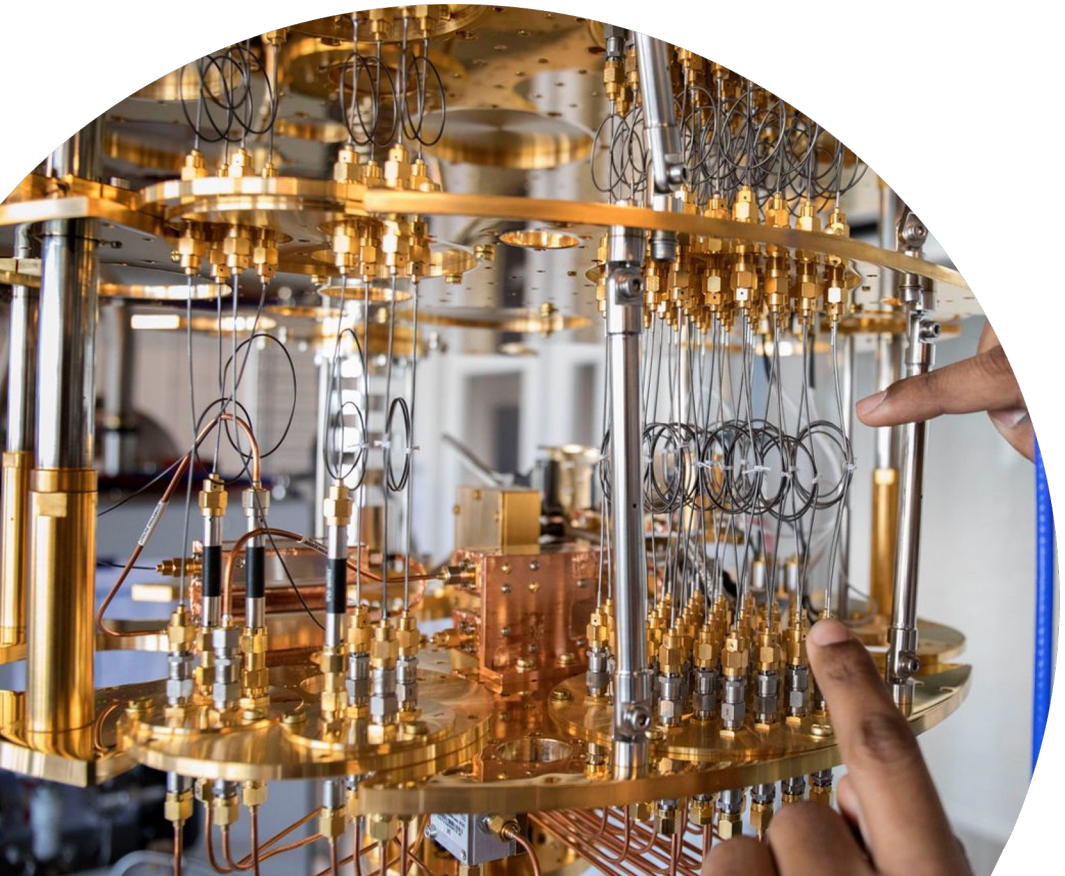


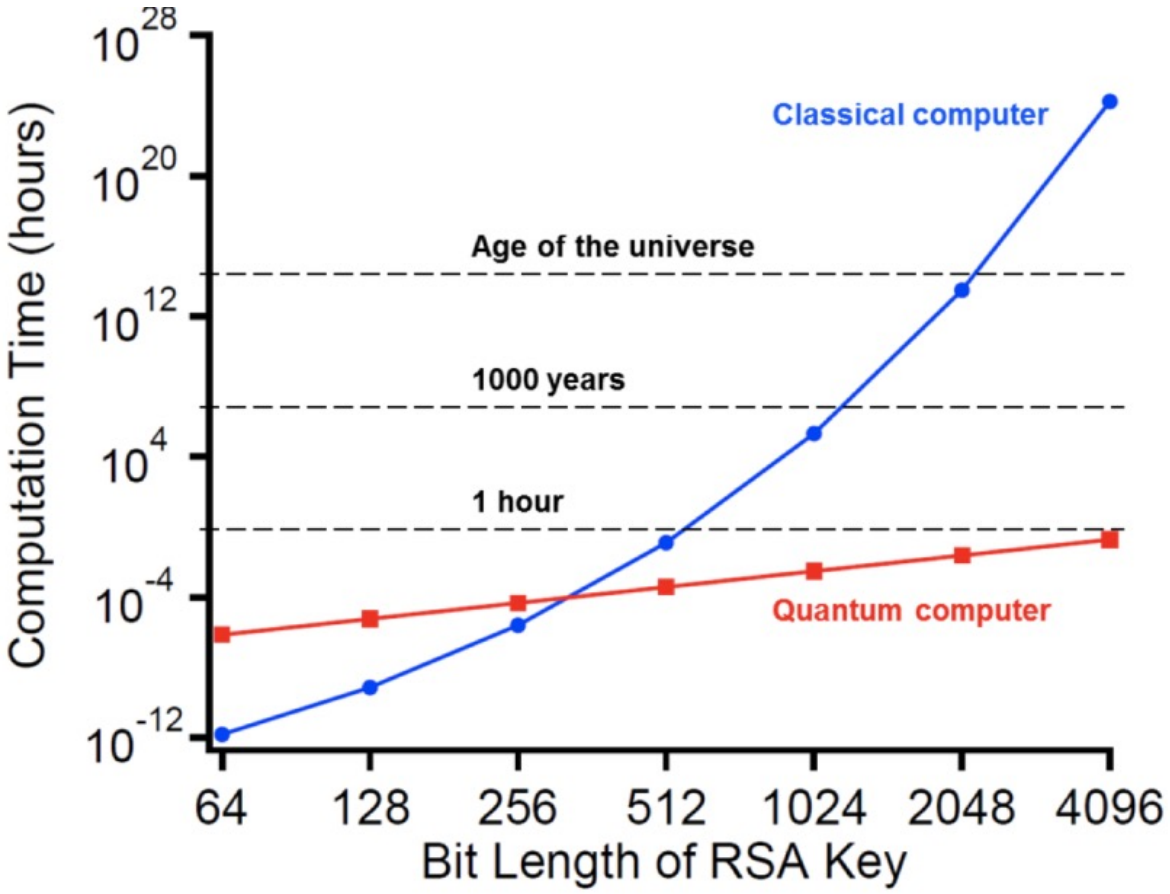
Een testbed om post-kwantumalgoritmes voor DNS te evalueren

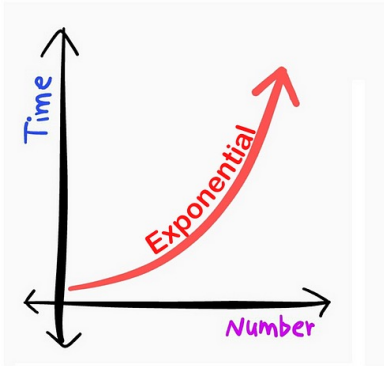
Elmer Lastdrager

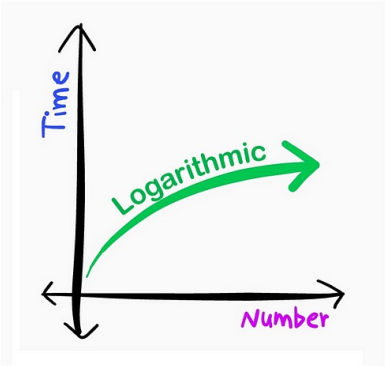
16 april 2024

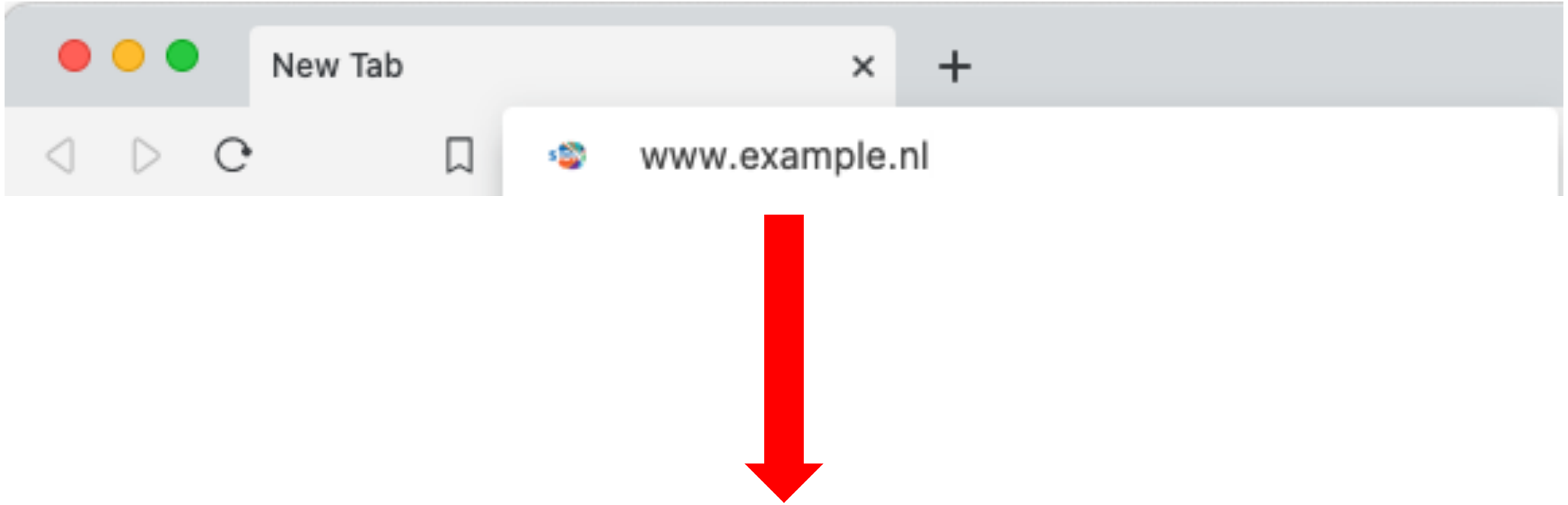
SIDN LABS

Kwantumcomputers en cryptografische sleutels



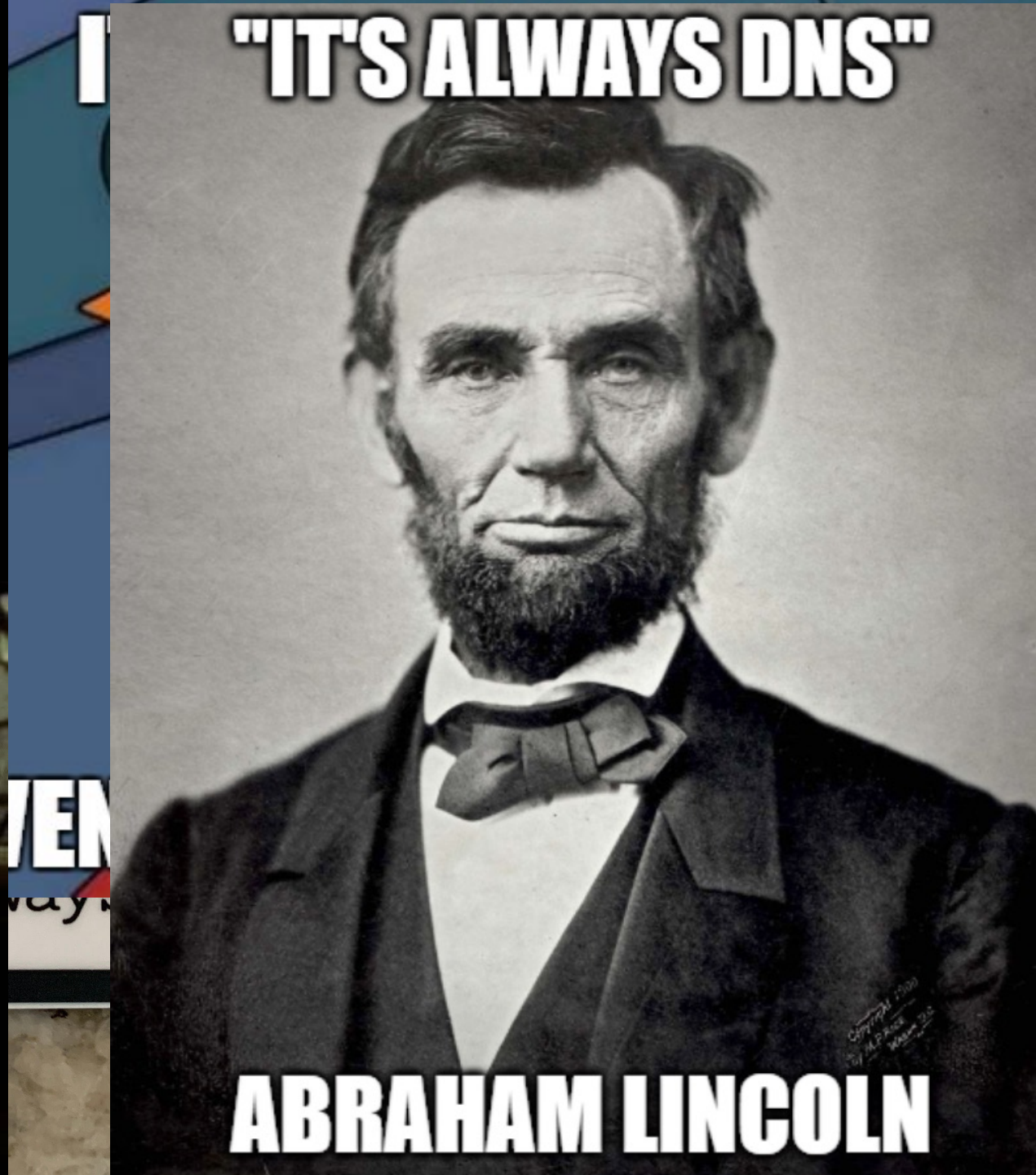


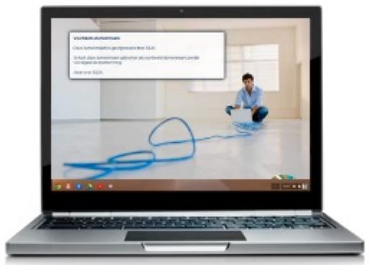




2a00:d78:0:712:94:198:159:35


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


"IT'S ALWAYS DNS"
ABRAHAM LINCOLN



User

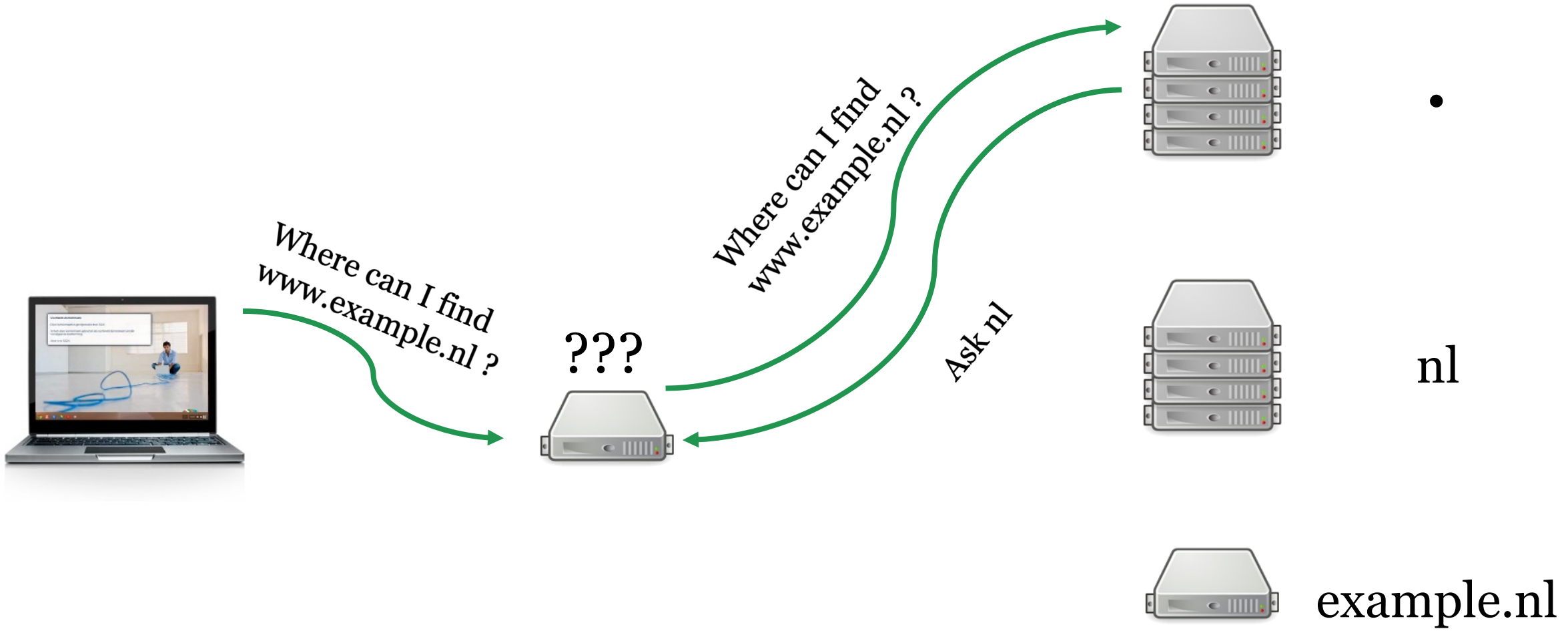
Resolver

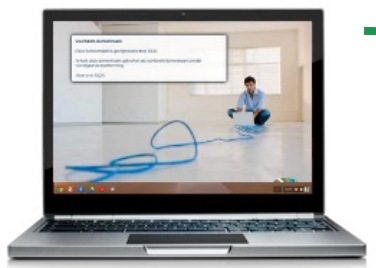
Authoritative name servers

Where can I find
www.example.nl ?

???

SDN LABS


Where can I find
www.example.nl ?
???
Where can I find
www.example.nl ?
Ask nl
.
nl
example.nl



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 ?

???

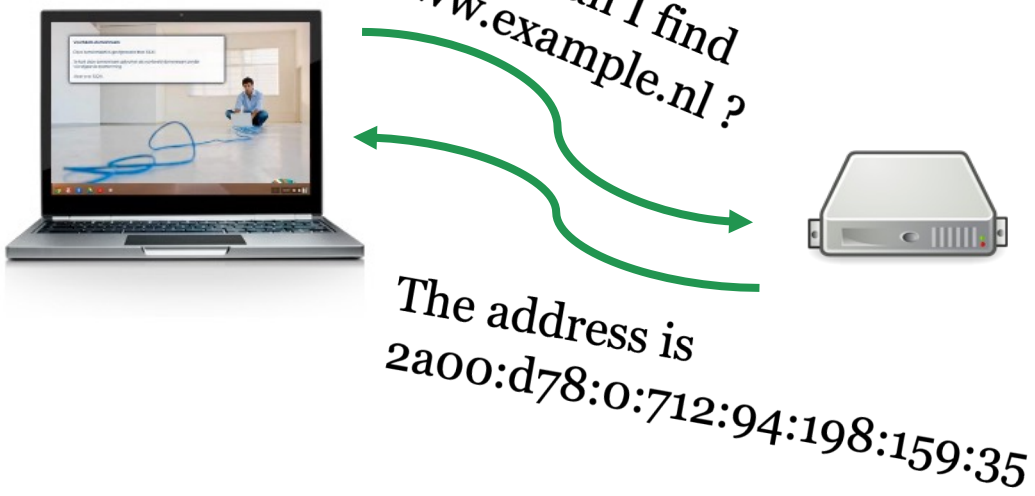
Where can I find
www.example.nl ?

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

.

nl

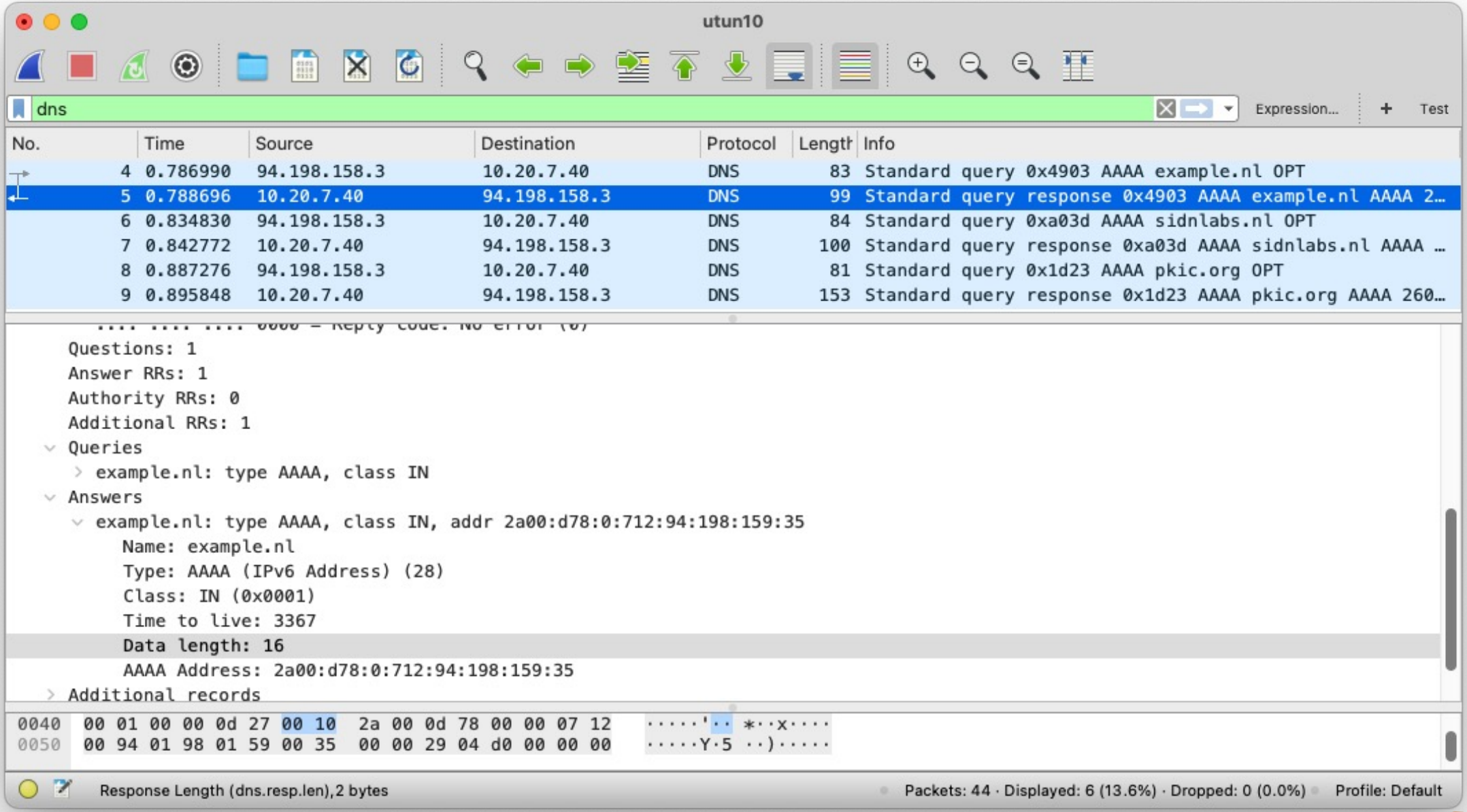
example.nl



.

nl

example.nl

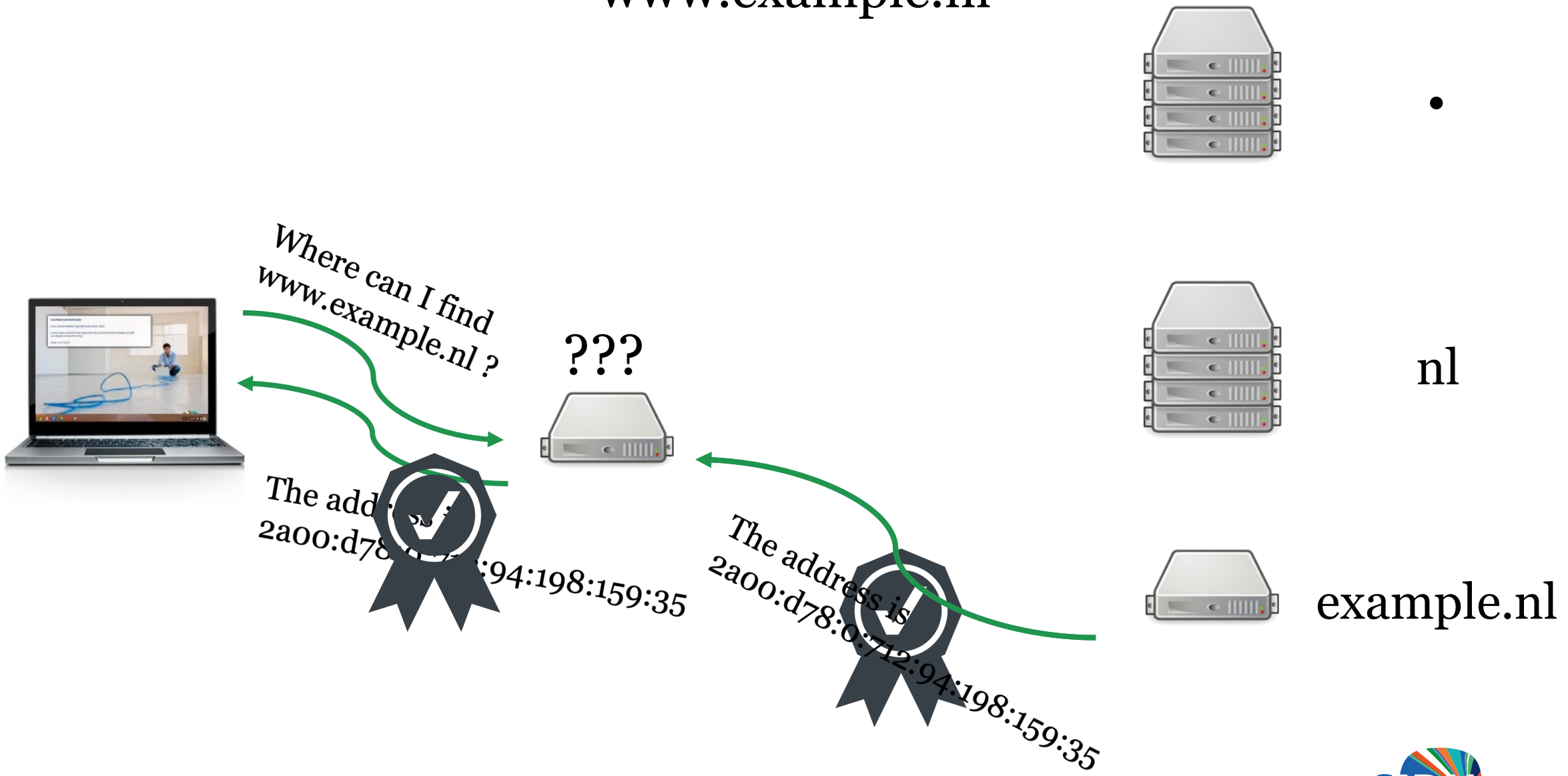

utun10
dns
Expression...
Test
No. Time Source Destination Protocol Length Info
4 0.786990 94.198.158.3 10.20.7.40 DNS 83 Standard query 0x4903 AAAA example.nl OPT
5 0.788696 10.20.7.40 94.198.158.3 DNS 99 Standard query response 0x4903 AAAA example.nl AAAA 2…
6 0.834830 94.198.158.3 10.20.7.40 DNS 84 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/

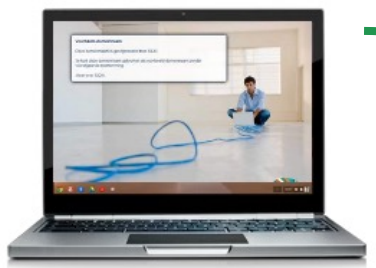
X25519Kyber768

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

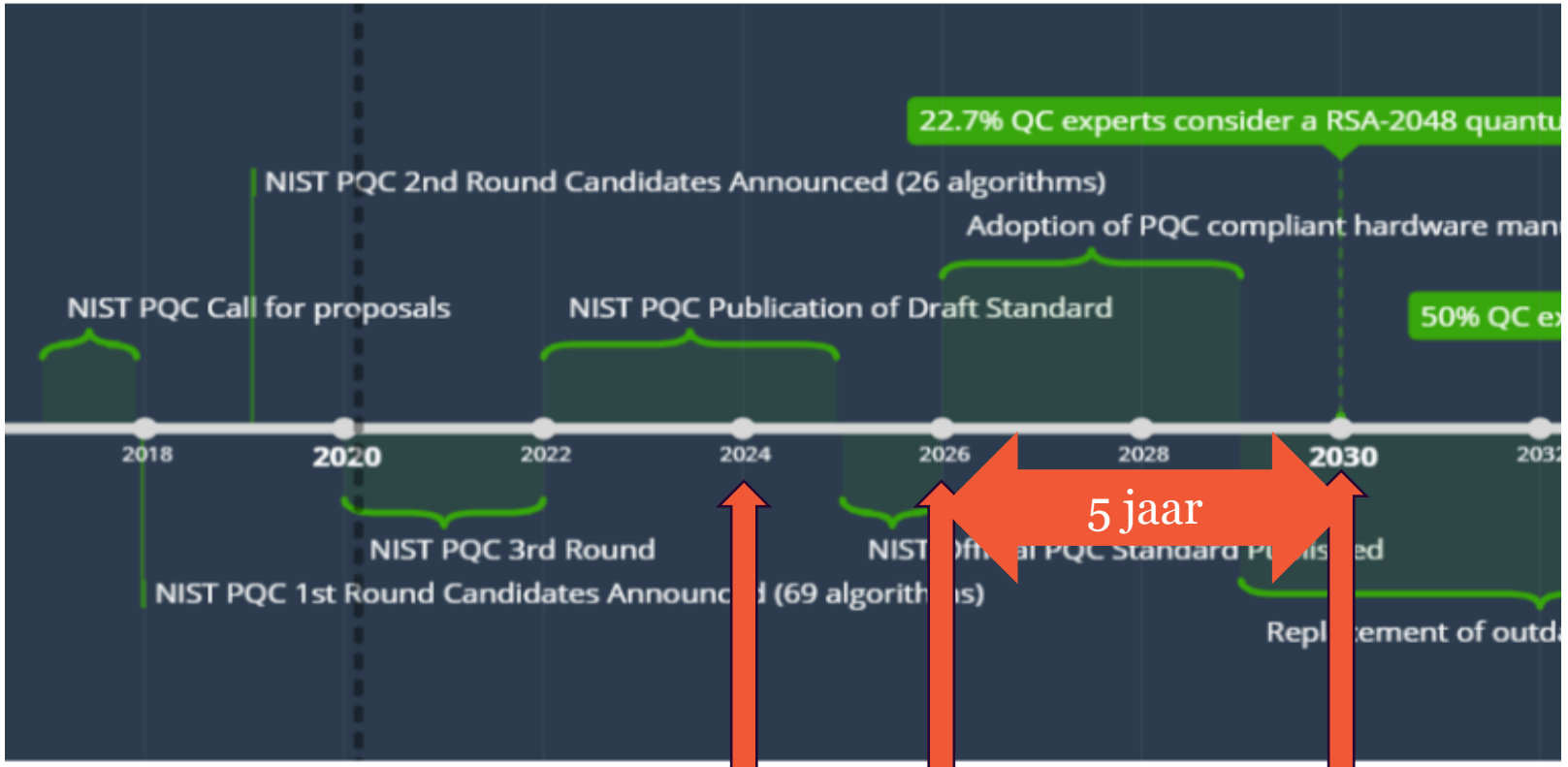
.

nl

example.nl

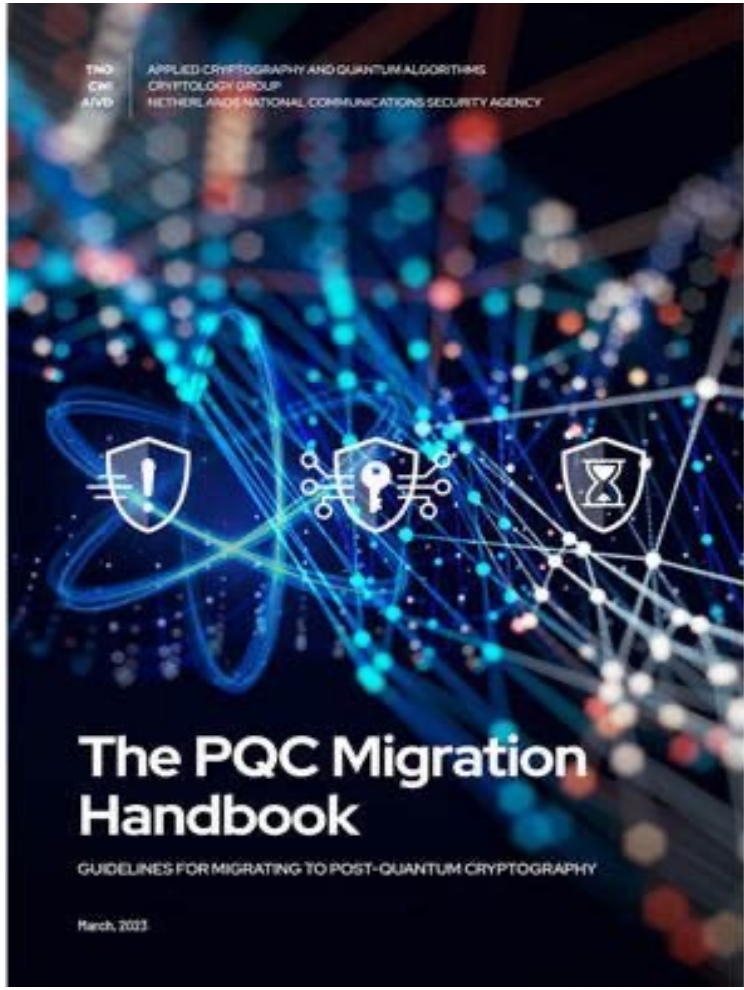
SIDN LABS

Wanneer is post-kwantumcryptografie nodig?



Standaarden voor PQC beschikbaar

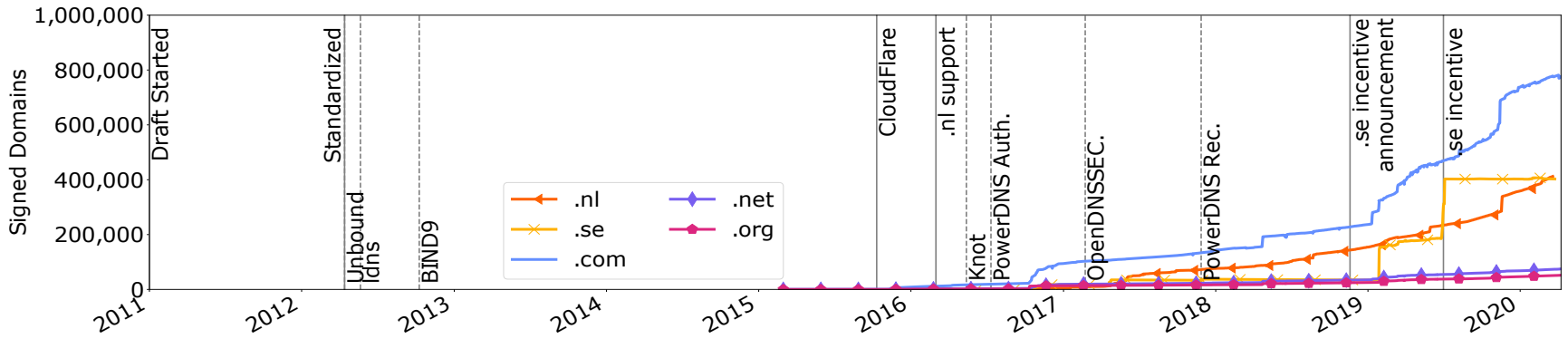
DNSSEC (misschien) kwetsbaar



SIDN LABS

Zijn we nog op tijd?

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	—

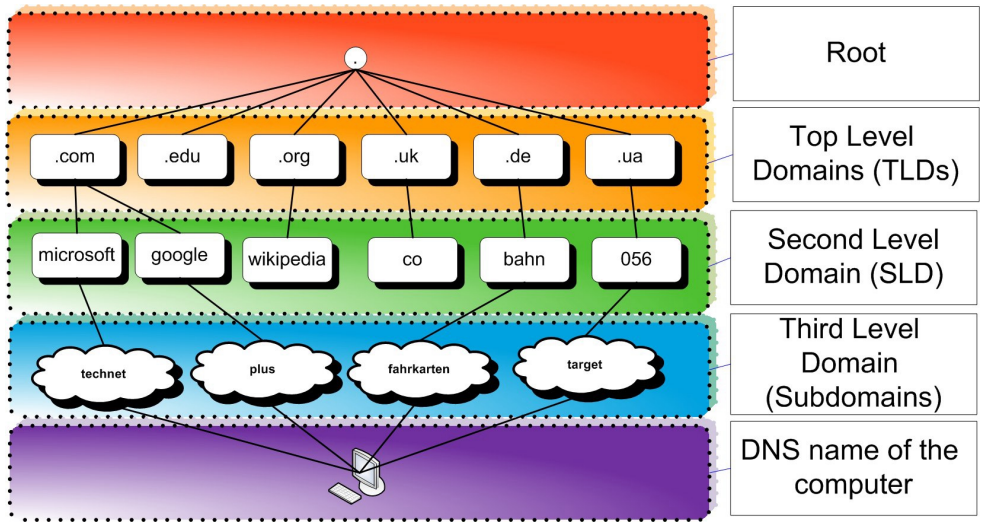
Table 2: Requirements for quantum-safe algorithms.

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.

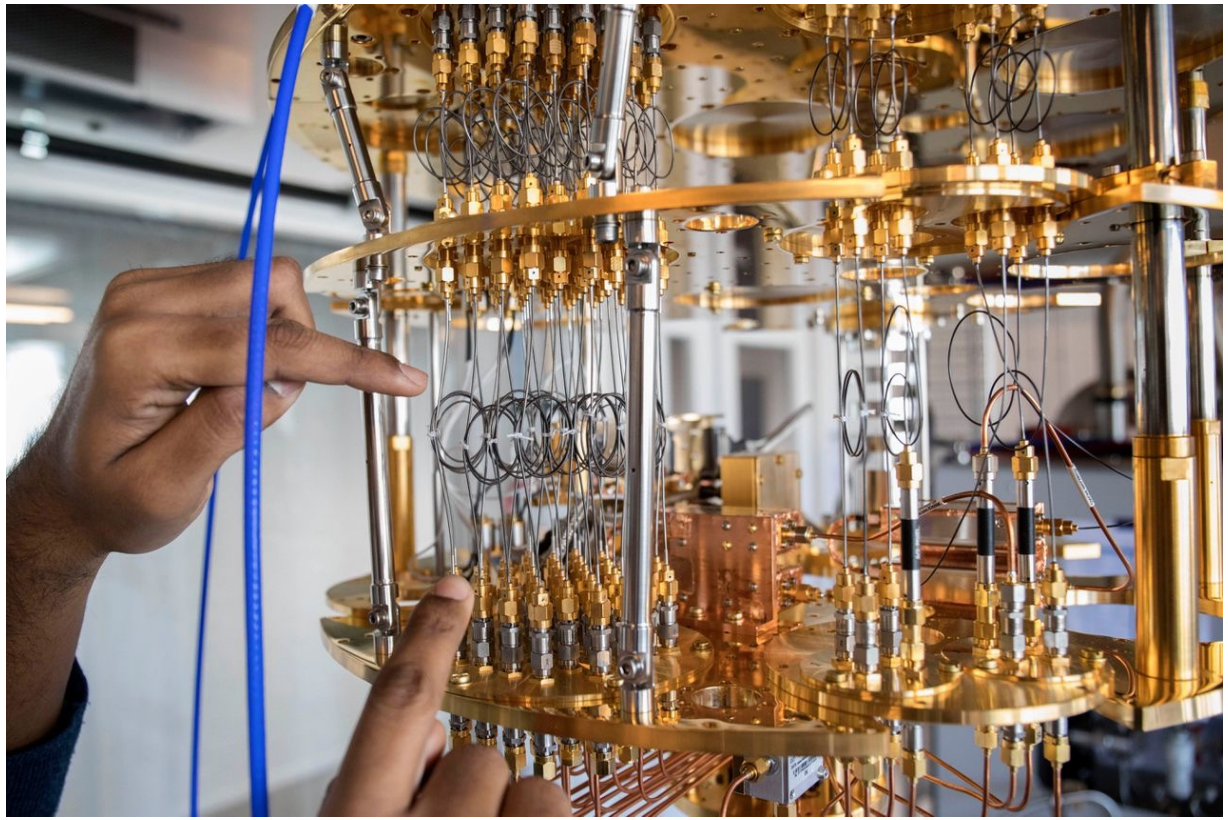
Jürgen Henn – 11foot8.com


gifbin.com

DNS is een complex systeem

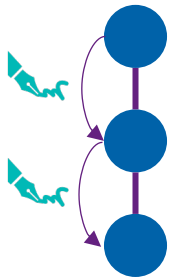


Post-kwantum Algoritmes Testen en Analyseren voor DNS



PATAD testbed: Het plan en het experiment

1) Het ontwerp van de test-infrastructuur

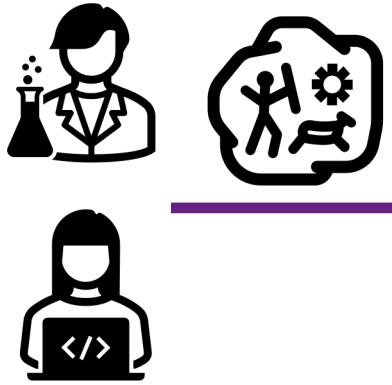


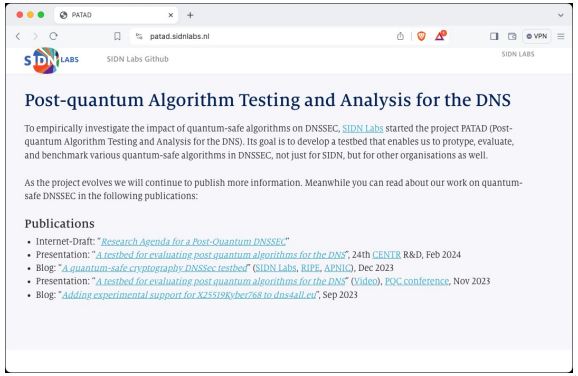
2) Het PQC algoritme dat we willen testen

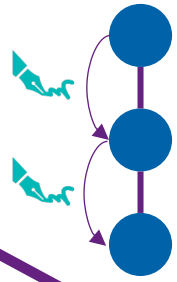
3) De metingen die we uitvoeren

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

PATAD testbed: Het bouwen van een testbed

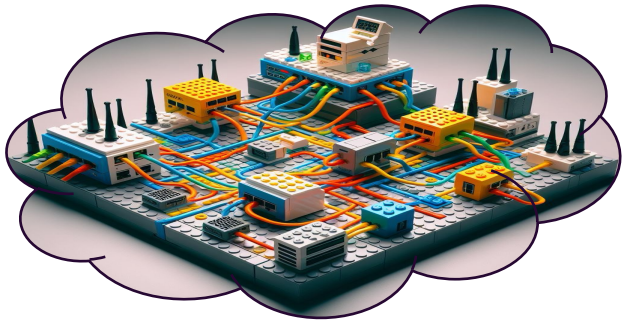






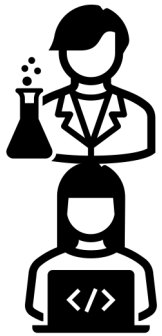
.nl

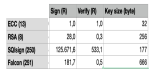
sidnlabs

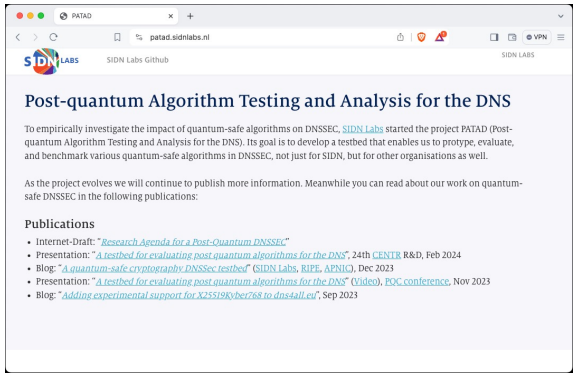


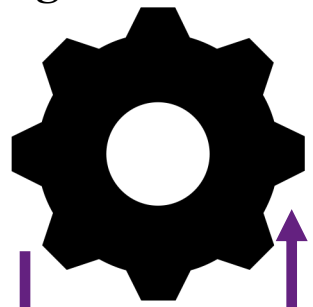
PATAD testbed: Resultaten

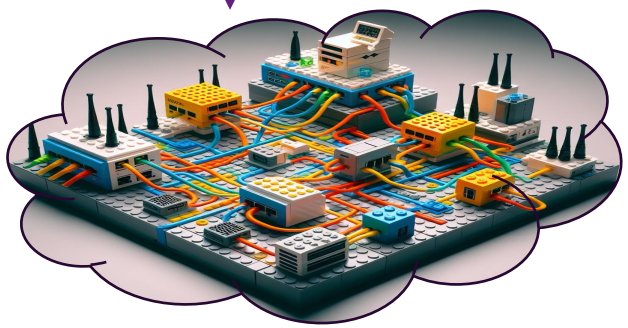
- voor 4 algoritmen
- sign 100x
- verify 100x
- geef de gemiddelden







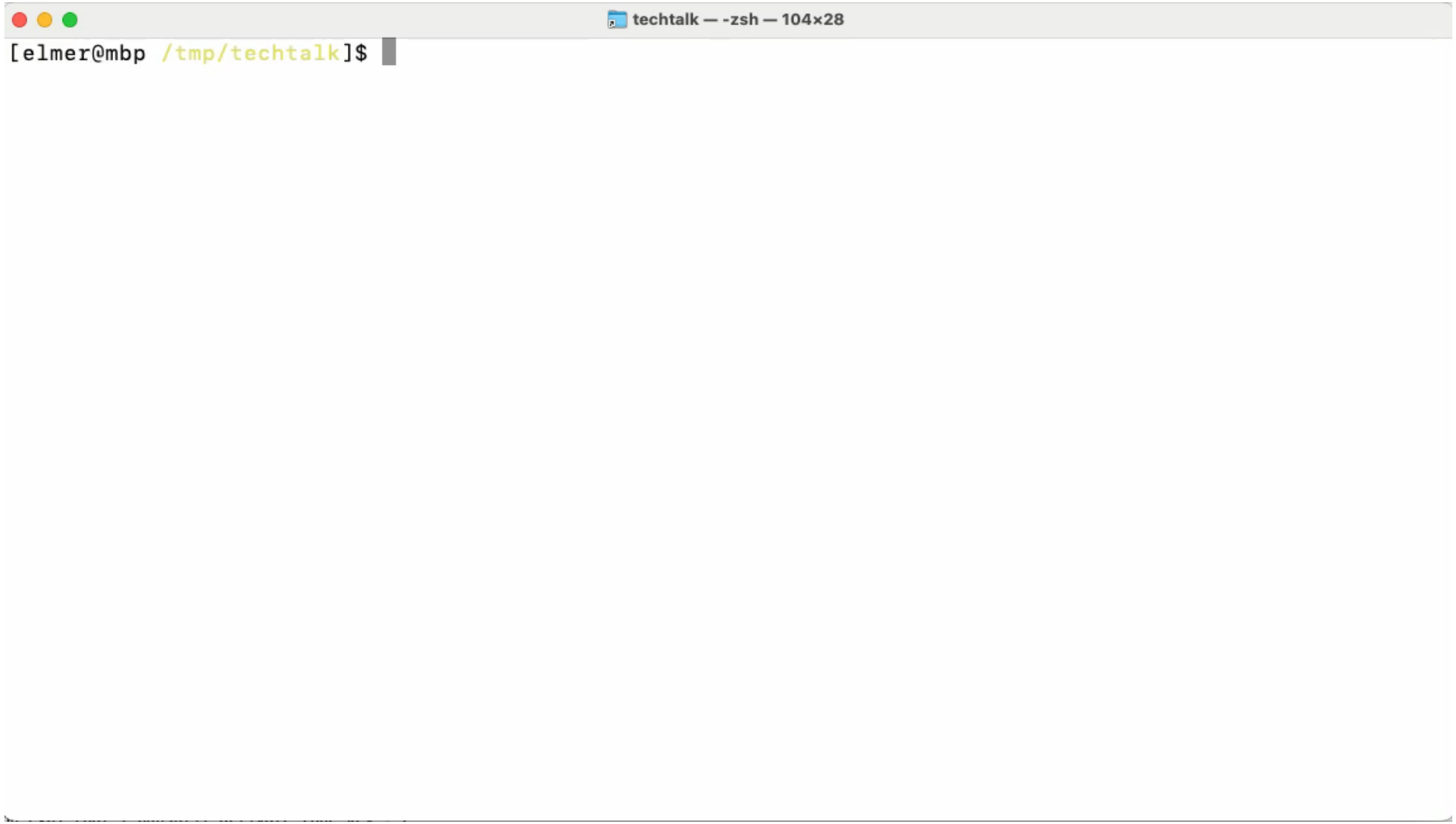




	Create (R)	Sign (R)	Verify (R)	Sig size (byte)
ECC (13)	1,0	1,0	1,0	32
RSA (8)	5.966,5	28,0	0,3	256
SQIsign (250)	55.431,3	125.671,6	533,1	177
Falcon (251)	448,5	181,7	0,5	666

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

Demo?



Vervolgstappen

PQC-Ready componenten ontwikkelen

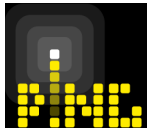
Testbed infrastructuur ontwikkelen

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

I R T F

SDN LABS

Bedankt voor je aandacht

Elmer Lastdrager
elmer.lastdrager@sidn.nl

https://www.sidnlabs.nl