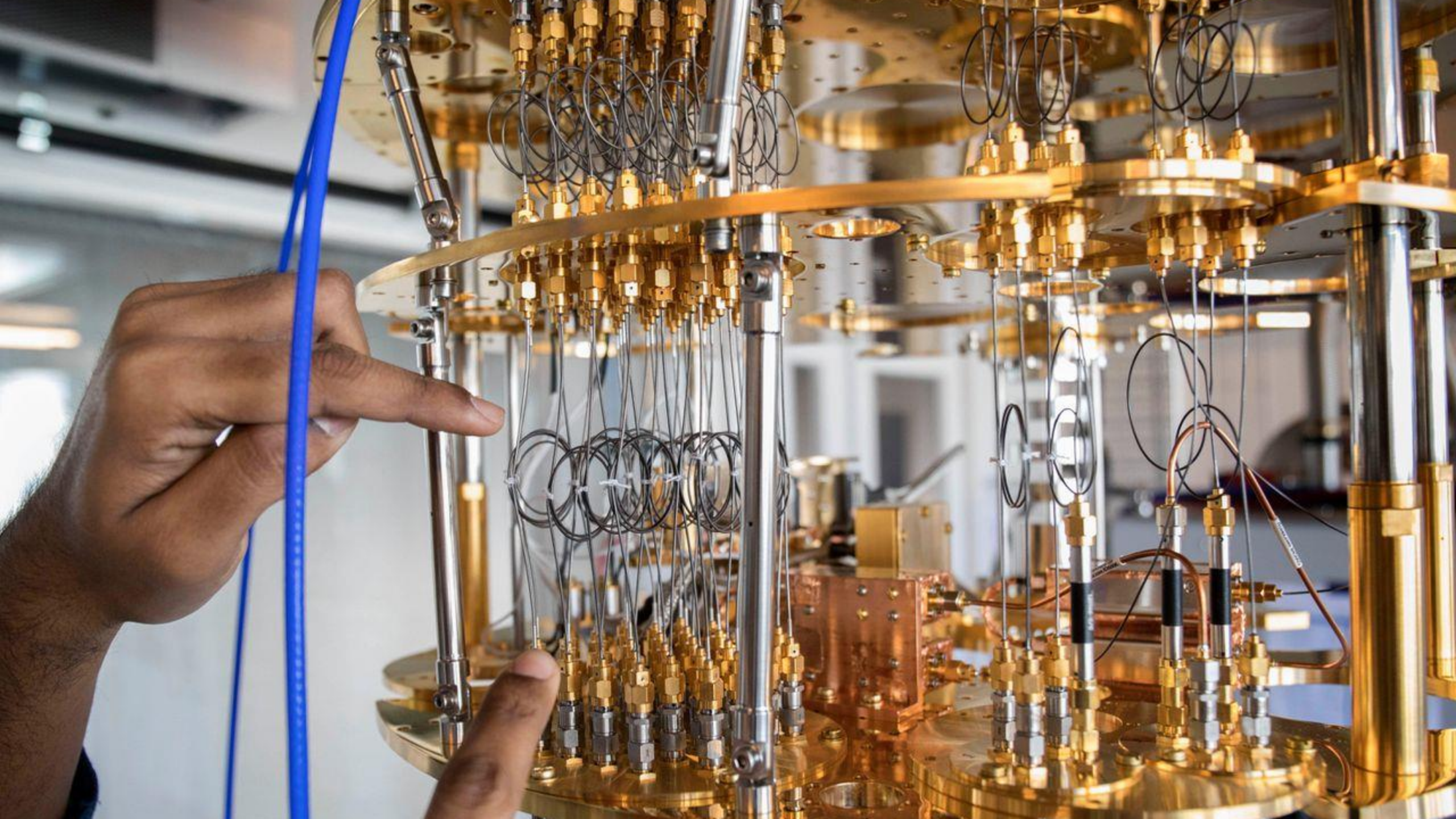


Evaluating Post-Quantum Cryptography for the Domain Name System

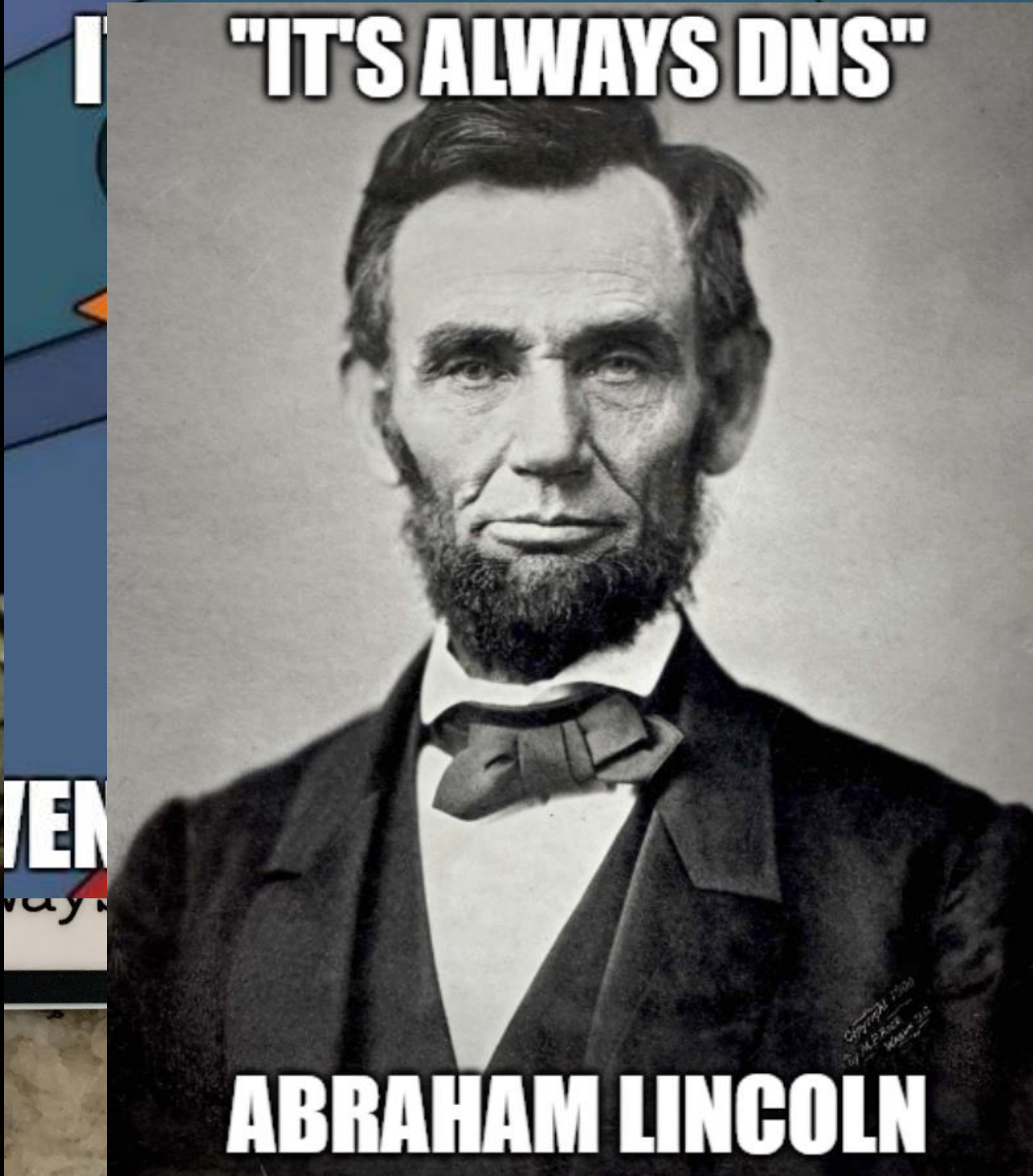
TUCCR Fall Workshop on Network Security
Research | Apeldoorn

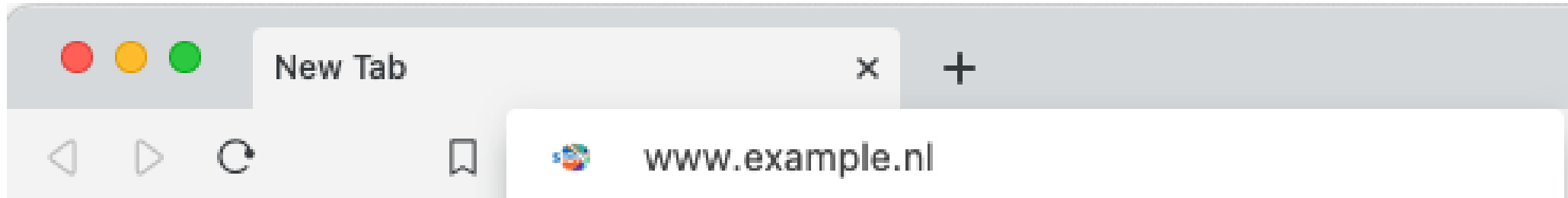
21 Oct 2024











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

utun10

dns

| 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... |

... Reply code: no error (0)

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 .....'. *..x....
0050 00 94 01 98 01 59 00 35 00 00 29 04 d0 00 00 00 .....Y.5 ..).....
  
```

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



.



nl



example.nl



Where can I find
www.example.nl ?

???



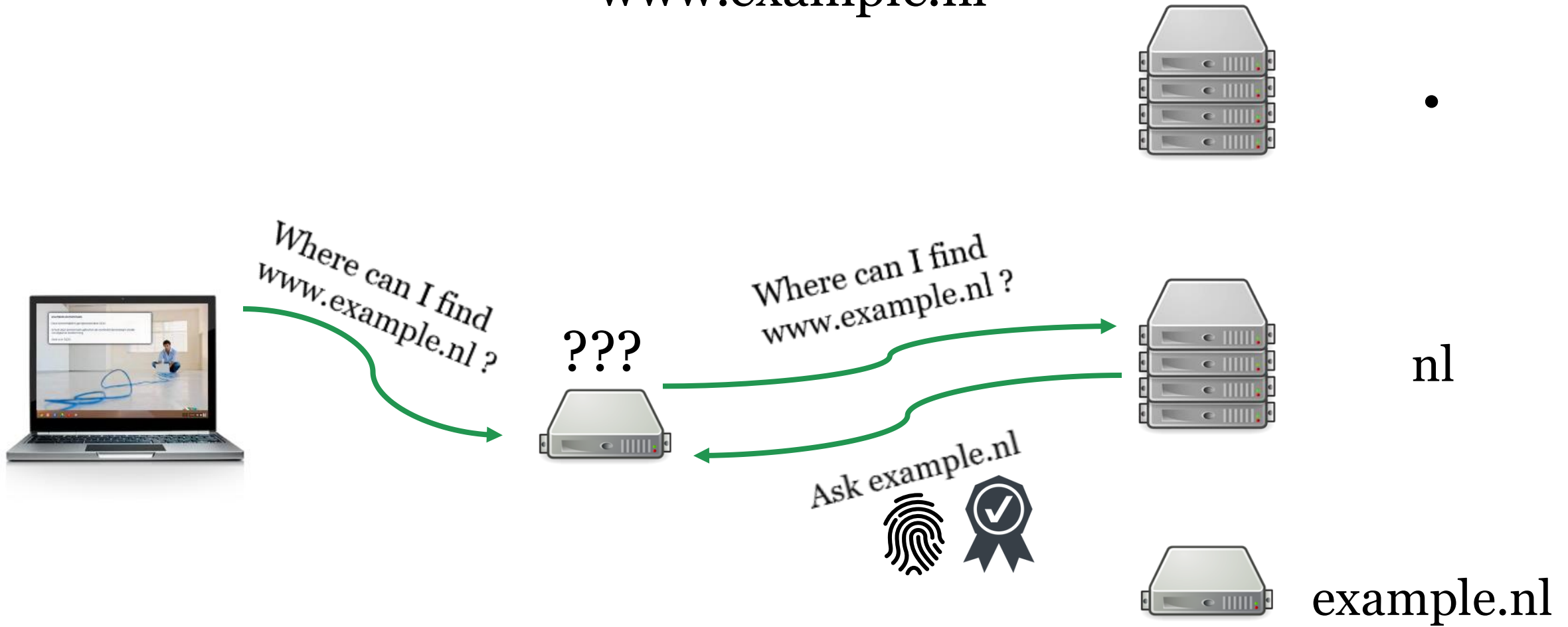
The address is
2a00:d78:0:112:94:198:159:35



The address is
2a00:d78:0:112:94:198:159:35



www.example.nl



www.example.nl



Where can I find
www.example.nl ?



Where can I find
www.example.nl ?

Ask nl





nl

example.nl



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

Table 2: Requirements for quantum-safe algorithms.

| 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 |
| SQLsign | l | 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 |
| SQLsign | I | 1 | 5,669,000,000 | 108,000,000 |
| VOX | 128 | 1 | 664,265 | 168,567 |

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



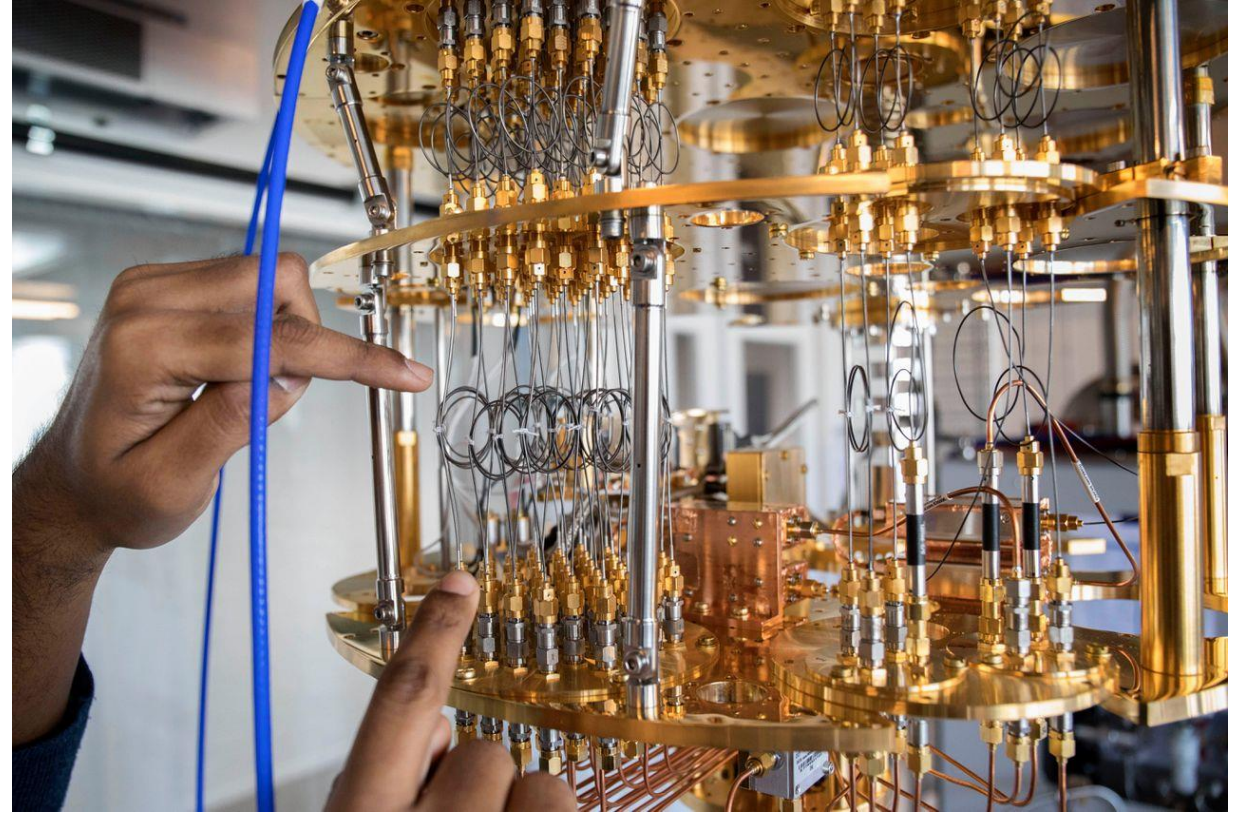


Jürgen Henn – 11foot8.com



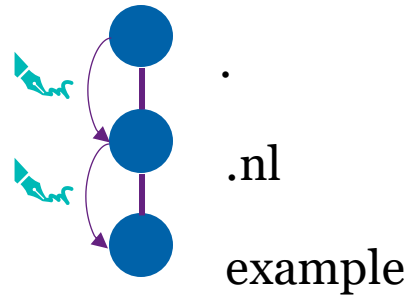


Post-quantum Algorithms Testing and Analysis for the DNS



PATAD testbed: plan and experiment

1) Test infrastructure



2) The PQC algorithm that we want to test

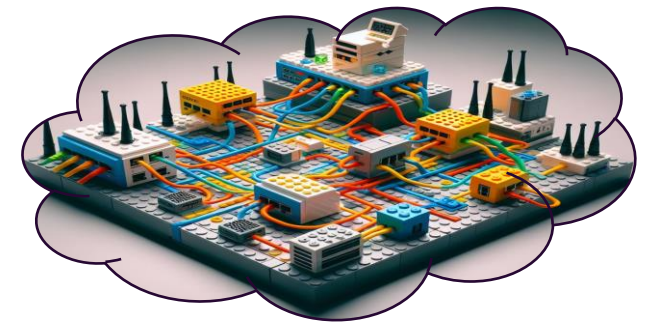
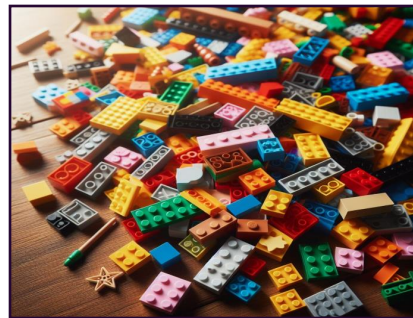
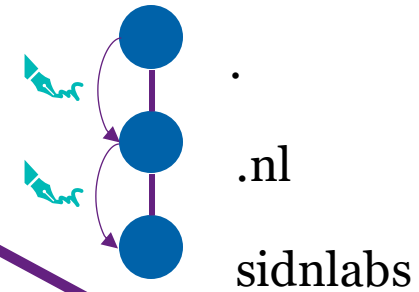
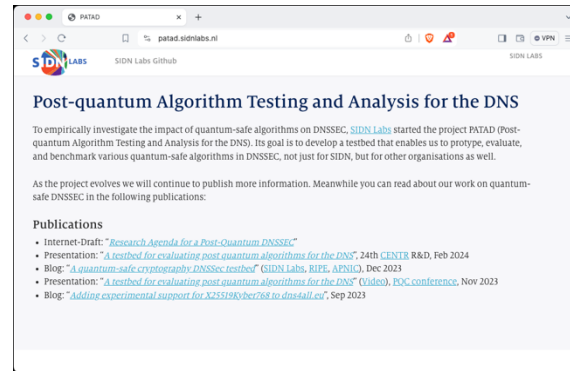
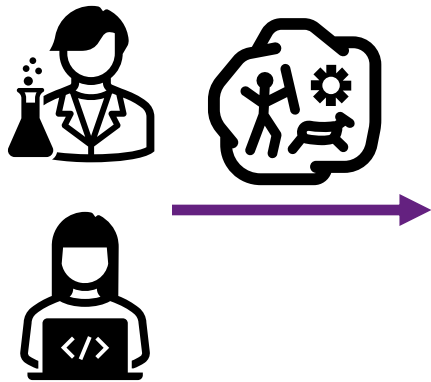


3) The measurements we want to perform

e.g. sign .nl zone



PATAD testbed: building a testbed



PATAD testbed: experiment with MAYO-2

Resolvers



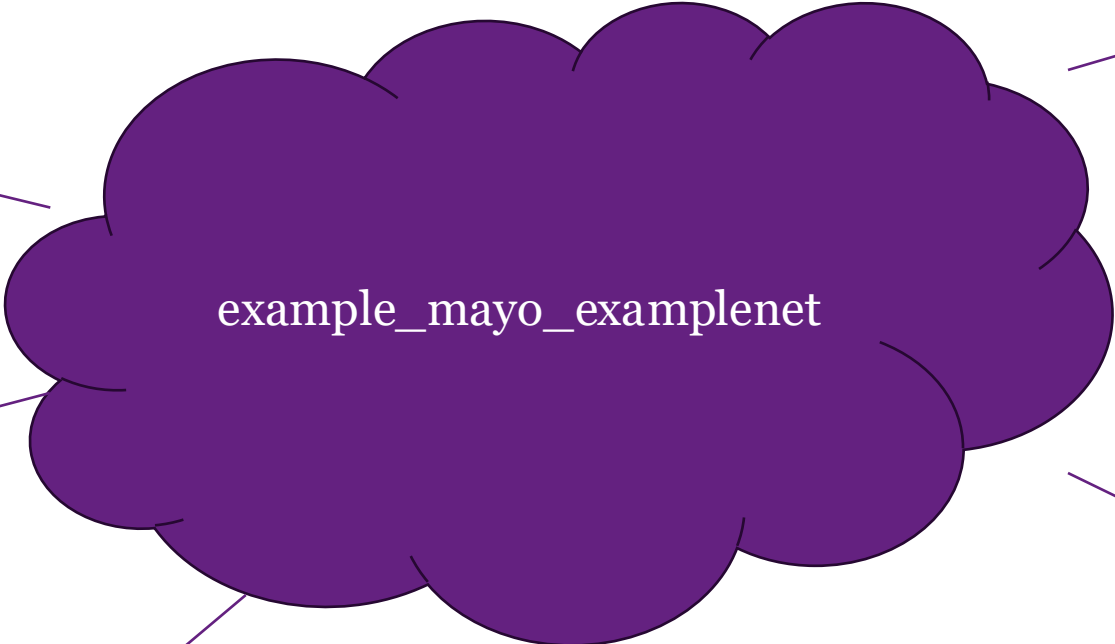
exp1-resolver



exp1-resolver-dnssec



laptop



Authoritative nameservers



exp1-root



exp1-nl



exp1-sidnlabs

Supported PQC algorithms:

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



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:



Research partners:



**UNIVERSITY
OF TWENTE.**



Running PQC testbed yourself



<https://patad.sidnlabs.nl>

<https://github.com/SIDN/pqc-testbed>



Open discussion

We are open for collaboration



Follow us

 SIDN.nl

 @SIDN

 SIDN

Thank you for your time!