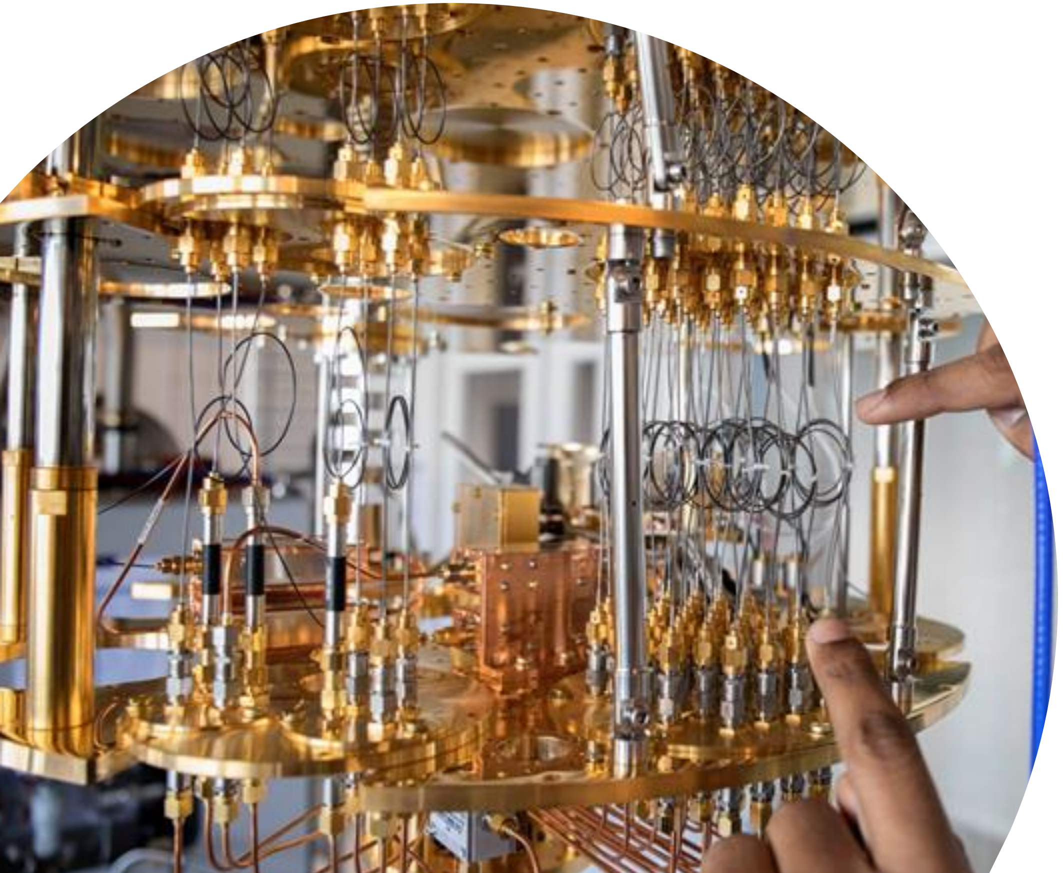


A testbed to evaluate post-quantum cryptography for DNSSEC

Caspar Schutijser

Radboud Digital Security group Lunch Talk
October 2, 2024

SIDN LABS

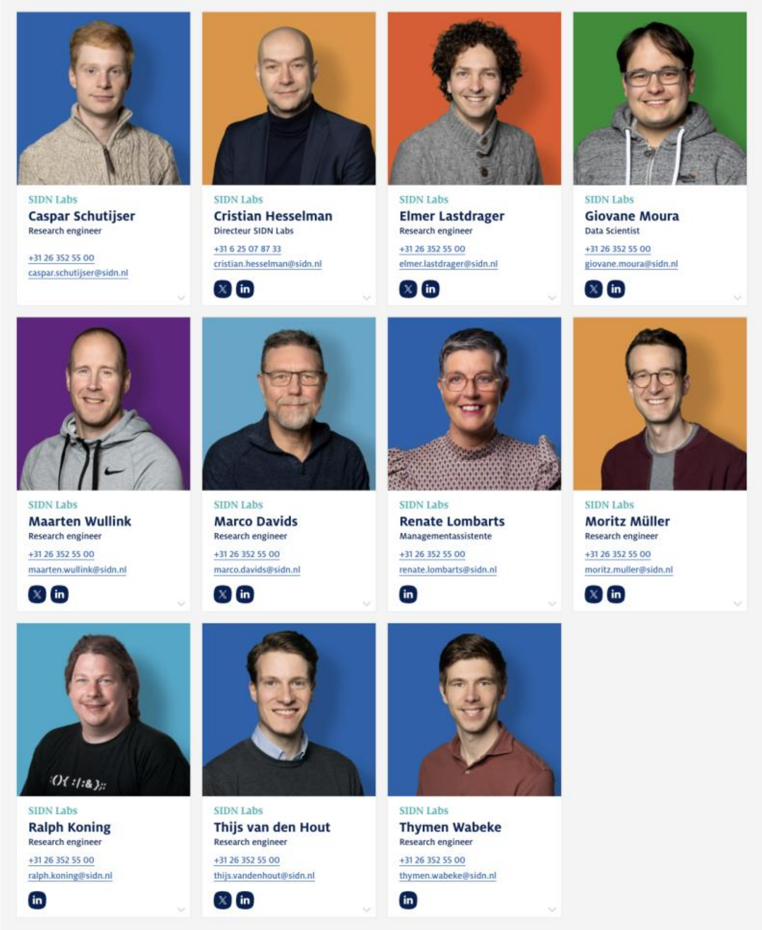
.nl

SIDN Labs is the research arm of SIDN

- Goal: further increase the security of the Internet, with a special focus on .nl and the Netherlands

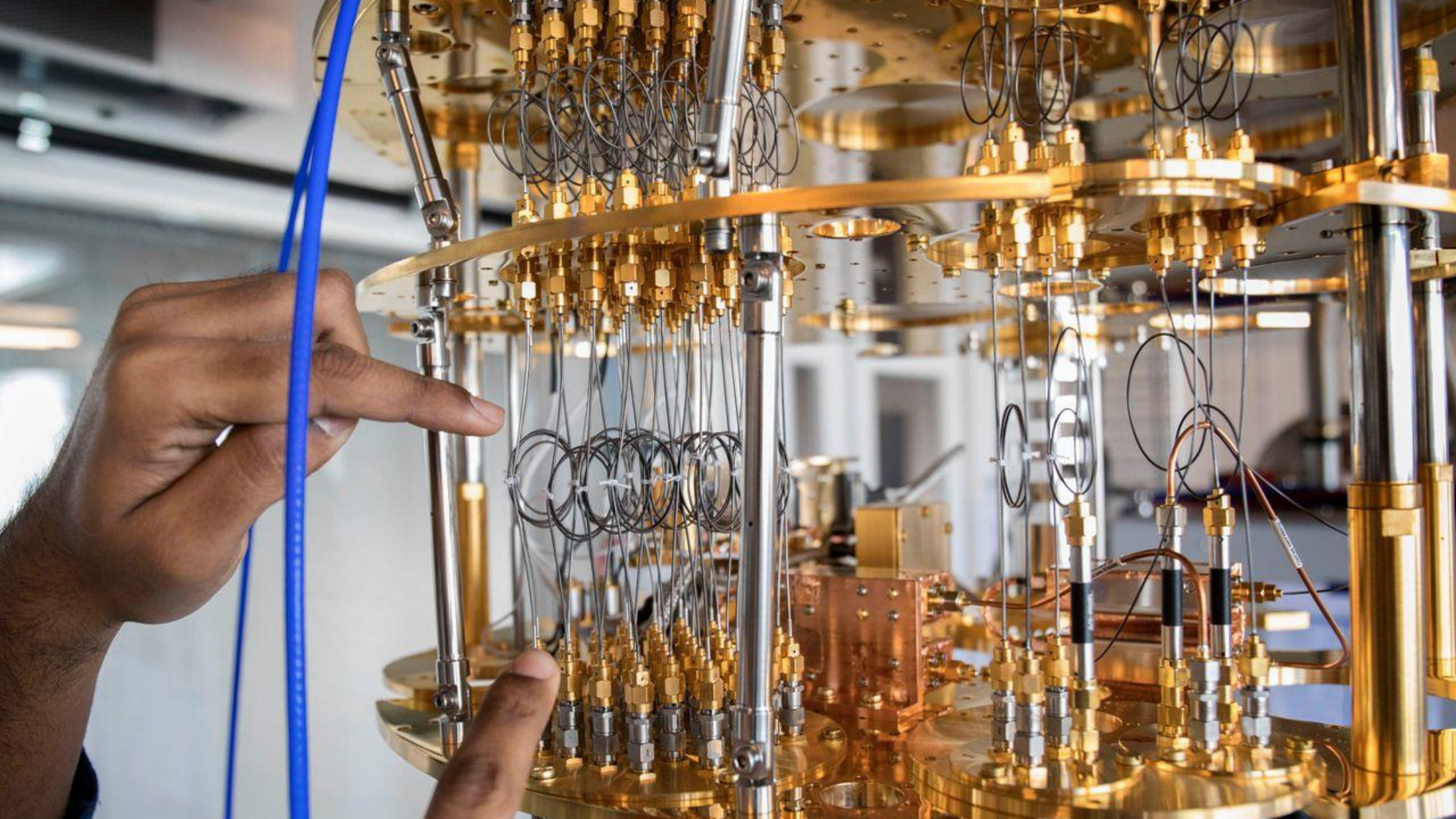
- Applied technical research: large-scale Internet measurements, prototyping new Internet systems, evaluating them, contributing to standards

- Results are public and generic (e.g., measurement methods and insights, designs, software) plus SIDN-specific adaptations for SIDN teams



SIDN LABS


KWANTUM
KWANTUM
KWANTUM
KWANTUM



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

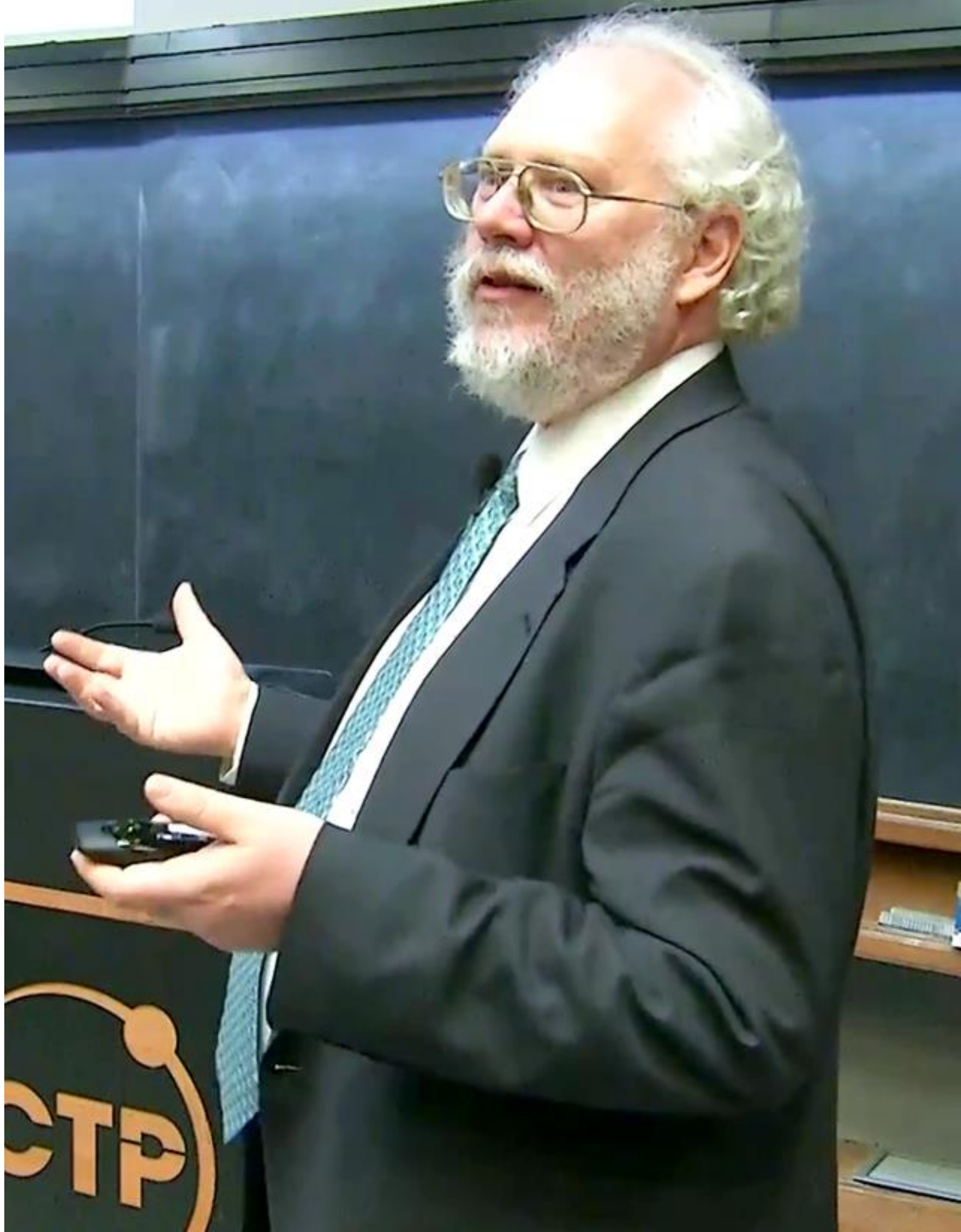
Peter W. Shor†

Abstract

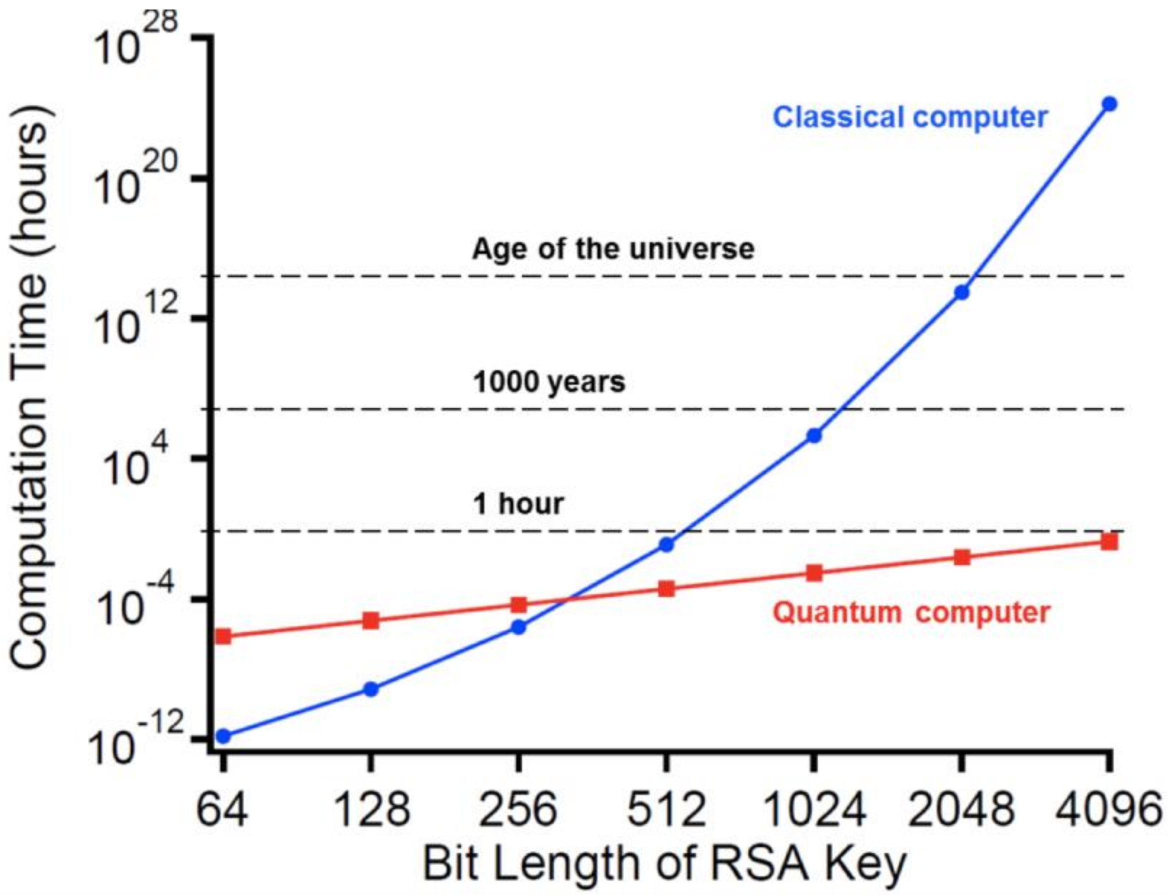
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration.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

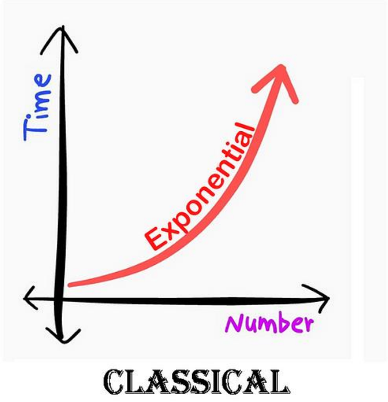
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

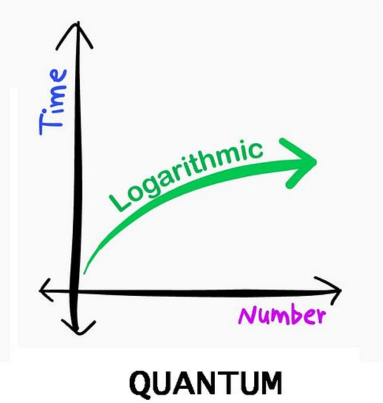
AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10



Quantum computers and cryptographic keys







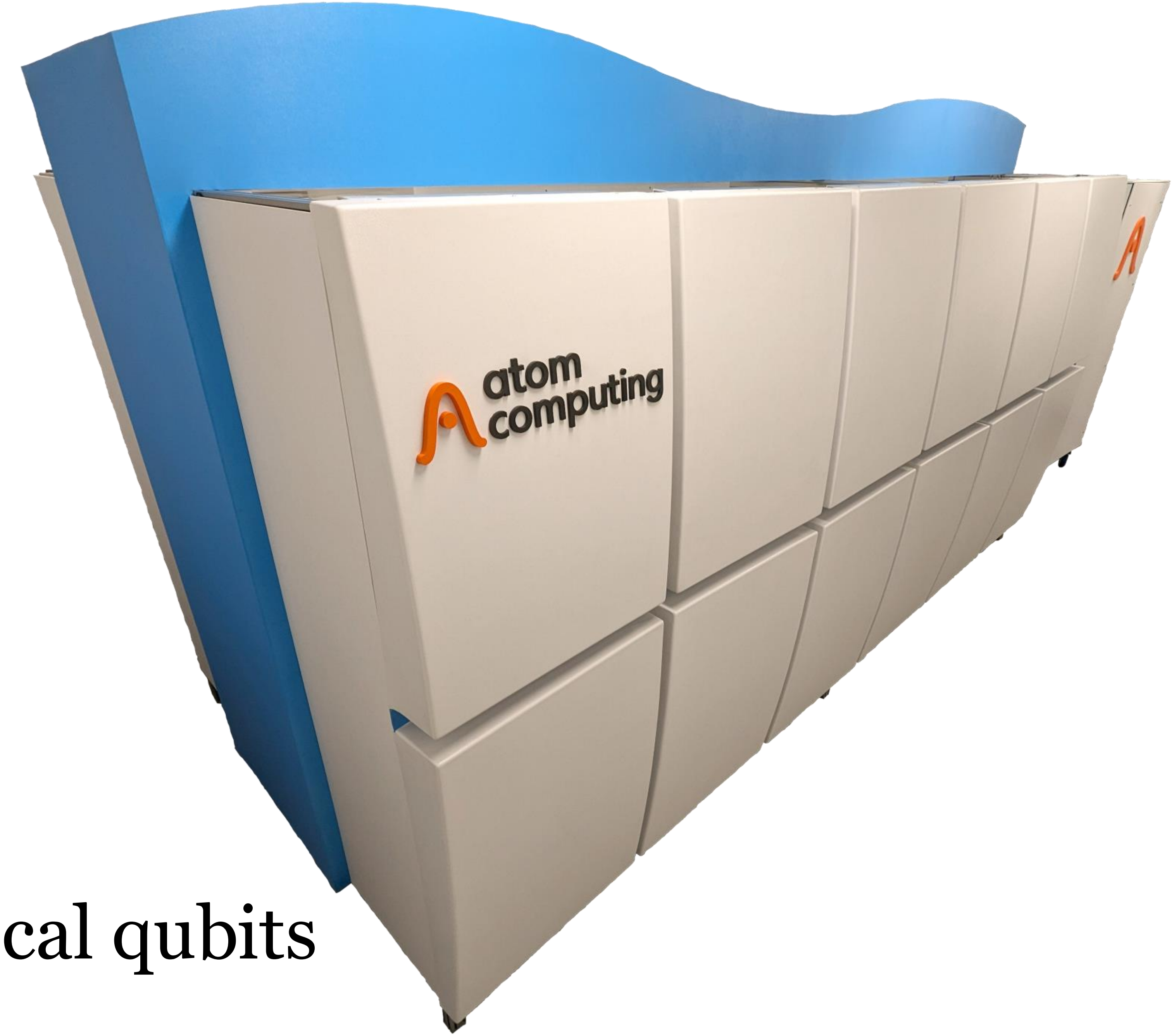
TECHNOLOGIE

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

SIDN LABS



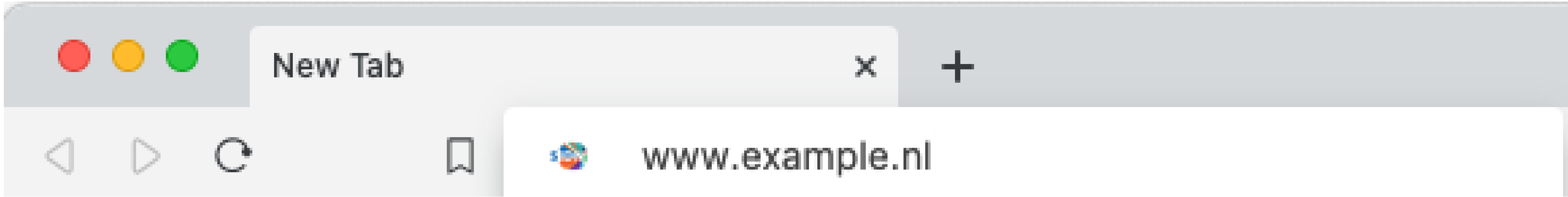
1180 physical qubits

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

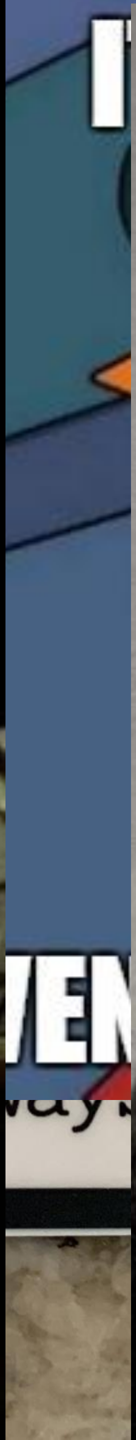
SIDN LABS

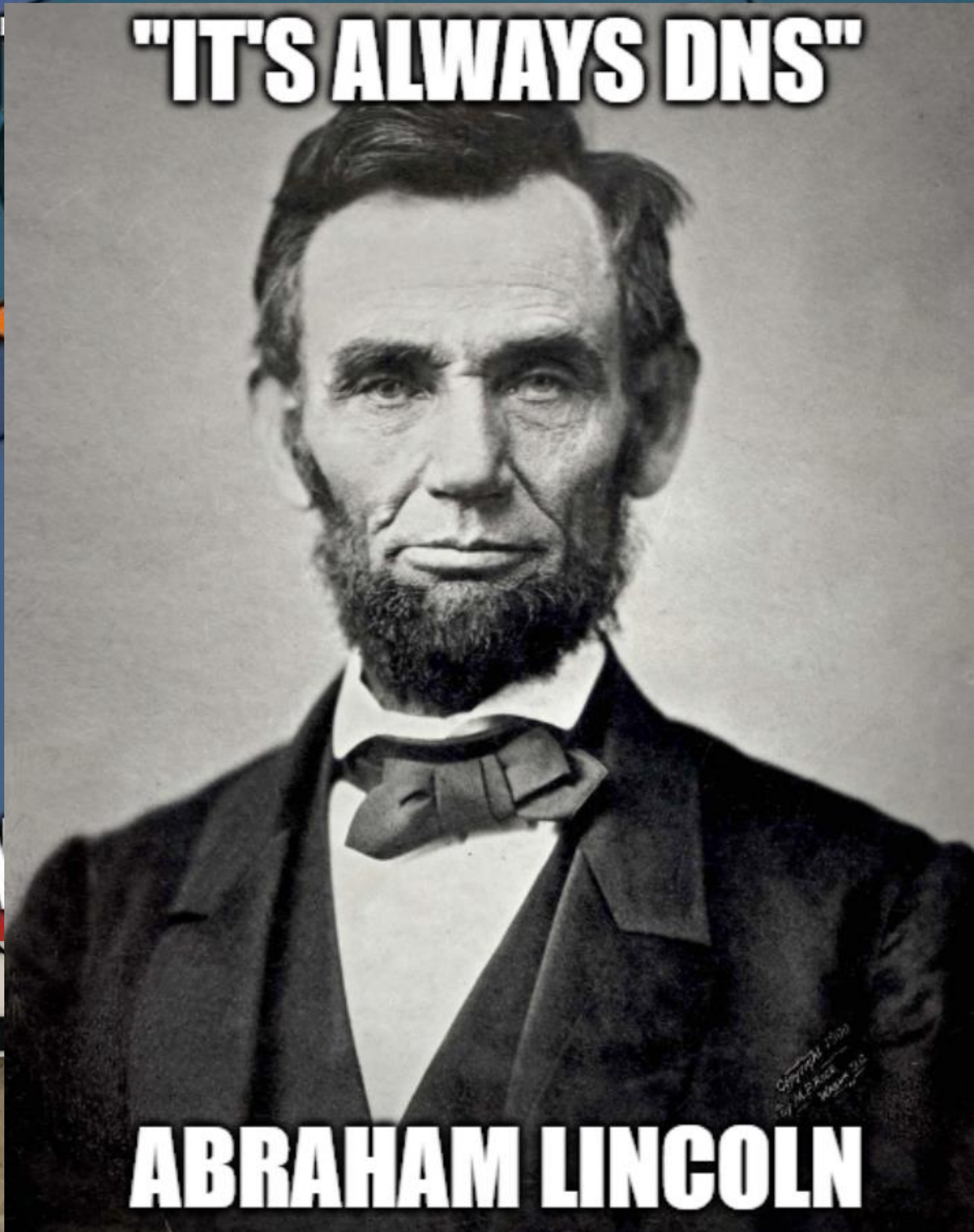

SIDN
IDN

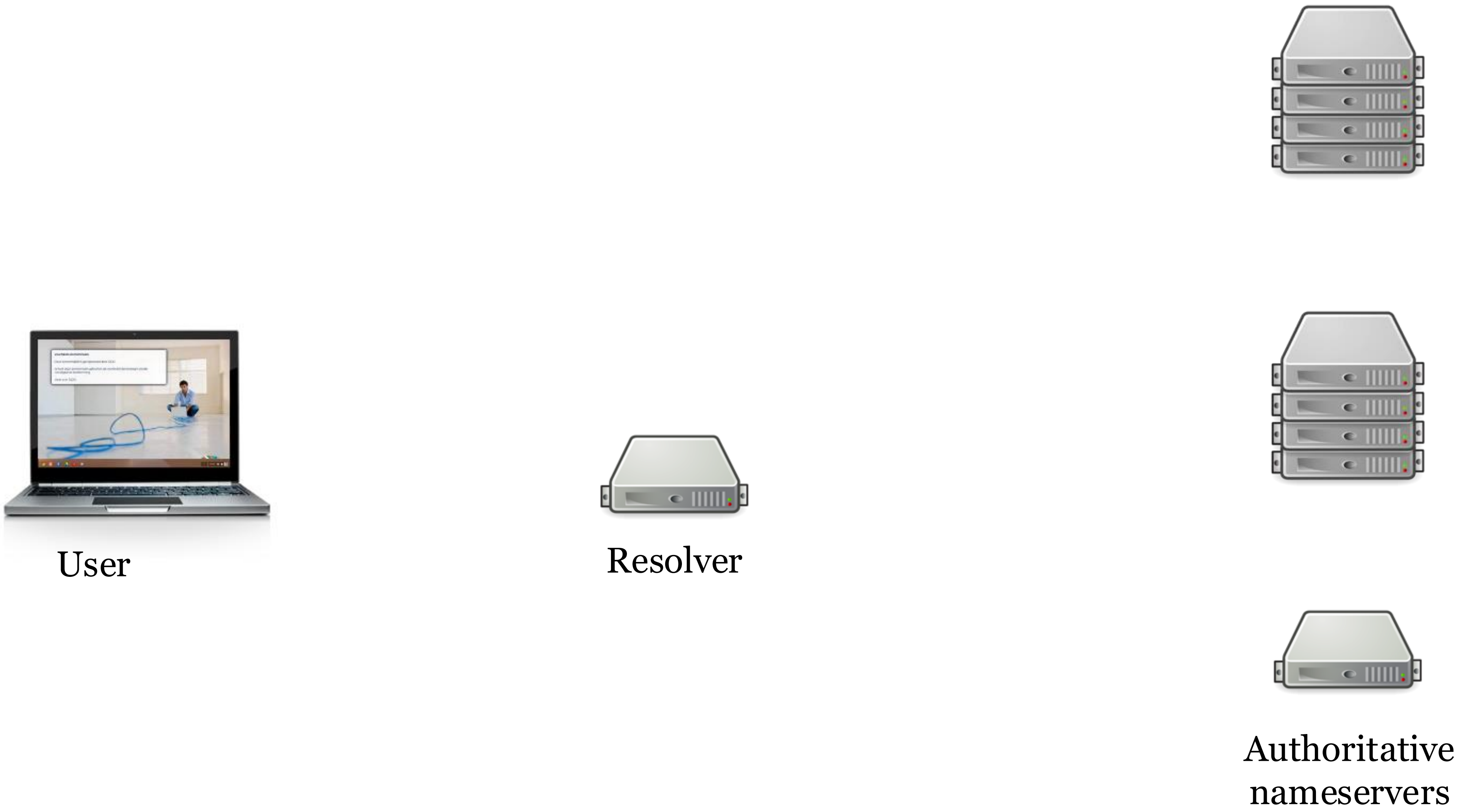


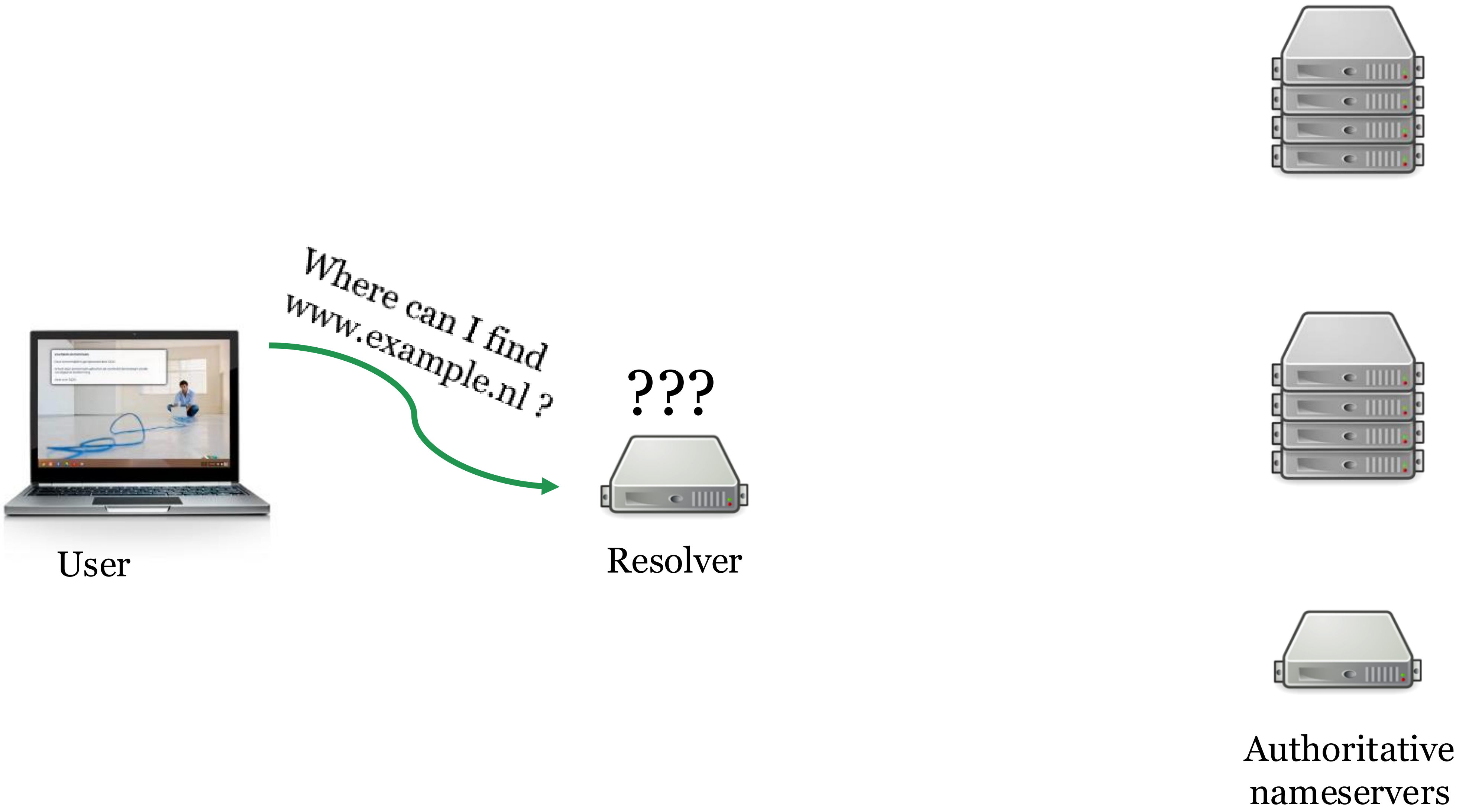
2a00:d78:0:712:94:198:159:35

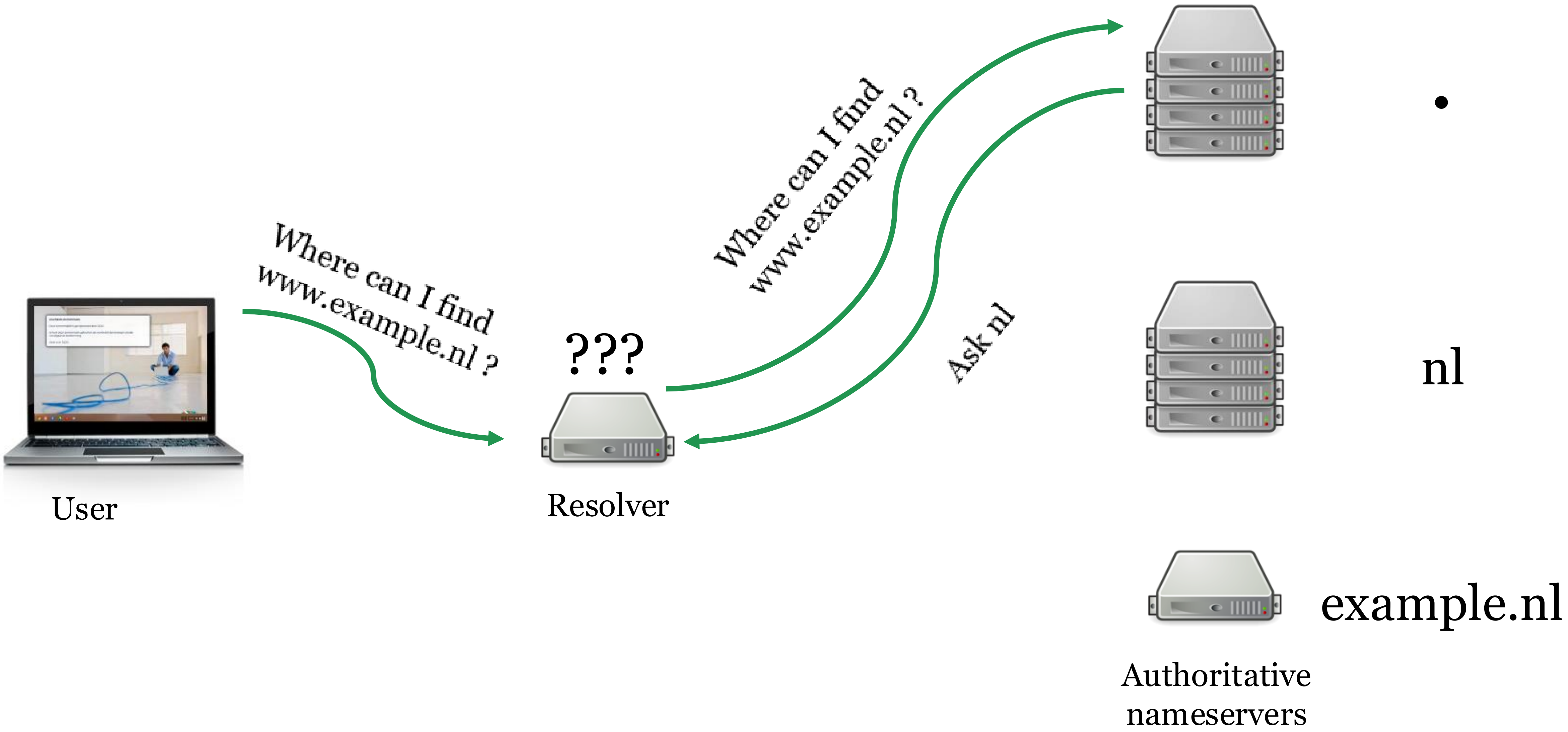

Why is it when something happens, it's always you three?
DNS
BGP
DHCP

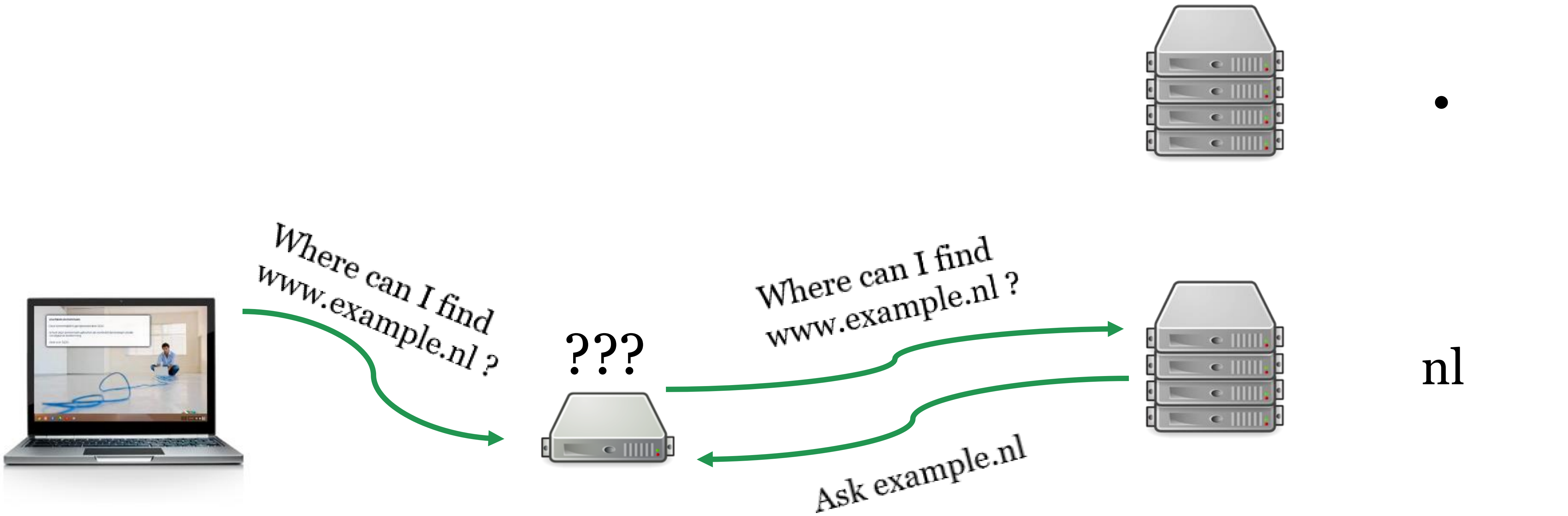



"IT'S ALWAYS DNS"
ABRAHAM LINCOLN

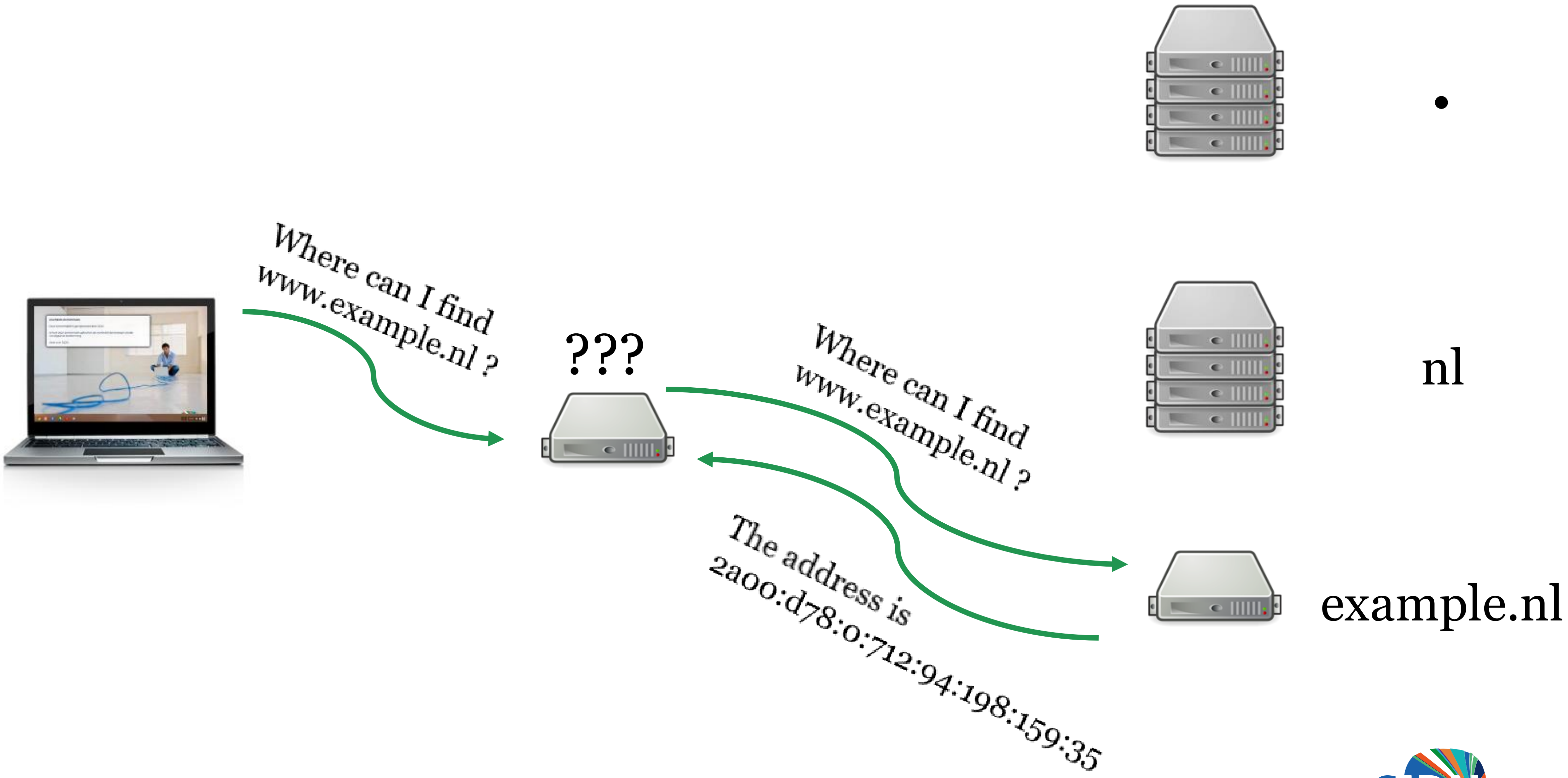

User
Resolver
Authoritative nameservers


Where can I find www.example.nl ?
???
User
Resolver
Authoritative nameservers

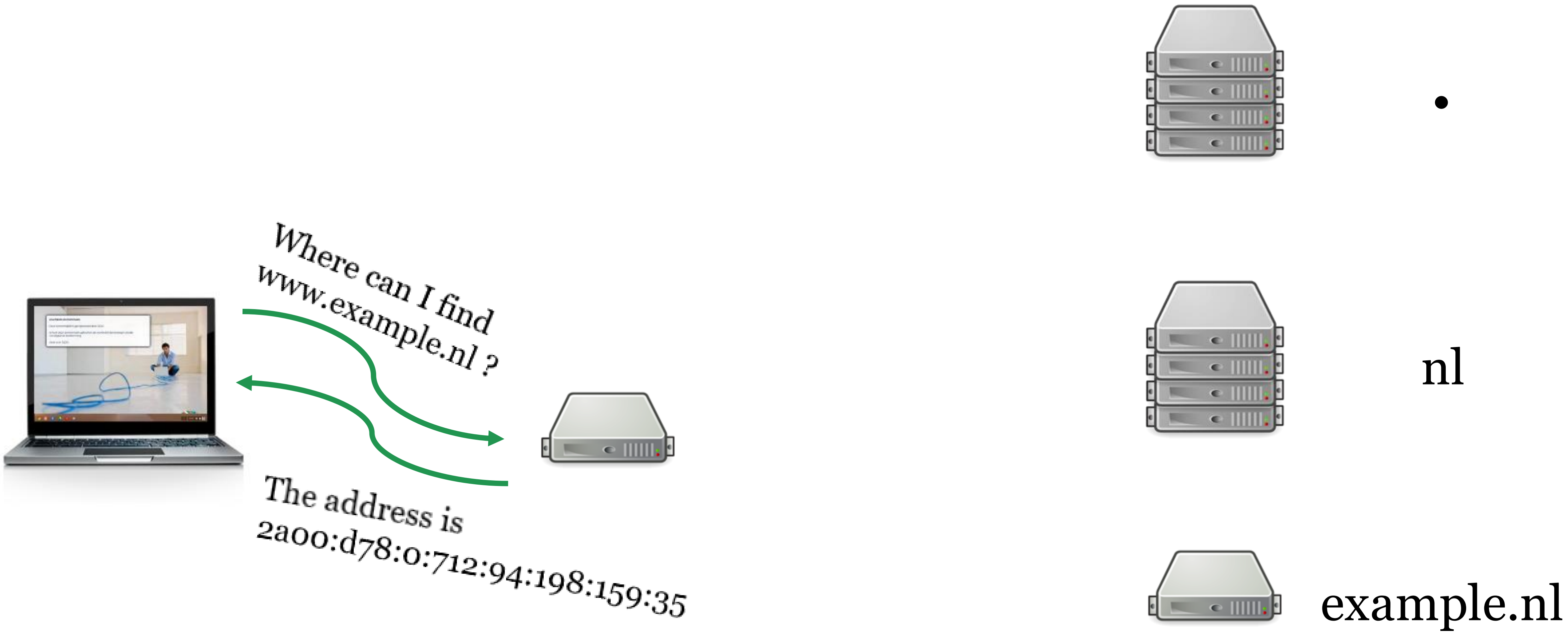

Where can I find www.example.nl ?
???
Where can I find www.example.nl ?
Ask nl
.
nl
example.nl
User
Resolver
Authoritative nameservers

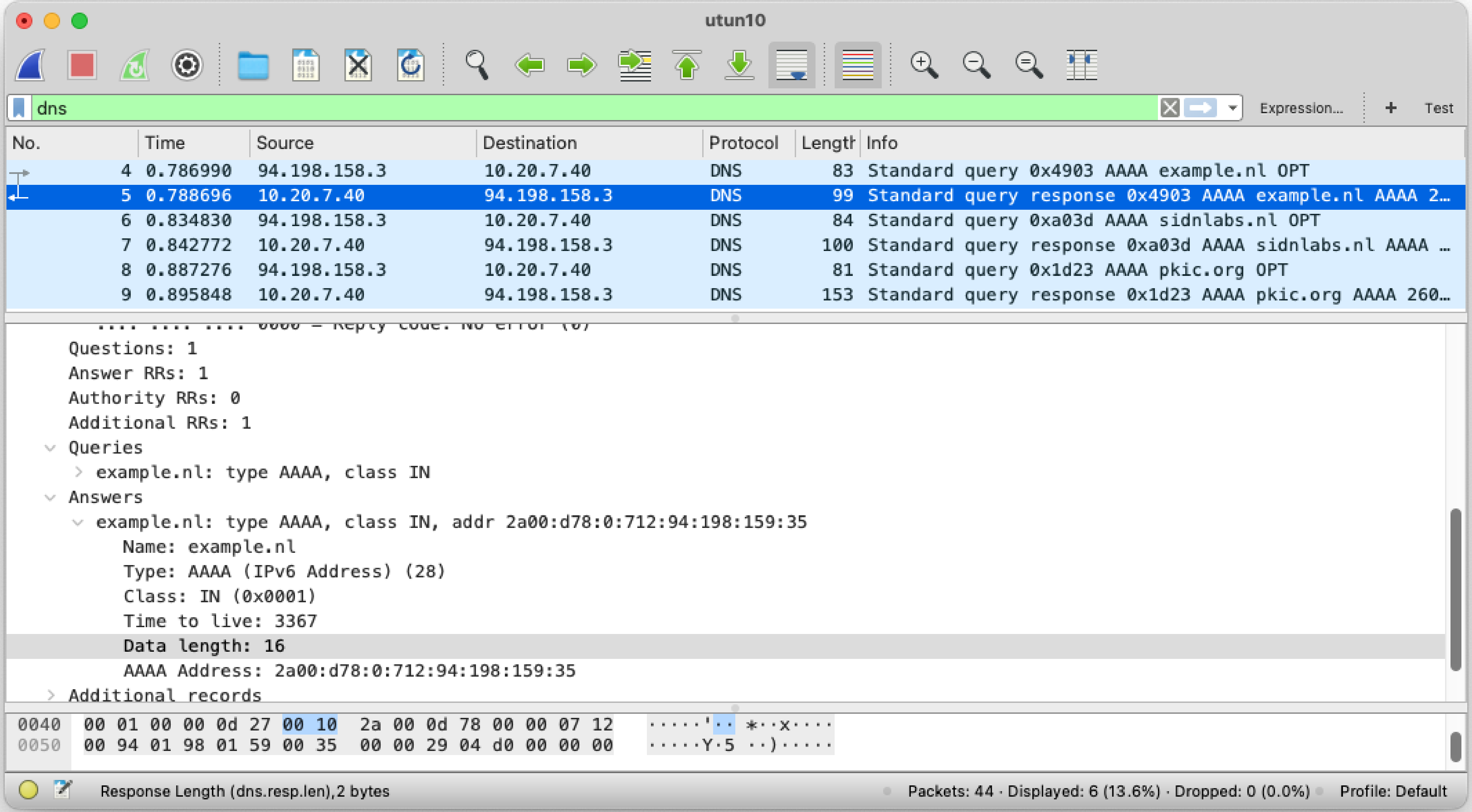


Where can I find www.example.nl ?
???
Where can I find www.example.nl ?
Ask example.nl
.
nl
example.nl



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


Where can I find
www.example.nl ?
The address is
2a00:d78:0:712:94:198:159:35
.
nl
example.nl



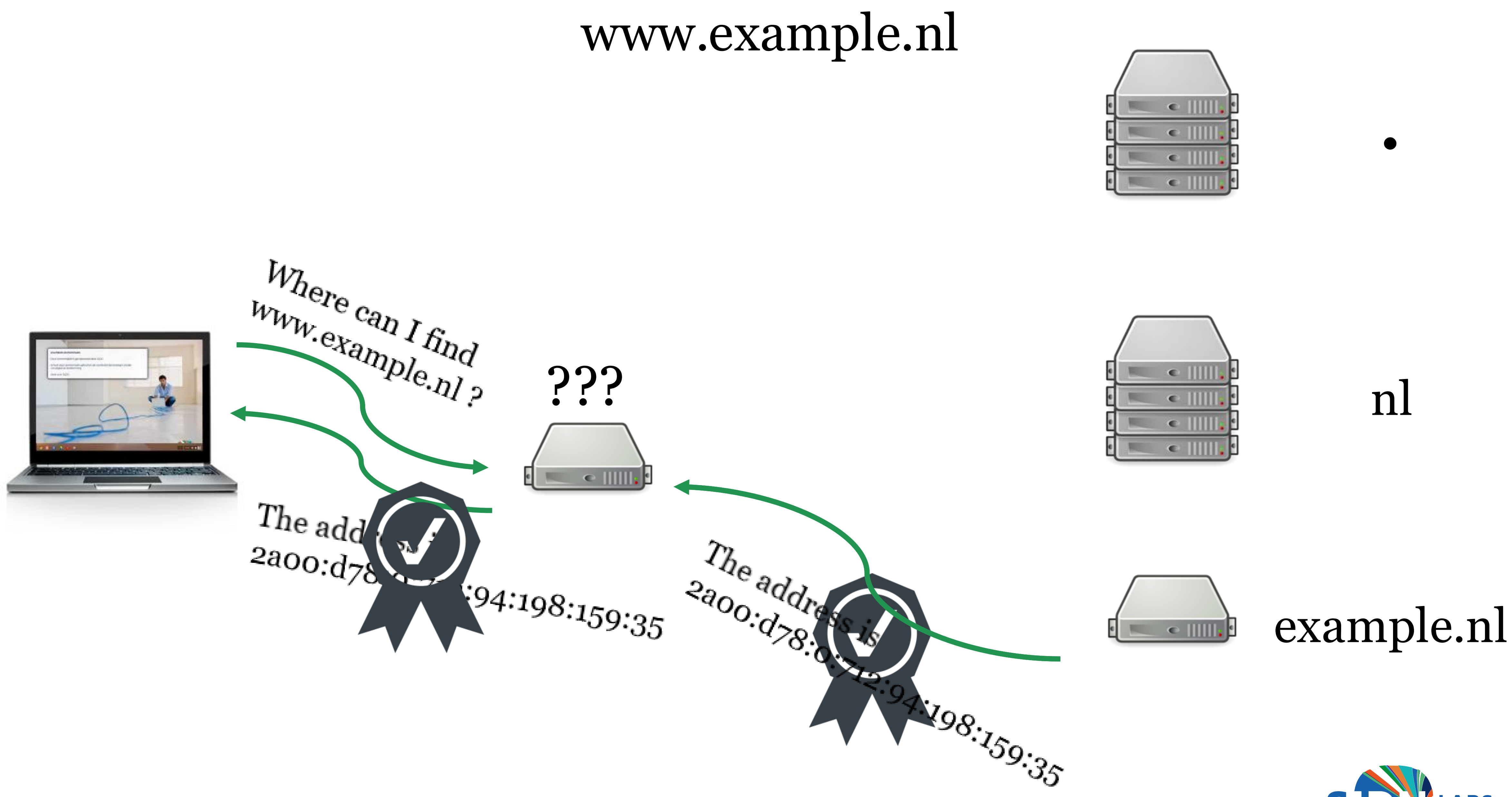
utun10
dns
Expression…
+
Test
No.
Time
Source
Destination
Protocol
Length
Info
4 0.786990 94.198.158.3 10.20.7.40 DNS 83 Standard query 0x4903 AAAA example.nl OPT
5 0.788696 10.20.7.40 94.198.158.3 DNS 99 Standard query response 0x4903 AAAA example.nl AAAA 2…
6 0.834830 94.198.158.3 10.20.7.40 DNS 84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

SIDN LABS

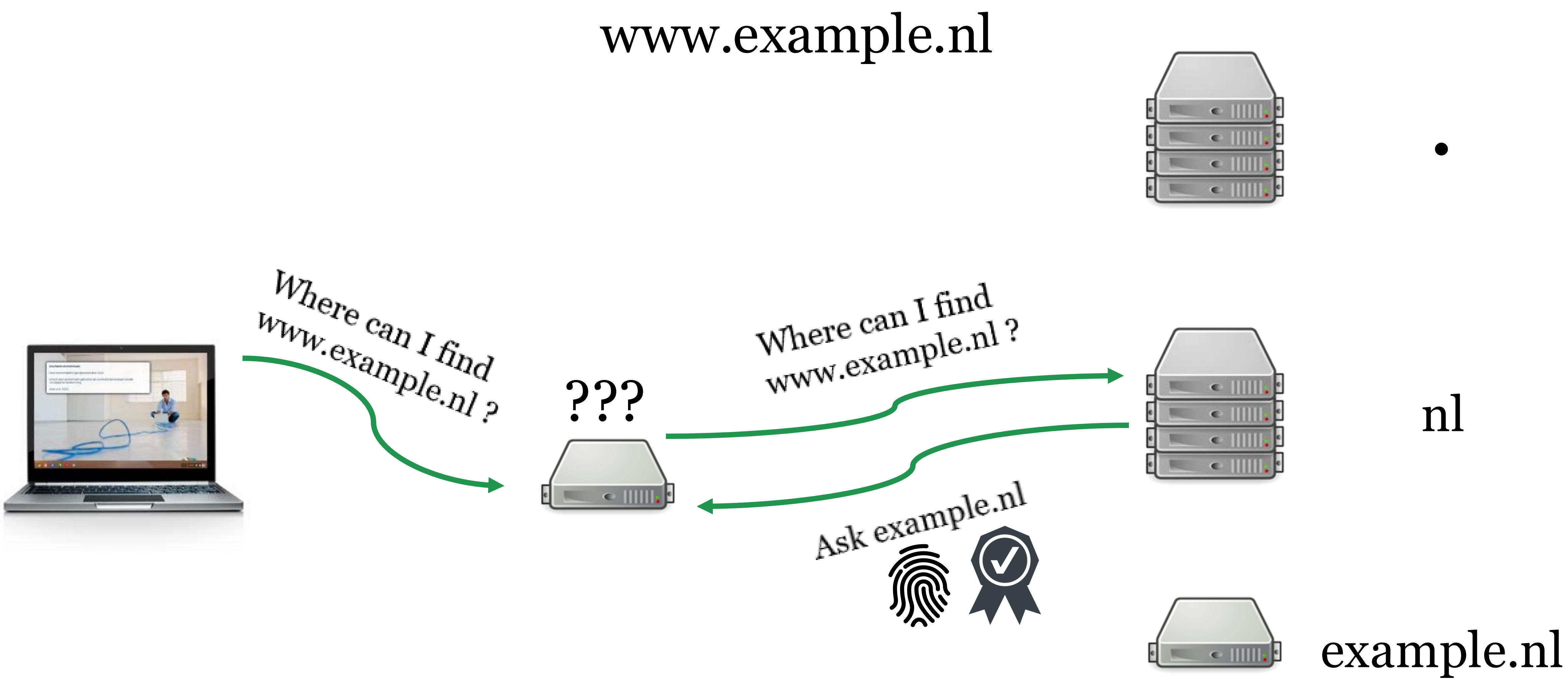
DoH, DoT, DNScrypt
https://dns4all.eu/

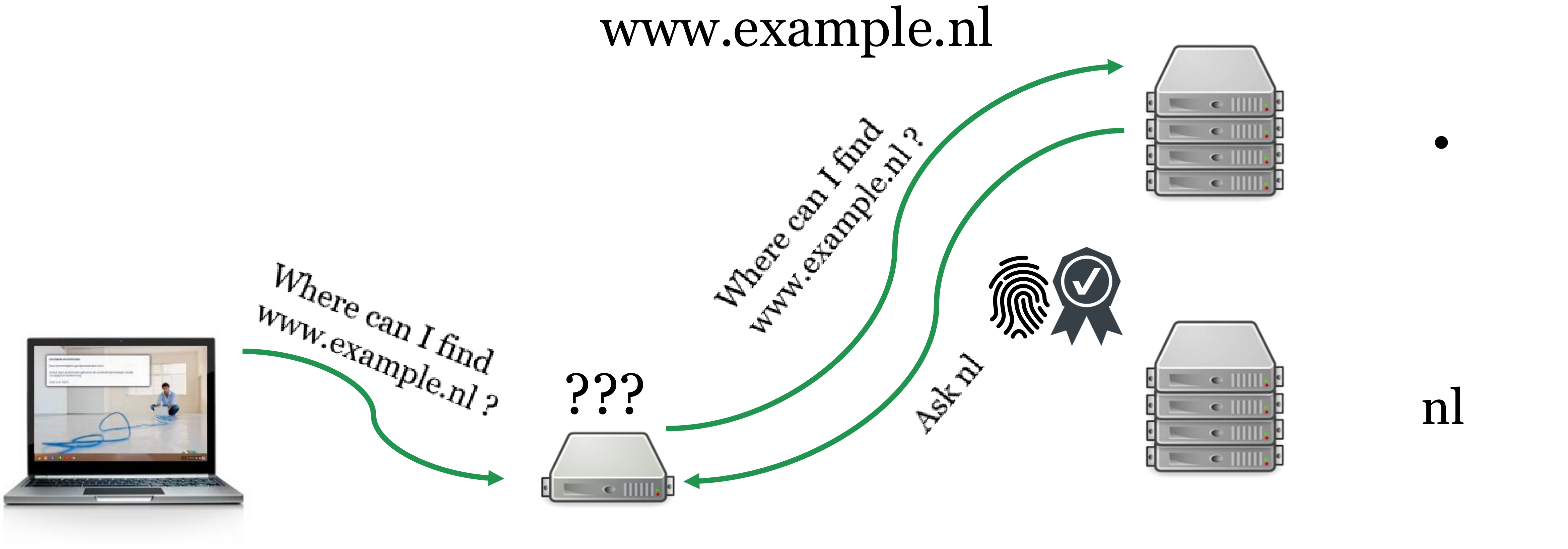
X25519Kyber768

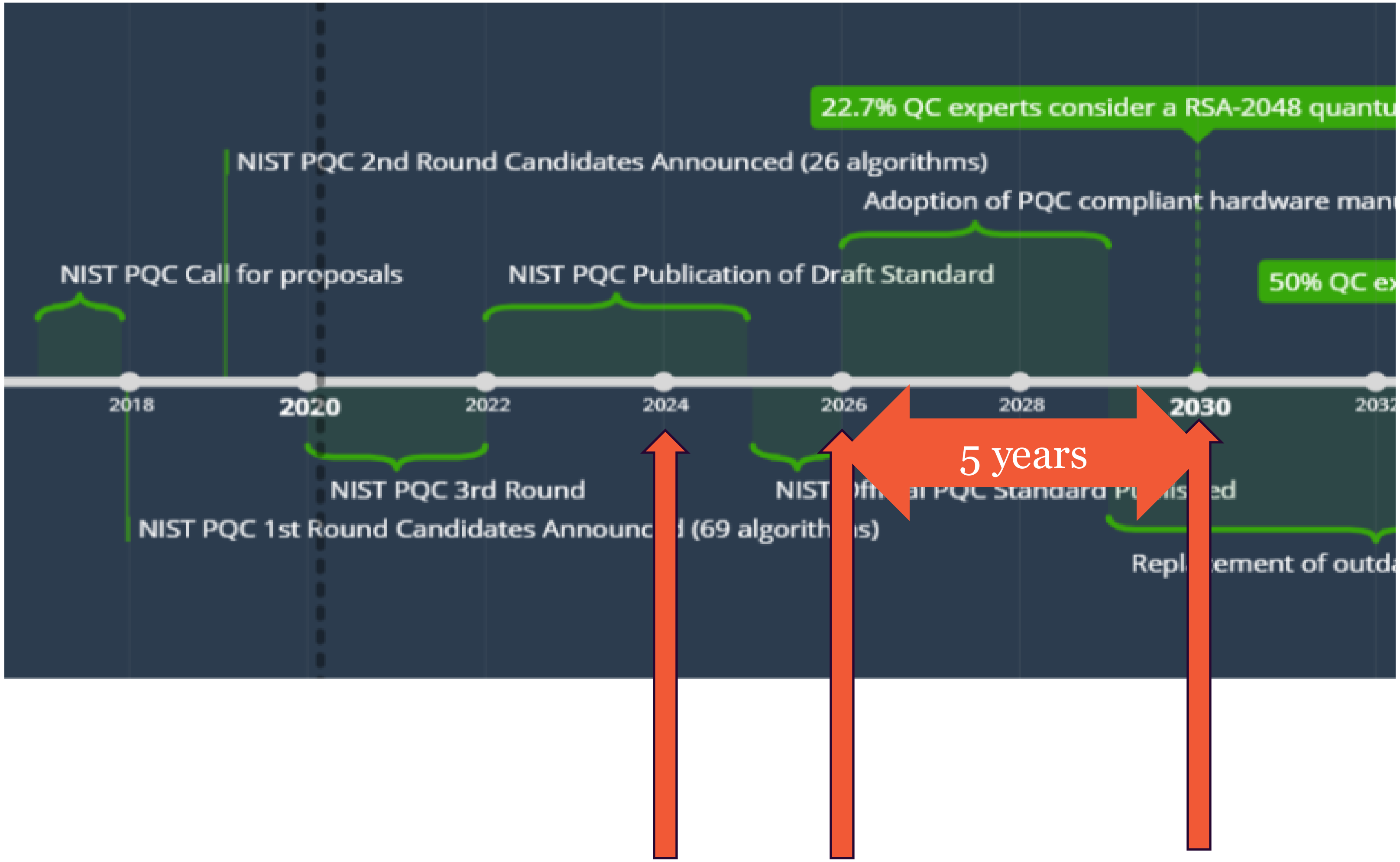
DNSSEC



www.example.nl
.
nl
example.nl
Where can I find
www.example.nl ?
???
The add
2a00:d78
:94:198:159:35
The address is
2a00:d78:0:712:94:198:159:35


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

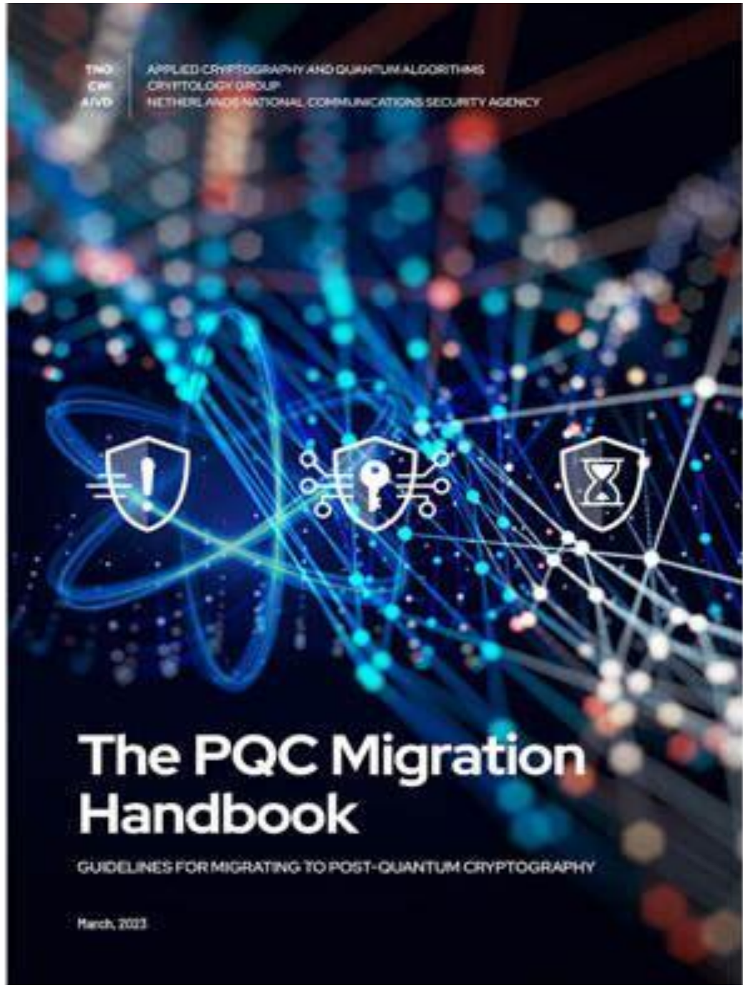

www.example.nl
Where can I find www.example.nl ?
???
Where can I find www.example.nl ?
Ask nl
.
nl
example.nl



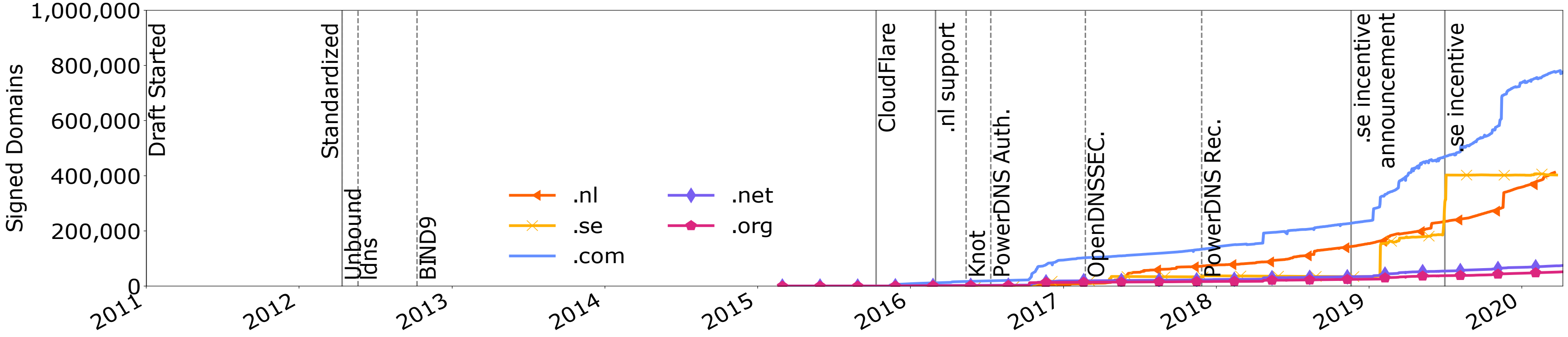
We're here

PQC standards available

DNSSEC vulnerable (perhaps)



Time to deploy new algorithm in DNSSEC, +- 10 years



Timeline showing deployment of ECDSA256, from '*Making DNSSEC Future Proof*' by dr. Moritz Müller.


Requirements

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.

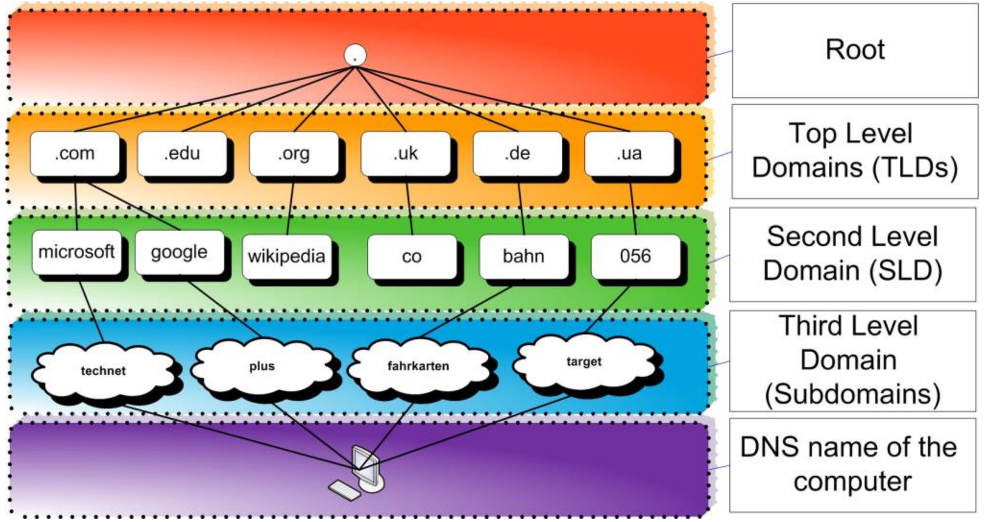
M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

SIDN LABS

Jürgen Henn – 11foot8.com


gifbin.com

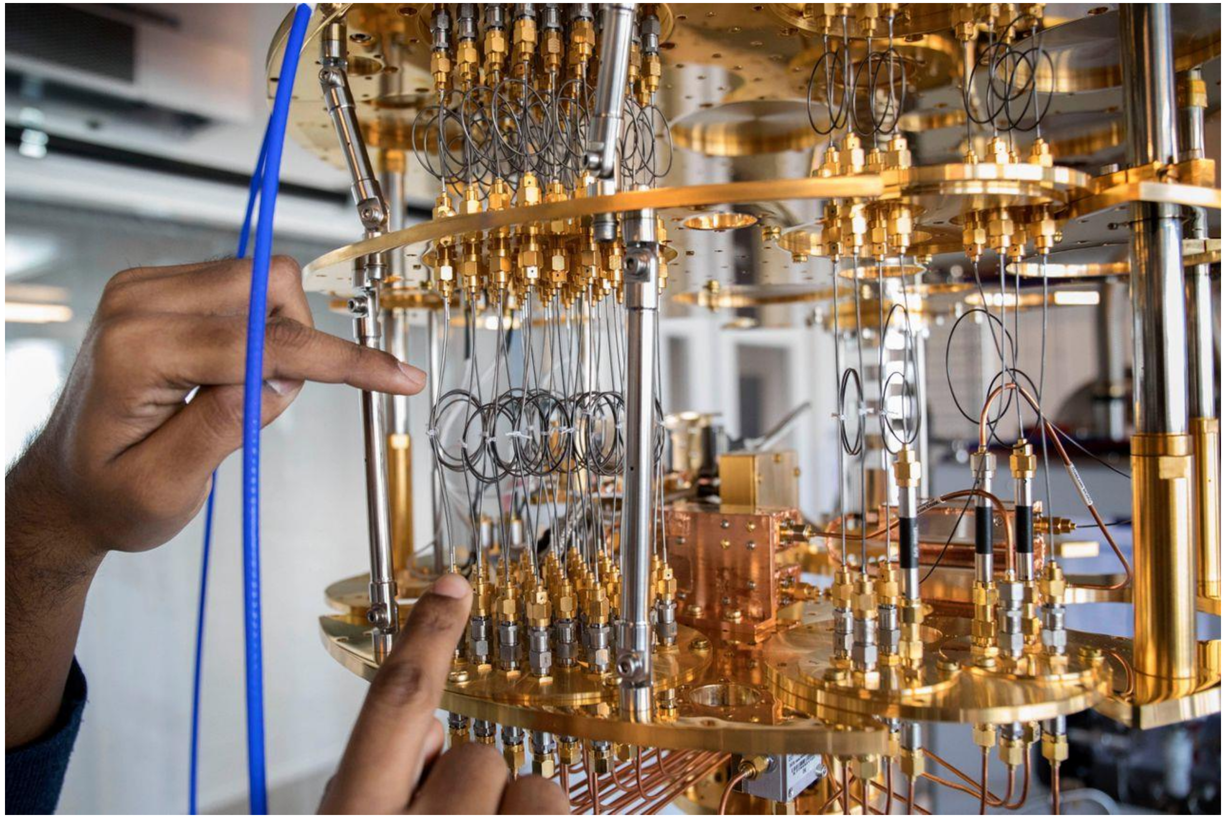

DNS


.
.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

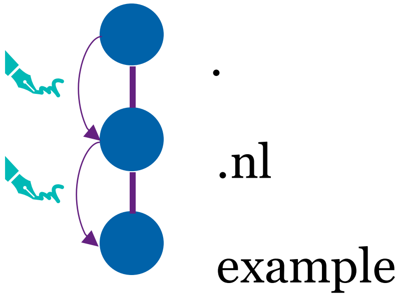
SIDN LABS

Post-quantum Algorithms Testing and Analysis for the DNS



PATAD testbed: plan and experiment

1) Test infrastructure

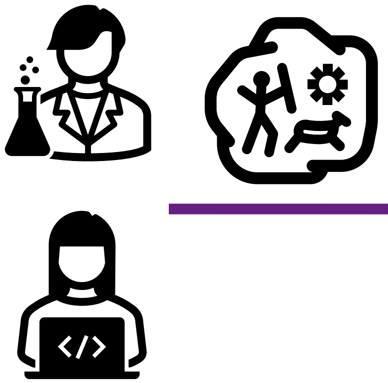


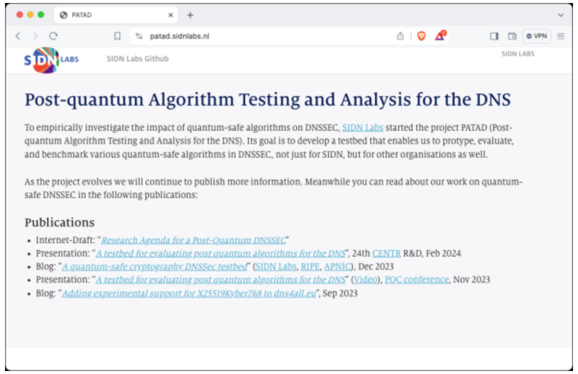
2) The PQC algorithm that we want to test

3) The measurements we want to perform

Sign 100x, verify 100x, calculate the averages

PATAD testbed: building a testbed





PATAD

patad.sidnlabs.nl

SIDN Labs Github

SIDN LABS

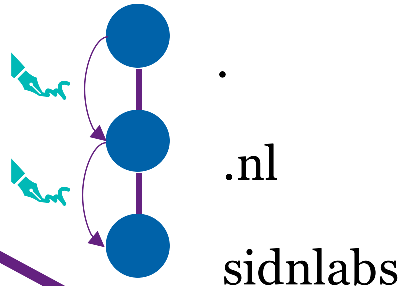
Post-quantum Algorithm Testing and Analysis for the DNS

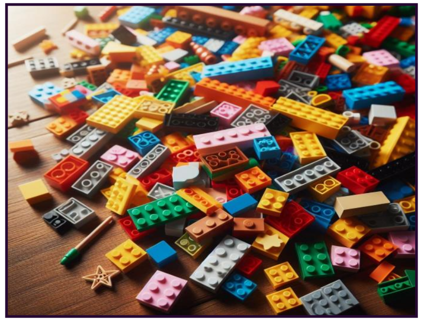
To empirically investigate the impact of quantum-safe algorithms on DNSSEC, SIDN Labs started the project PATAD (Post-quantum Algorithm Testing and Analysis for the DNS). Its goal is to develop a testbed that enables us to protype, evaluate, and benchmark various quantum-safe algorithms in DNSSEC, not just for SIDN, but for other organisations as well.

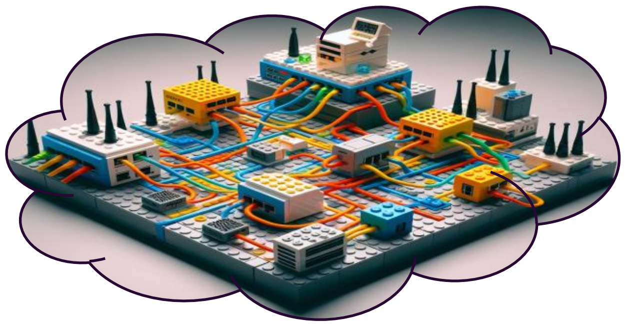
As the project evolves we will continue to publish more information. Meanwhile you can read about our work on quantum-safe DNSSEC in the following publications:

Publications

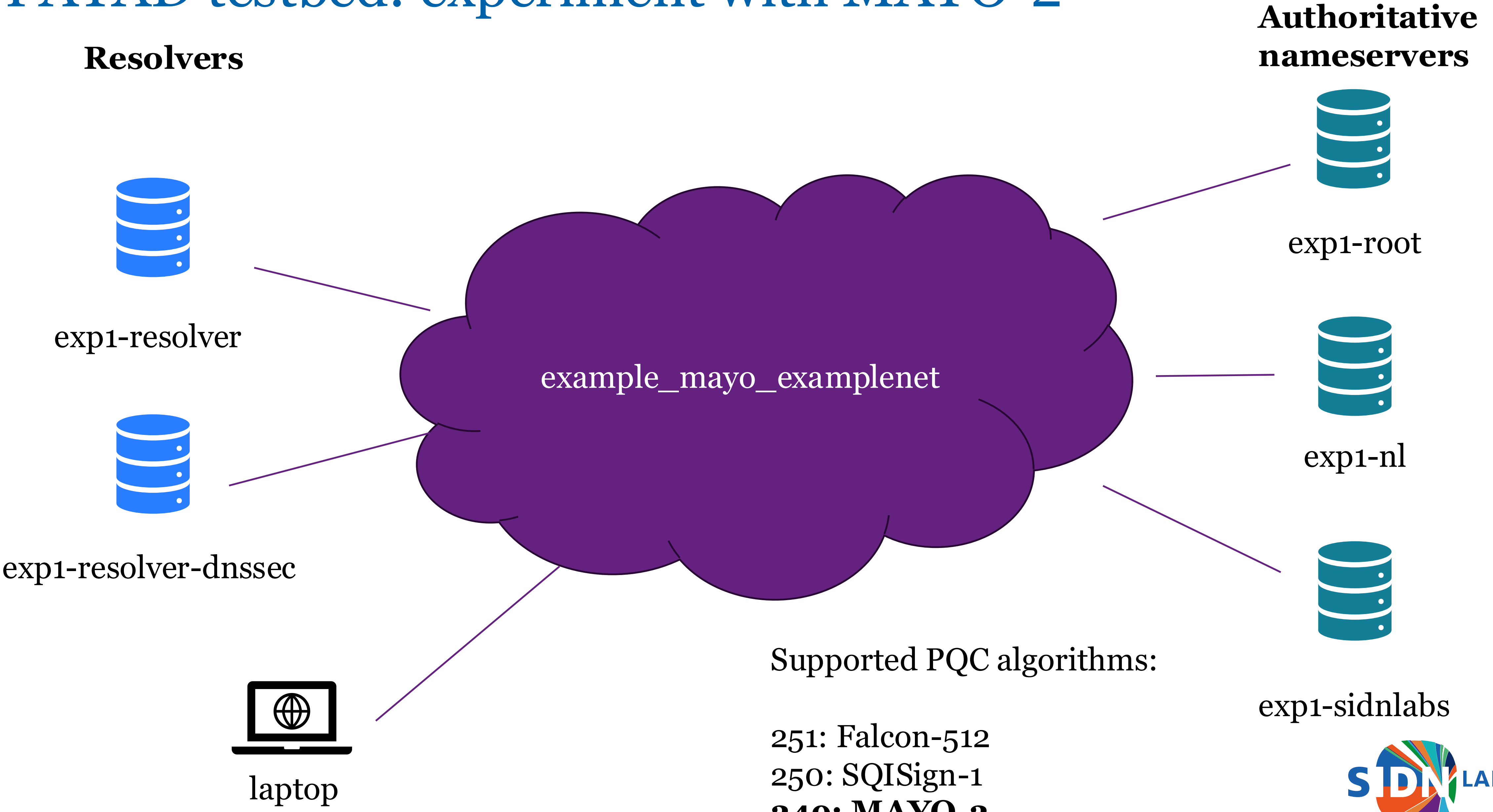
- Internet-Draft: "*Research Agenda for a Post-Quantum DNSSEC*"
- Presentation: "*A testbed for evaluating post quantum algorithms for the DNS*", 24th CENTR R&D, Feb 2024
- Blog: "*A quantum-safe cryptography DNSSec testbed*" (SIDN Labs, RIPE, APNIC), Dec 2023
- Presentation: "*A testbed for evaluating post quantum algorithms for the DNS*" (Video), PQC conference, Nov 2023
- Blog: "*Adding experimental support for X25519Kyber768 to dns4all.eu*", Sep 2023







PATAD testbed: experiment with MAYO-2

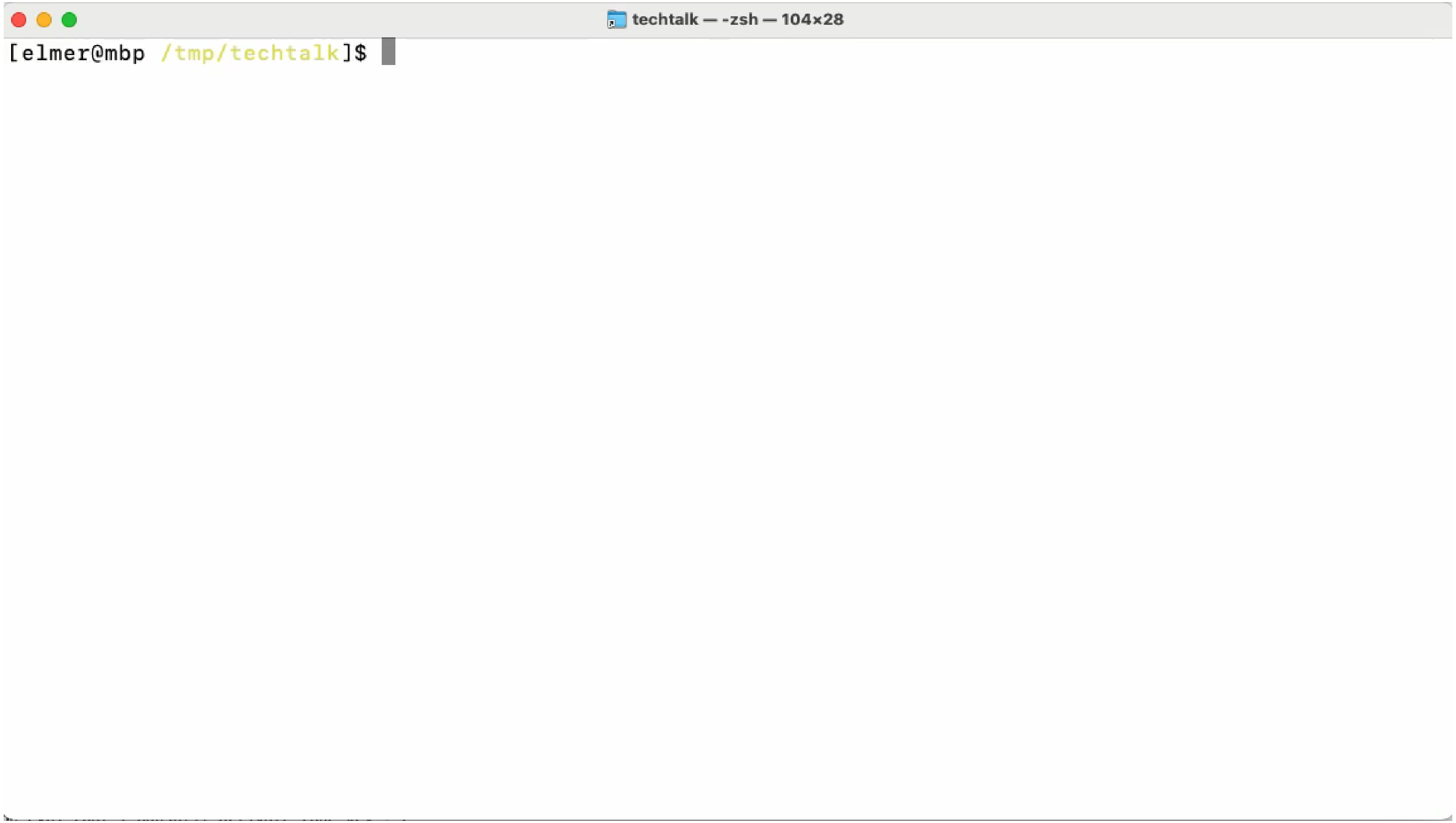


Supported PQC algorithms:

251: Falcon-512
250: SQISign-1
249: MAYO-2

SIDN LABS

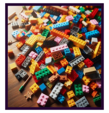
Demo?



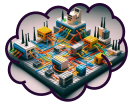
PATAD testbed is available as open source software

- Specify your own topology.
- Run your own experiments!
- More information: patad.sidnlabs.nl

Next steps



Develop more PQC DNSSEC components



Improve testbed infrastructure

Perform experiments on our testbed

Encourage others to use testbed and to work together

PATAD blog appeared on:

RIPE Labs APNIC

Research partners:

SURF UNIVERSITY OF TWENTE.

SIDN LABS

Do your master's project at SIDN Labs?

https://www.sidnlabs.nl/en/graduating

Other vacancies (B.Sc. and M.Sc.):

https://www.sidn.nl/en/work-at-sidn

Wanna know more? Contact Inge Loeff at our HR team at inge.loeff@sidn.nl

Thanks for your attention

Caspar Schutijser
caspar.schutijser@sidn.nl

https://www.sidnlabs.nl

SIDN LABS