Our work on post-quantum DNSSEC

Caspar Schutijser | *Preparing the DNS for the Post-Quantum Cryptography transition* webinar

18 maart 2026

SIDN LABS

Empirically investigating impact of PQC on DNSSEC

DNS' stringent requirements

- Signature size
- Public key size
- Validation speed
- Signing speed

Agenda

1. Past study: Evaluating PQC (Falcon and Mayo) in DNSSEC Signing for TLD Operators

2. Current study: impact of PQ DNSSEC on DNS resolvers

Evaluating PQC (Falcon and Mayo) in DNSSEC Signing for TLD Operators

Caspar Schutijser, Elmer Lastdrager, Ralph Koning, and Cristian Hesselman

24 July 2025

SIDN LABS

Hardware support (AVX2)	Proof of nonexistence
4 algorithms	3 zone files

Algorithm	Public key size	Signature size
RSA-1280	162*	160
ECDSA-P256	64	64
Falcon-512	897	666
MAYO-2 (R1)	5488	180

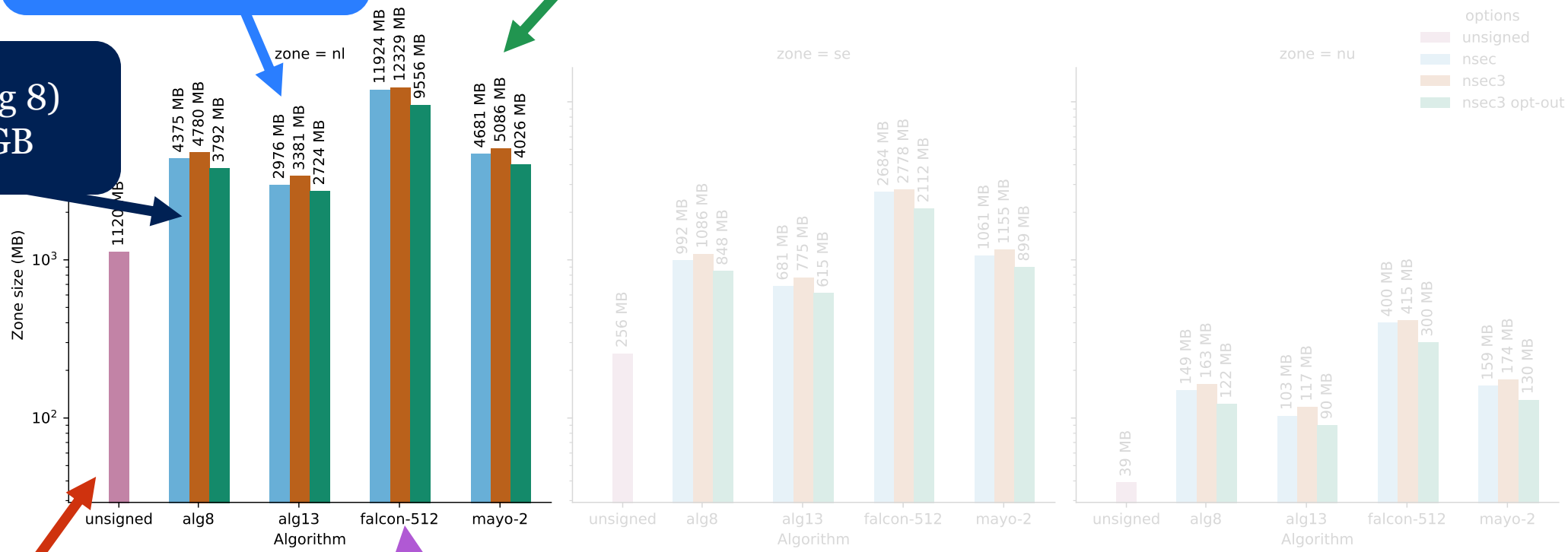
all numbers are in bytes

Zone sizes

ECC (alg 13)
~3 GB

Mayo ~5 GB

RSA (alg 8)
~4.5 GB

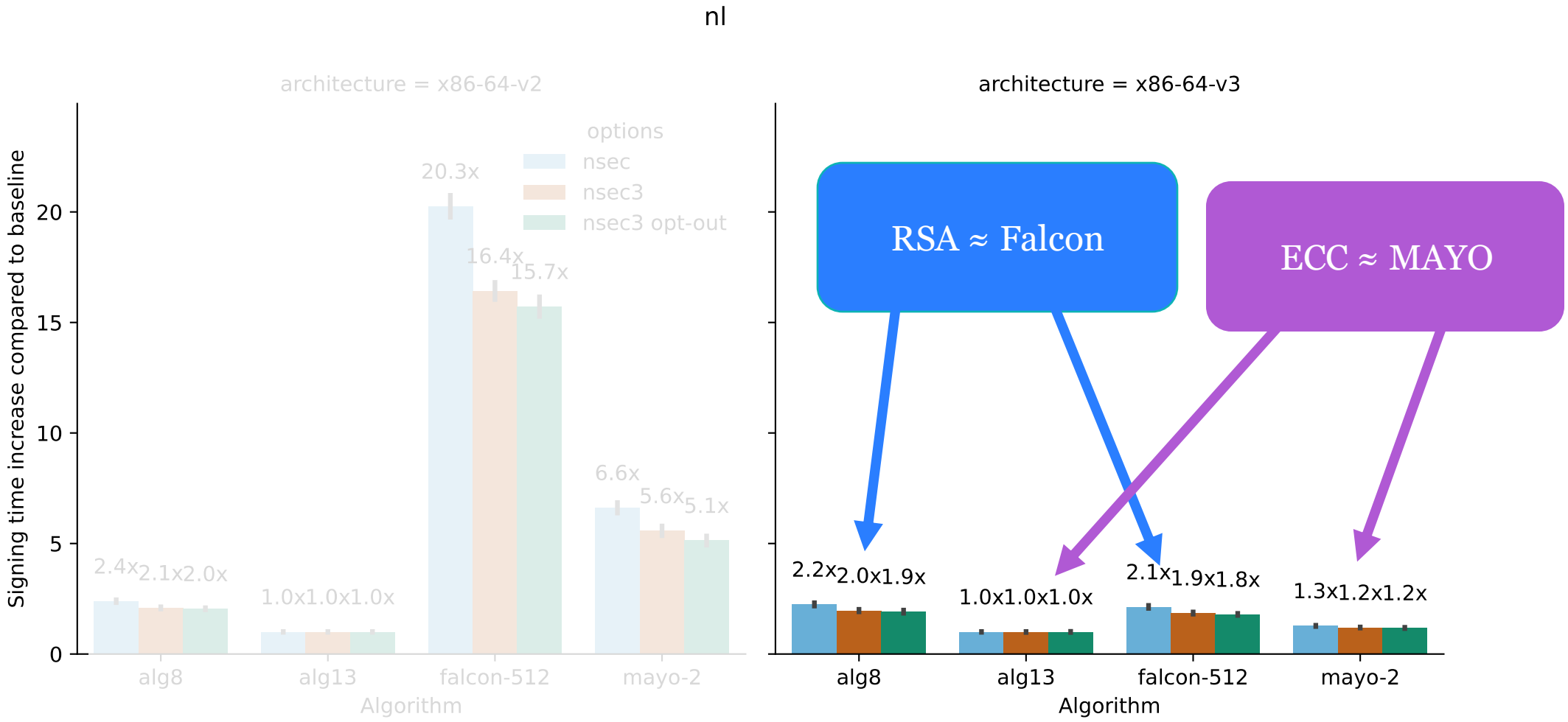


Unsigned ~1 GB

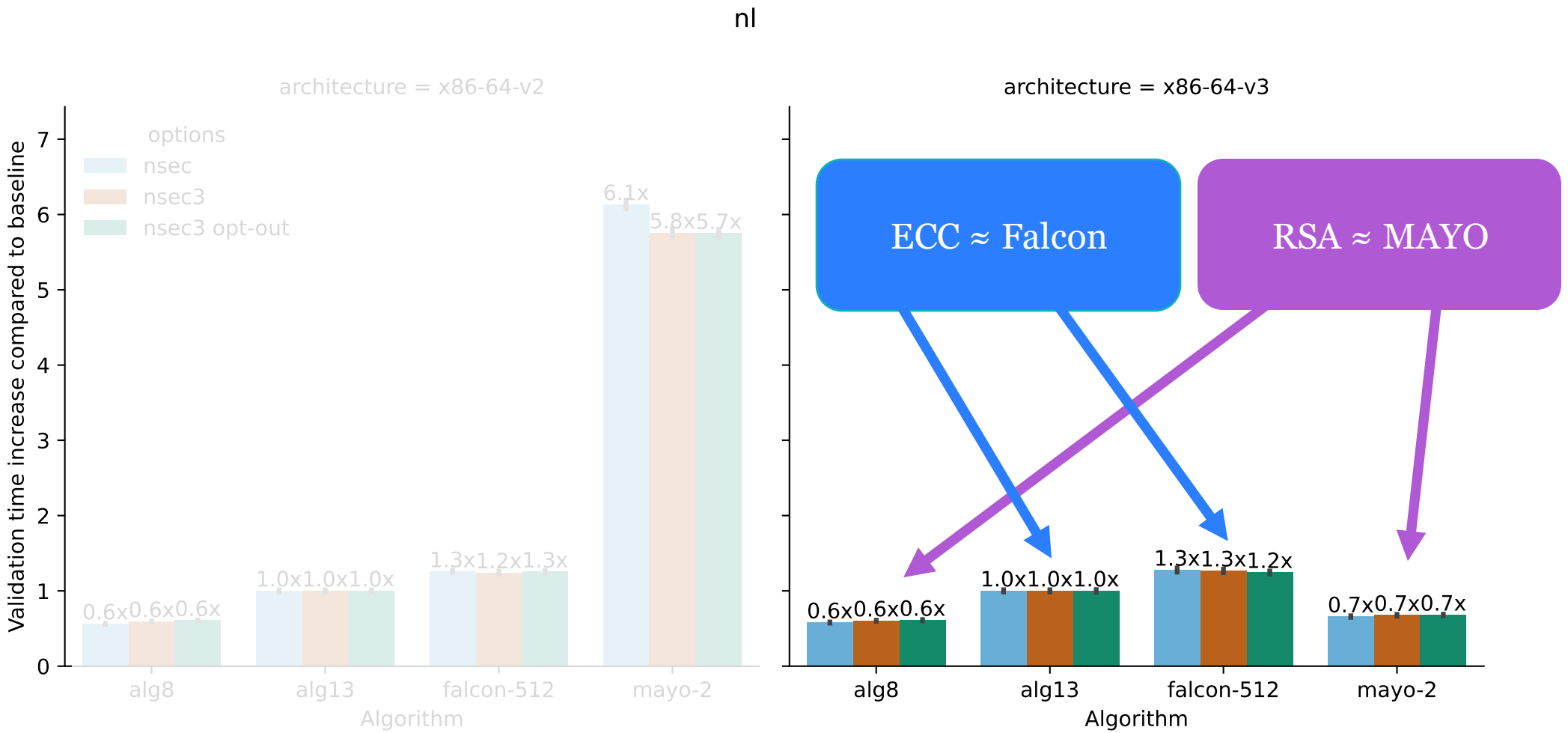
Falcon ~12 GB

SIDN LABS

Signing time of entire .nl zone



Validating the entire .nl zone



Conclusions

Impact on computation time looks comparable to what we have experience with*†‡

Signed zonefiles can become quite a bit bigger, will also affect size of DNS answers

SIDN LABS

Download our paper

"*Evaluating Post-Quantum Cryptography in DNSSEC Signing for Top-Level Domain Operators*" in Network Traffic Measurement and Analysis Conference (TMA2025)

https://tma.ifip.org/2025/wp-content/uploads/sites/14/2025/06/tma2025_paper4.pdf

Agenda

1. Past study: Evaluating PQC (Falcon and Mayo) in DNSSEC Signing for TLD Operators

2. Current study: impact of PQ DNSSEC on DNS resolvers

Impact on DNS resolvers matters

DNS resolvers have to do a lot of work

Resource exhaustion attacks

Bigger DNS answers implies more use of TCP

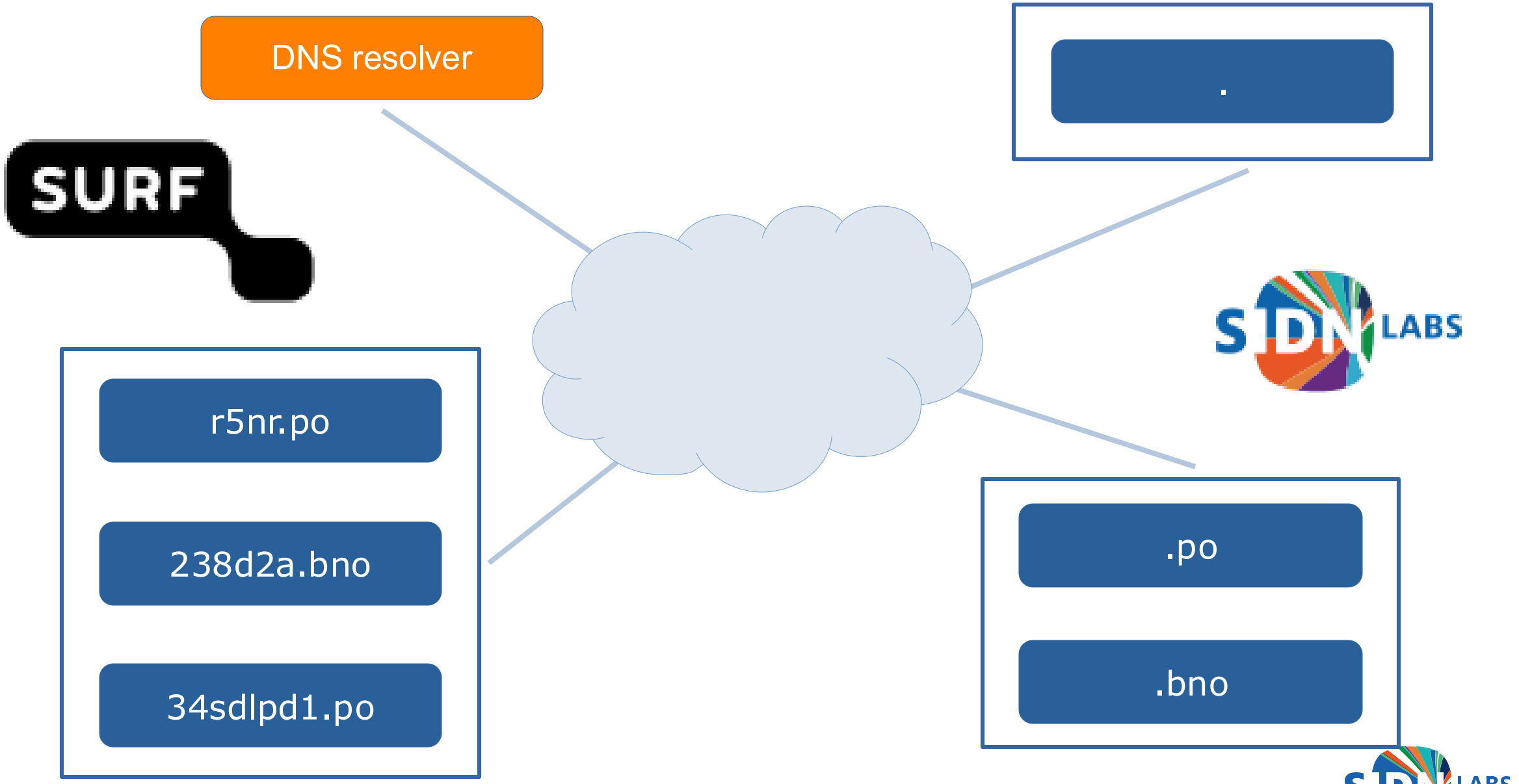
What is the impact of PQC?

UNIVERSITY
OF TWENTE.

Testbed with replica of "DNS world"

- Authoritative name servers (root, TLDs, regular DNS zones)
- Resolver
- Client (to perform resolver measurements with)

Support for PQC algorithms


DNS resolver
SURF
.
r5nr.po
238d2a.bno
34sdlpd1.po
.po
.bno

Replaying realistic traffic

Step 1: collect data from DNS resolver (in anonymized form)

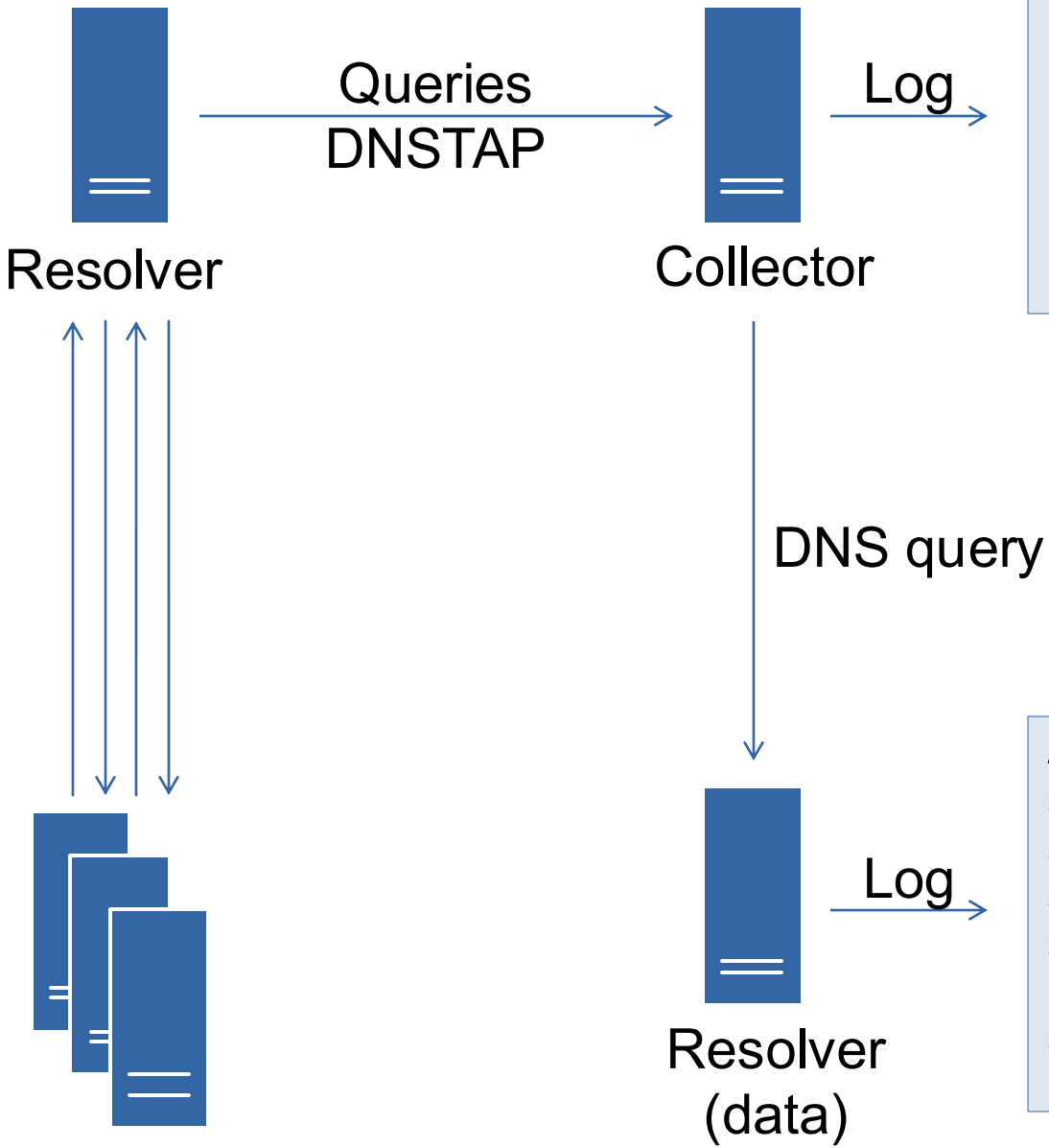
Step 2: rebuild DNS zones based on DNS answers

Step 3: sign zones using PQC algorithms

Step 4: replay queries

Important: data is anonymized

- Exact contents of DNS records are not important
- But format and amounts are

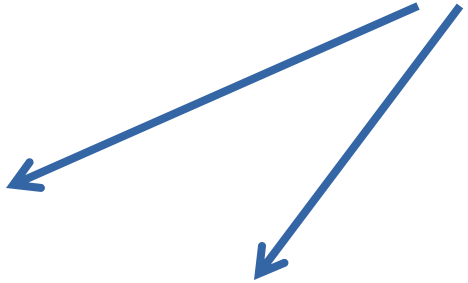


Queries
12:04 surf.nl A UDP
12:07 sidn.nl MX TCP

Answers
surf.nl NS ns1.surfnet.nl.
surf.nl NS ns2.surfnet.nl.
surf.nl A 145.100.190.243
sidn.nl NS ns5.sidn.nl.
ns5.sidn.nl A 145.40.68.55
sidn.nl MX 0 sidn-nl.v-v1.mx.microsoft.

Answers
surf.nl NS ns1.surfnet.nl.
surf.nl NS ns2.surfnet.nl.
surf.nl A 145.100.190.243
sidn.nl NS ns5.sidn.nl.
ns5.sidn.nl A 145.40.68.55
sidn.nl MX 0 sidn-nl.v-v1.mx.microsoft.

Answers
r5nr.po NS mq8.ql9c1h8.po.
r5nr.po NS loq.ql9c1h8.po.
r5nr.po A 48.194.99.216
4itd.po NS ecr.4itd.po.
ecr.4itd.po A 166.246.223.124
4itd.po MX 5 r9p1jlg.8xrl.ym.1qz1utjhe.



$ORIGIN r5nr.po.
r5nr.po. 3600 SOA ...
@ NS mq8.ql9c1h8.po
@ NS loq.ql9c1h8.po
@ A 48.194.99.216

$ORIGIN 4itd.po.
4itd.po. 3600 SOA ...
@ NS ecr.4itd.po.
ecr A 166.246.223.124
@ MX 5 r9p1jlg.8xrl.ym.1qz1utjhe.

Measurements to determine impact

- Various scenarios and algorithms
- Impact on resolver
  - CPU
  - Memory
  - TCP fallbacks
  - Network traffic
  - Latency
  - …

Goal: input for DNS community

Thank you

More information:

caspar.schutijser@sidn.nl

patad.sidnlabs.nl