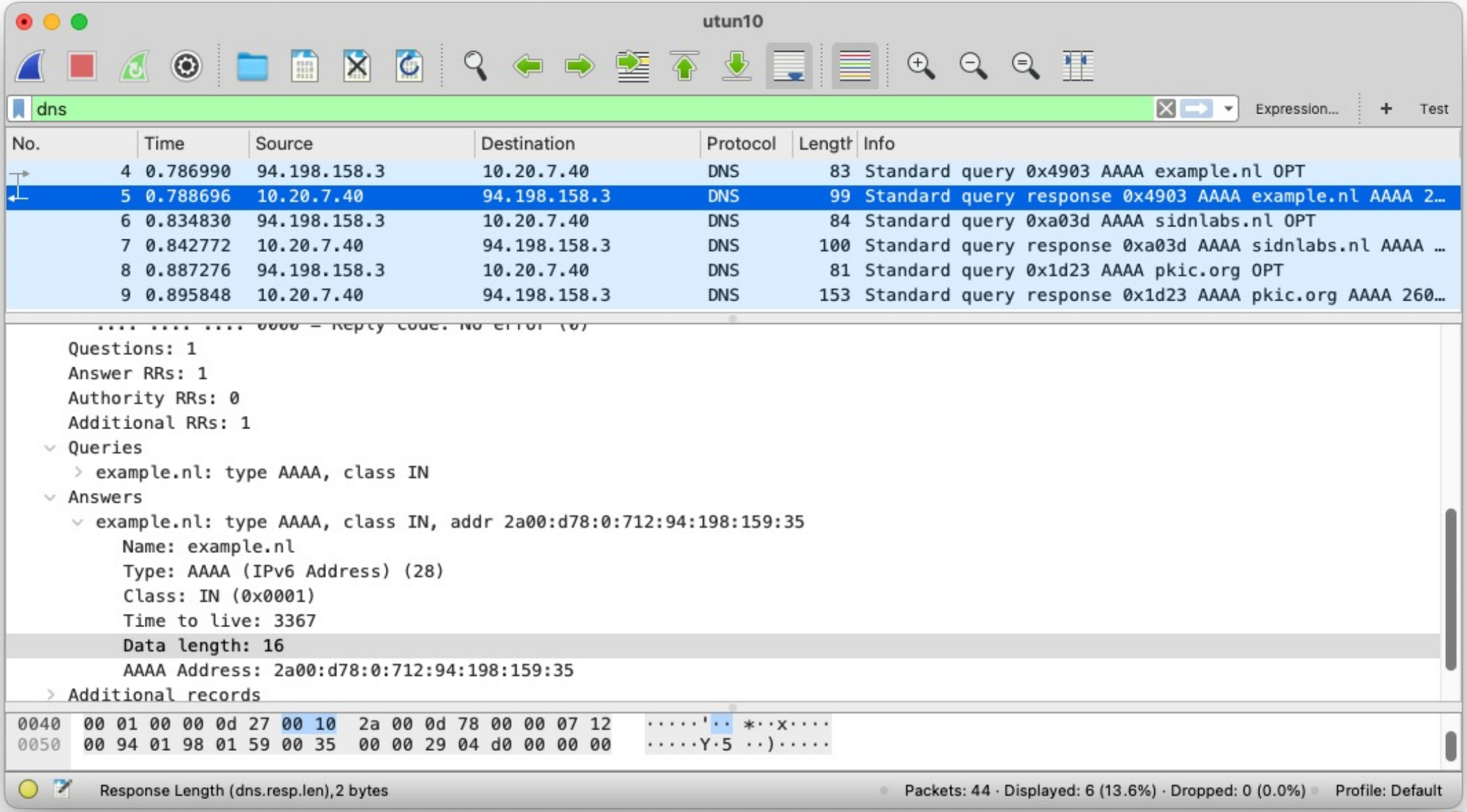
example.nl



.

nl

example.nl

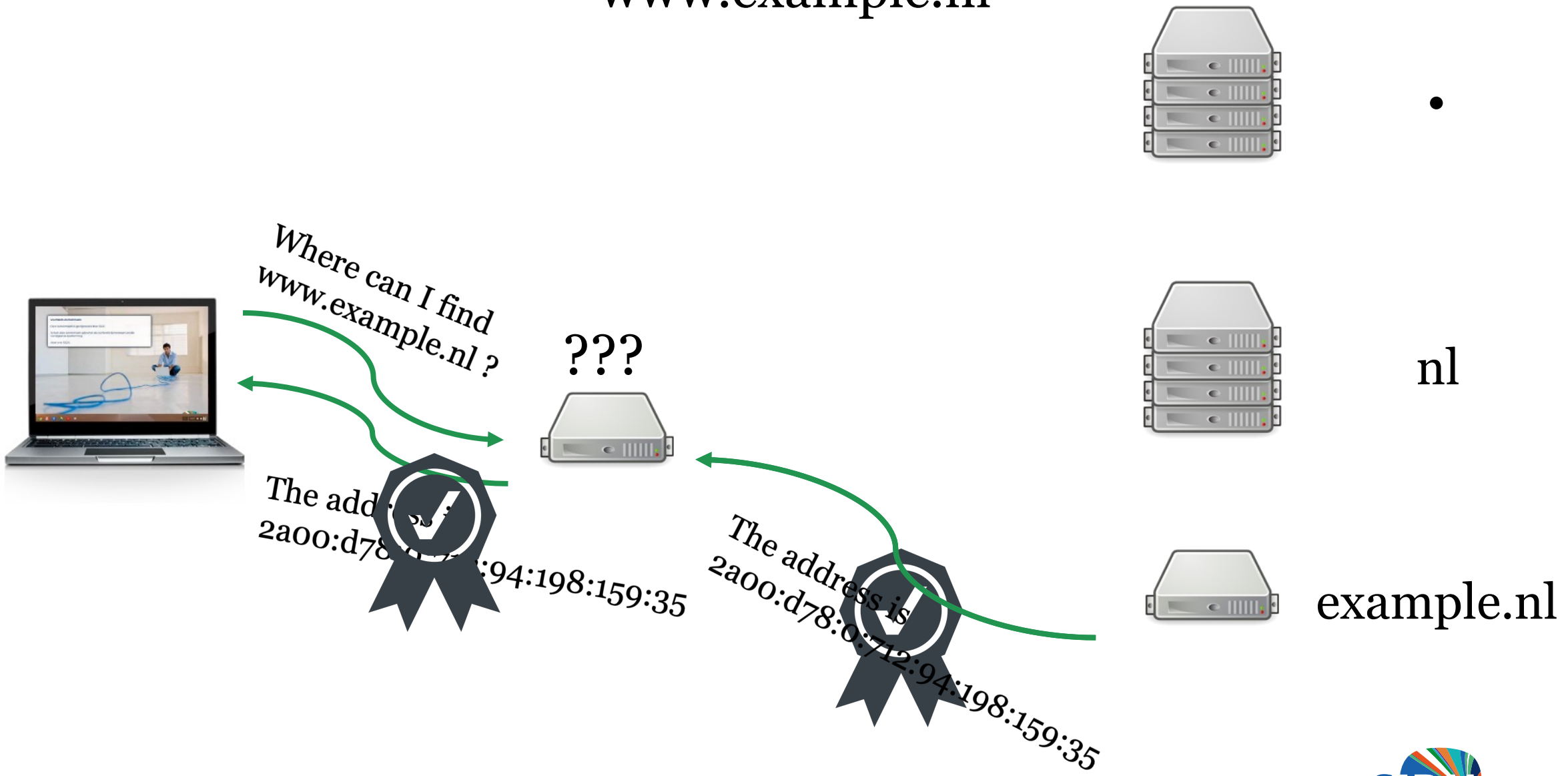

utun10
dns
Expression...
Test
No. Time Source Destination Protocol Length Info
4 0.786990 94.198.158.3 10.20.7.40 DNS 83 Standard query 0x4903 AAAA example.nl OPT
5 0.788696 10.20.7.40 94.198.158.3 DNS 99 Standard query response 0x4903 AAAA example.nl AAAA 2…
6 0.834830 94.198.158.3 10.20.7.40 DNS 84 Standard query 0xa03d AAAA sidnlabs.nl OPT
7 0.842772 10.20.7.40 94.198.158.3 DNS 100 Standard query response 0xa03d AAAA sidnlabs.nl AAAA …
8 0.887276 94.198.158.3 10.20.7.40 DNS 81 Standard query 0x1d23 AAAA pkic.org OPT
9 0.895848 10.20.7.40 94.198.158.3 DNS 153 Standard query response 0x1d23 AAAA pkic.org AAAA 260…
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
example.nl: type AAAA, class IN
Answers
example.nl: type AAAA, class IN, addr 2a00:d78:0:712:94:198:159:35
Name: example.nl
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 3367
Data length: 16
AAAA Address: 2a00:d78:0:712:94:198:159:35
Additional records
0040 00 01 00 00 0d 27 00 10 2a 00 0d 78 00 00 07 12
0050 00 94 01 98 01 59 00 35 00 00 29 04 d0 00 00 00
Response Length (dns.resp.len),2 bytes
Packets: 44 · Displayed: 6 (13.6%) · Dropped: 0 (0.0%)
Profile: Default

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

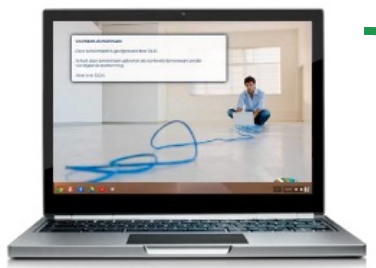
X25519Kyber768

DNSSEC

www.example.nl



www.example.nl



Where can I find www.example.nl ?

???

Where can I find www.example.nl ?

Ask example.nl

.

nl

example.nl

SIDN LABS

www.example.nl

Where can I find www.example.nl ?

???

Where can I find www.example.nl ?

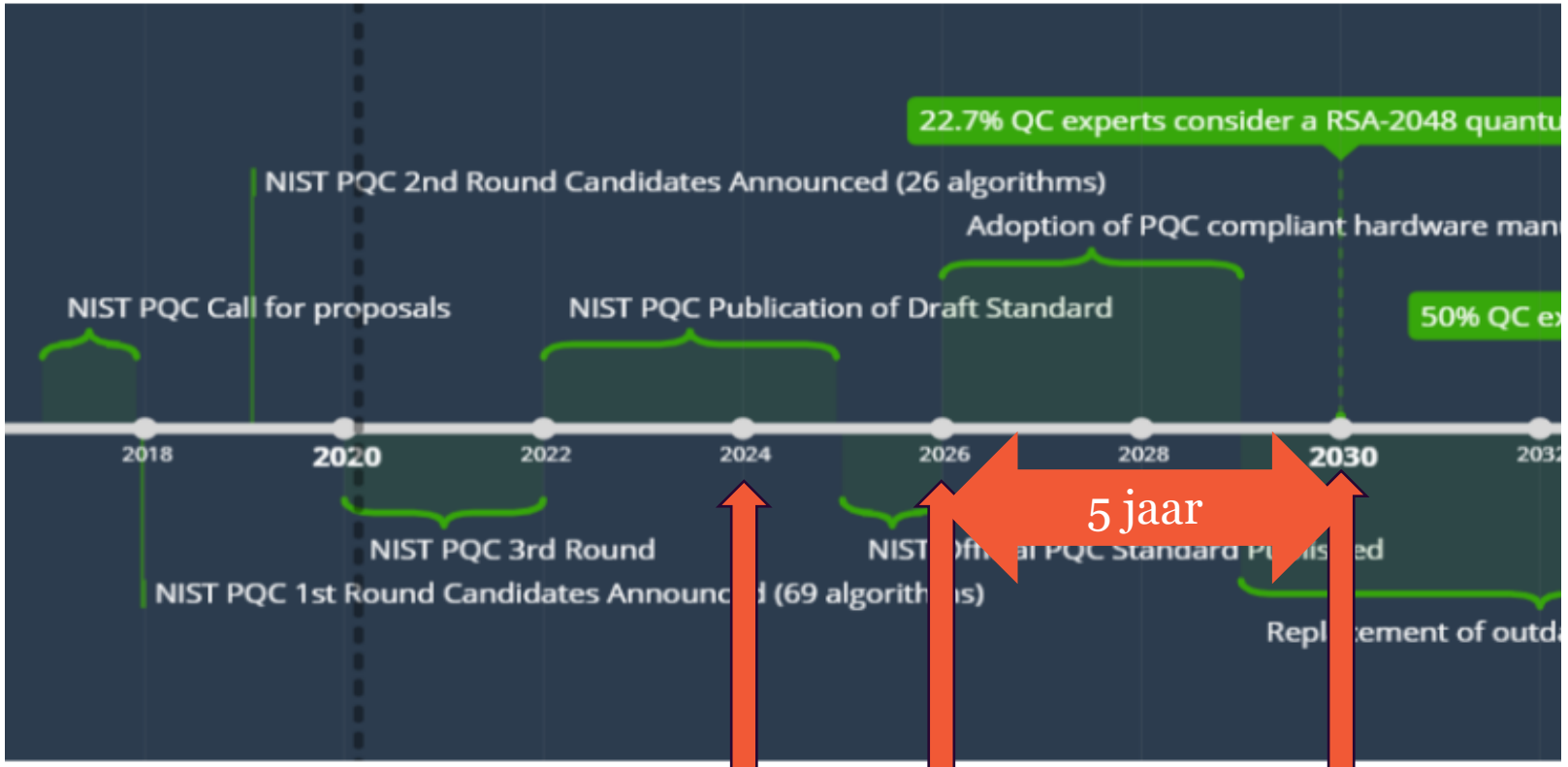
Ask nl

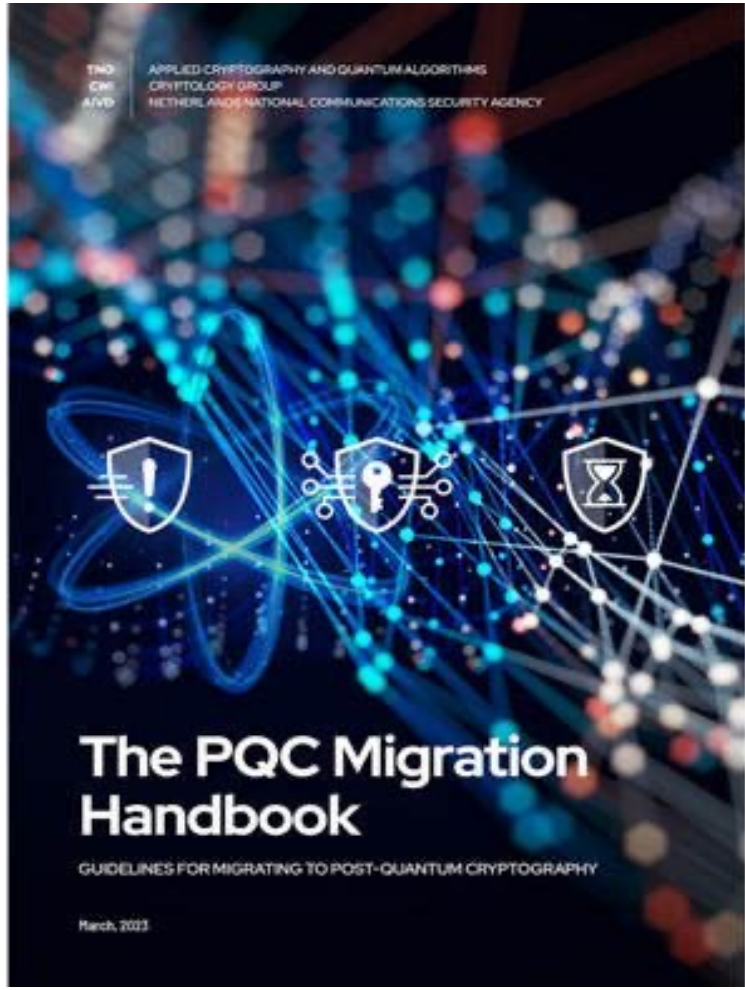
.

nl

example.nl

SIDN LABS



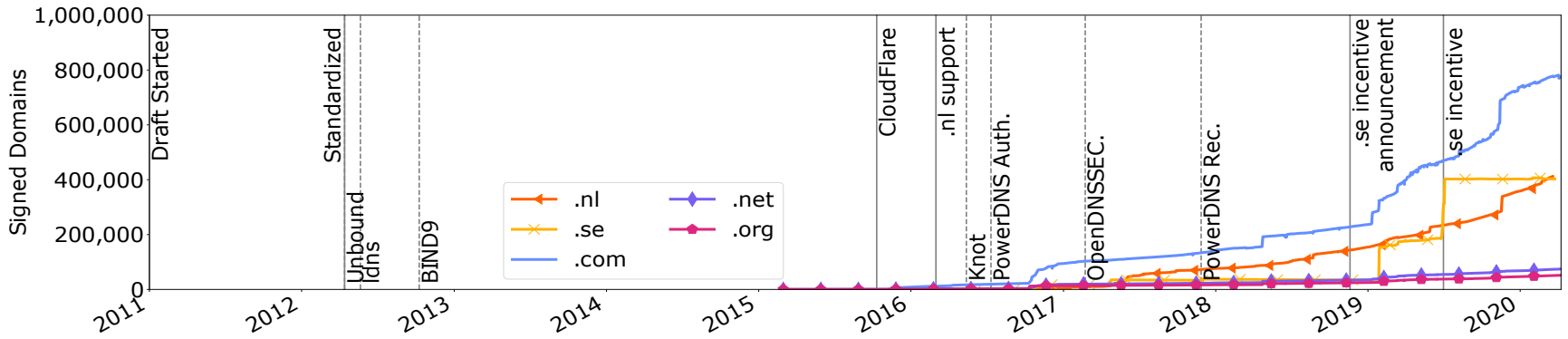


Standaarden voor PQC beschikbaar

DNSSEC (misschien) kwetsbaar

SIDN LABS

Uitrol nieuwe encryptie in DNS, +- 10 jaar



Tijdlijn uitrol ECDSA256 uit '*Making DNSSEC Future Proof*' door dr. Moritz Müller.


Requirements

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

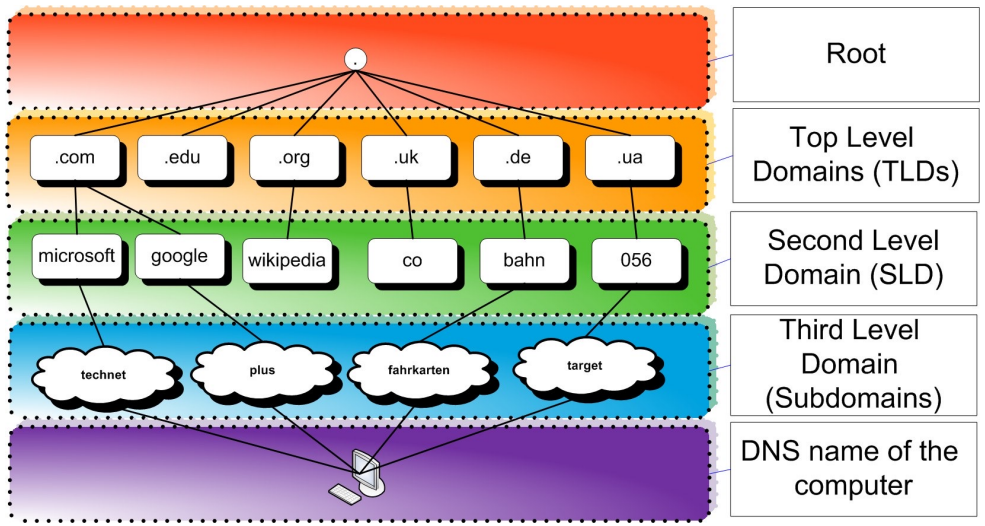
Table 2: Requirements for quantum-safe algorithms.

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.

Jürgen Henn – 11foot8.com

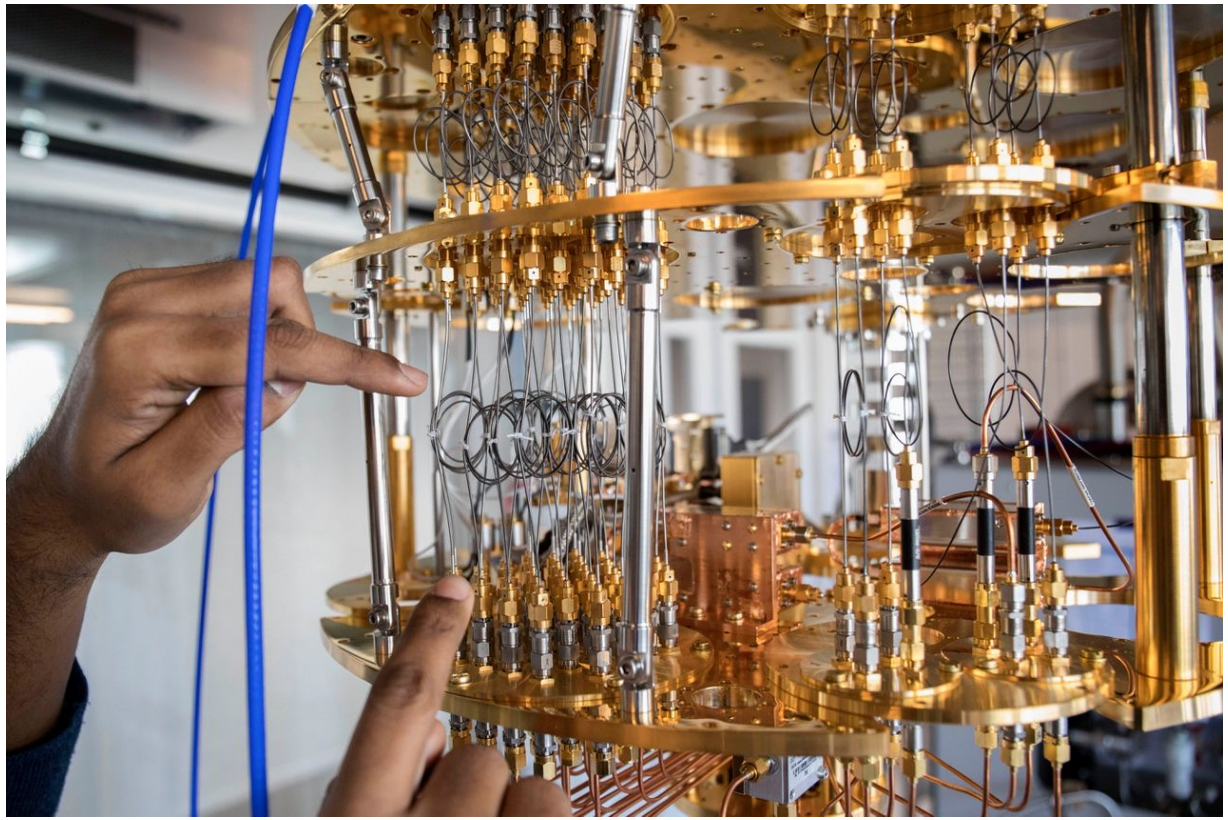

gifbin.com

DNS


.com
.edu
.org
.uk
.de
.ua
microsoft
google
wikipedia
co
bahn
056
technet
plus
fahrkarten
target
Root
Top Level Domains (TLDs)
Second Level Domain (SLD)
Third Level Domain (Subdomains)
DNS name of the computer

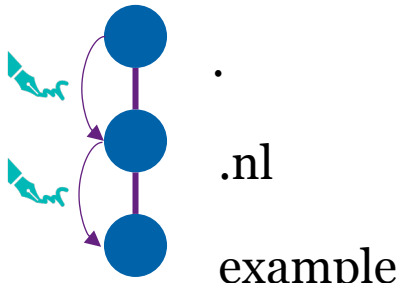
x2

Post-kwantum Algoritmes Testen en Analyseren voor DNS



PATAD testbed: het plan en het experiment

1) Het ontwerp van de test-infrastructuur

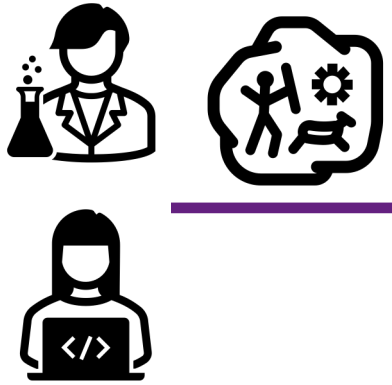


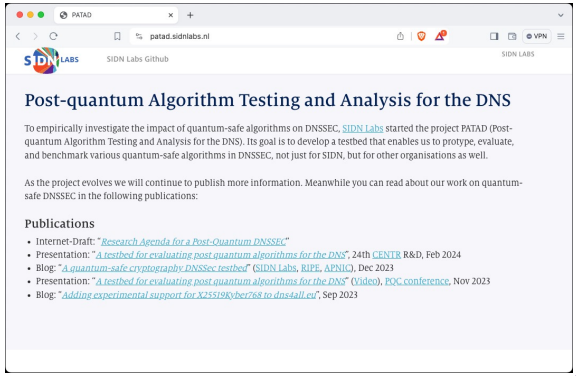
2) Het PQC algoritme dat we willen testen

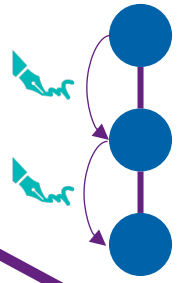
3) De metingen die we uitvoeren

Sign 100x, verify 100x, geef de gemiddelden.

PATAD testbed: het bouwen van een testbed

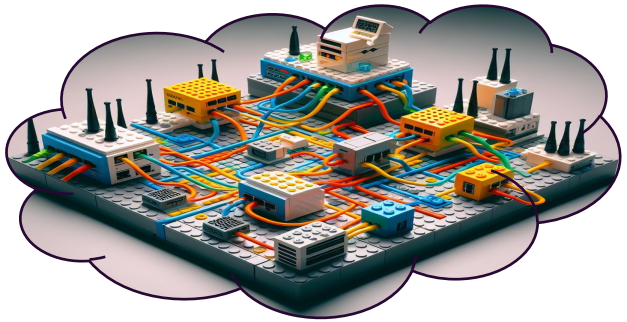






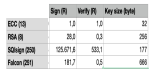
.nl

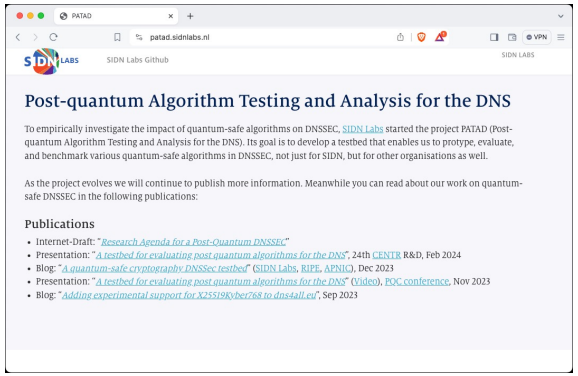
sidnlabs

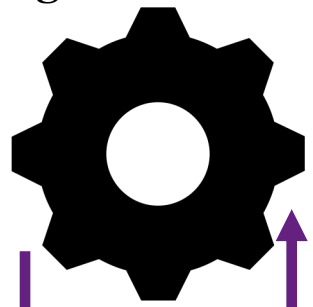


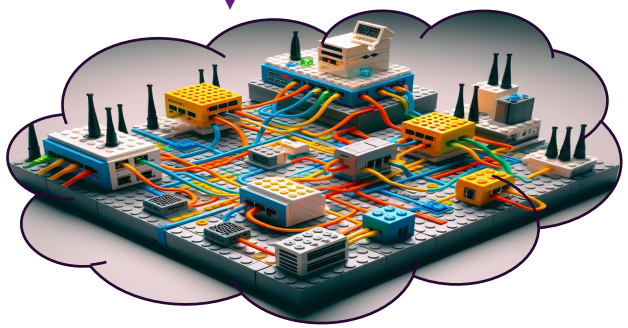
PATAD testbed: resultaten

- voor 4 algoritmen
- sign 100x
- verify 100x
- geef de gemiddelden





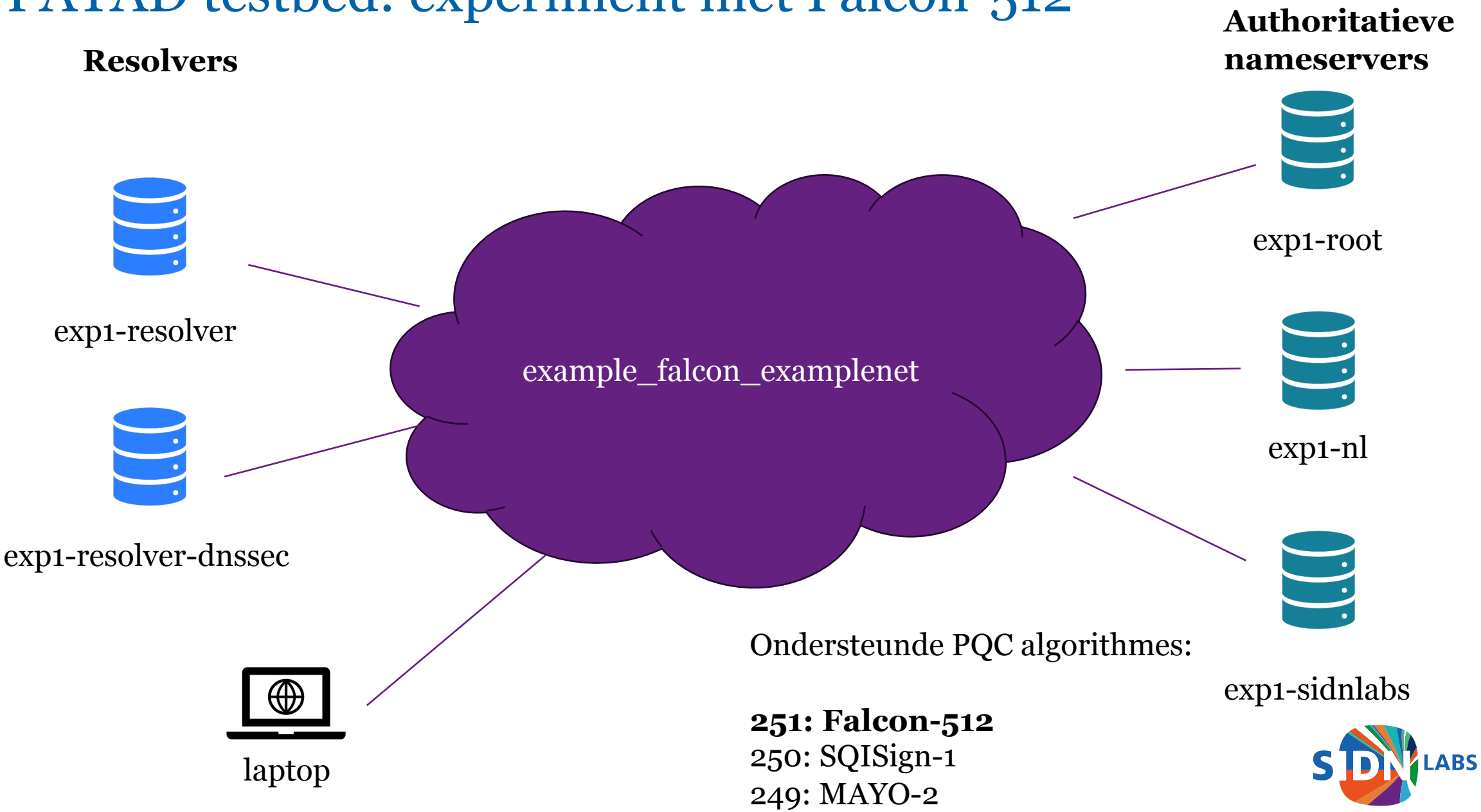




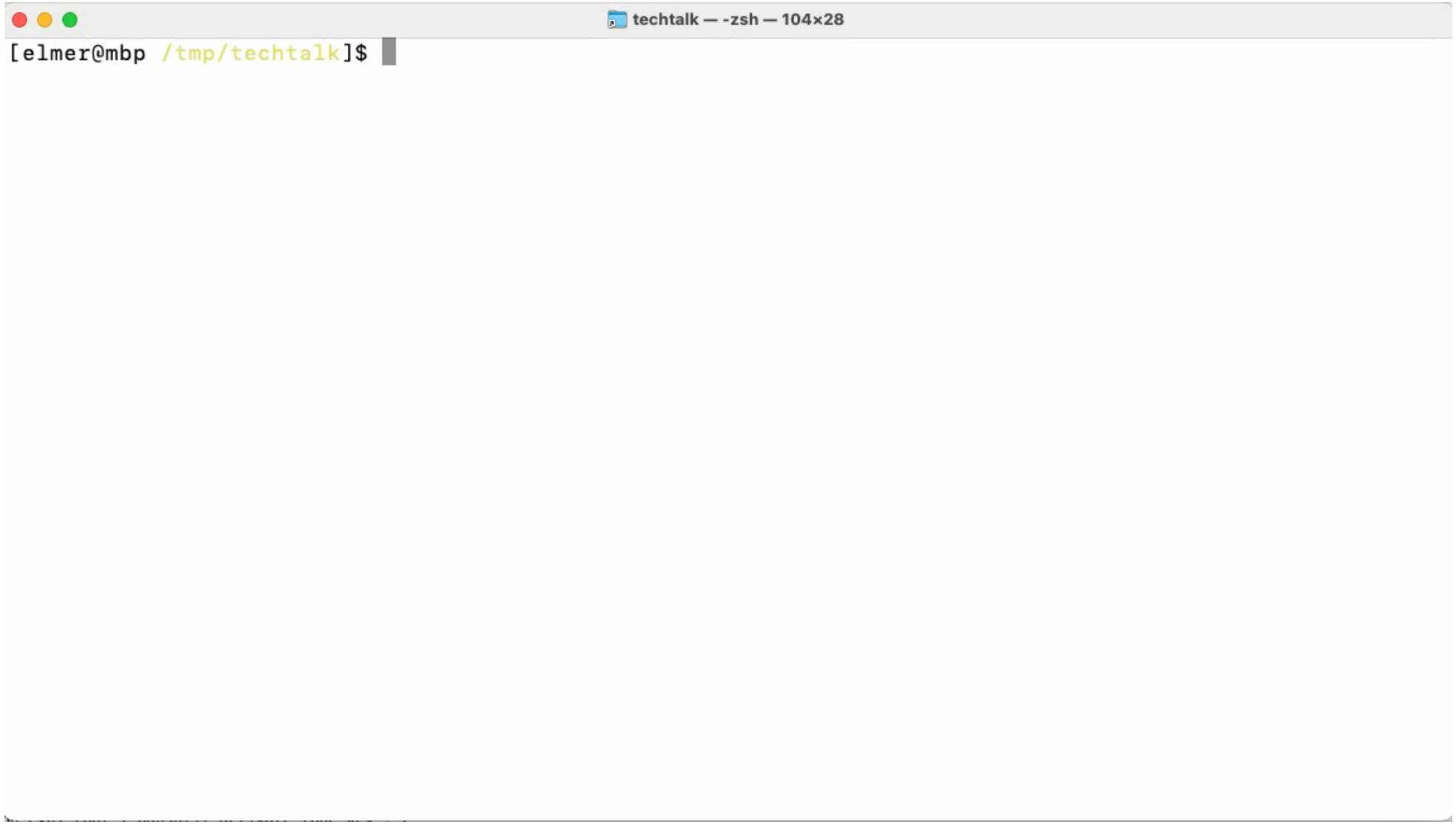
	Create (R)	Sign (R)	Verify (R)	Sig size (byte)	PubKey size (byte)
ECC (13)	1,0	1,0	1,0	32	32
RSA (8)	6.354	21	0,3	256	256
SQIsign1 (250)	68.625	120.582	610	177	204
Falcon (251)	566	154	0,6	666	897
Mayo2 (249)	52	76	3,2	180	5488

Dit is een *enkel ongeverifeerd* meetresultaat, graag weer vergeten na afloop ☺

PATAD testbed: experiment met Falcon-512



Demo?



Vervolgstappen

PQC-Ready componenten ontwikkelen

Testbed infrastructuur ontwikkelen

Het zelf uitvoeren van experimenten

Anderen mensen enthousiast maken om mee te werken en het testbed te gebruiken.

PATAD blog overgenomen:

RIPE Labs APNIC

Actieve onderzoekspartners:

SURF UNIVERSITY OF TWENTE.

Interesse en gesprekken:

CLOUDFLARE VERISIGN

IRTF

SIDN LABS

Bedankt voor je aandacht

Elmer Lastdrager
elmer.lastdrager@sidn.nl

https://www.sidnlabs.nl