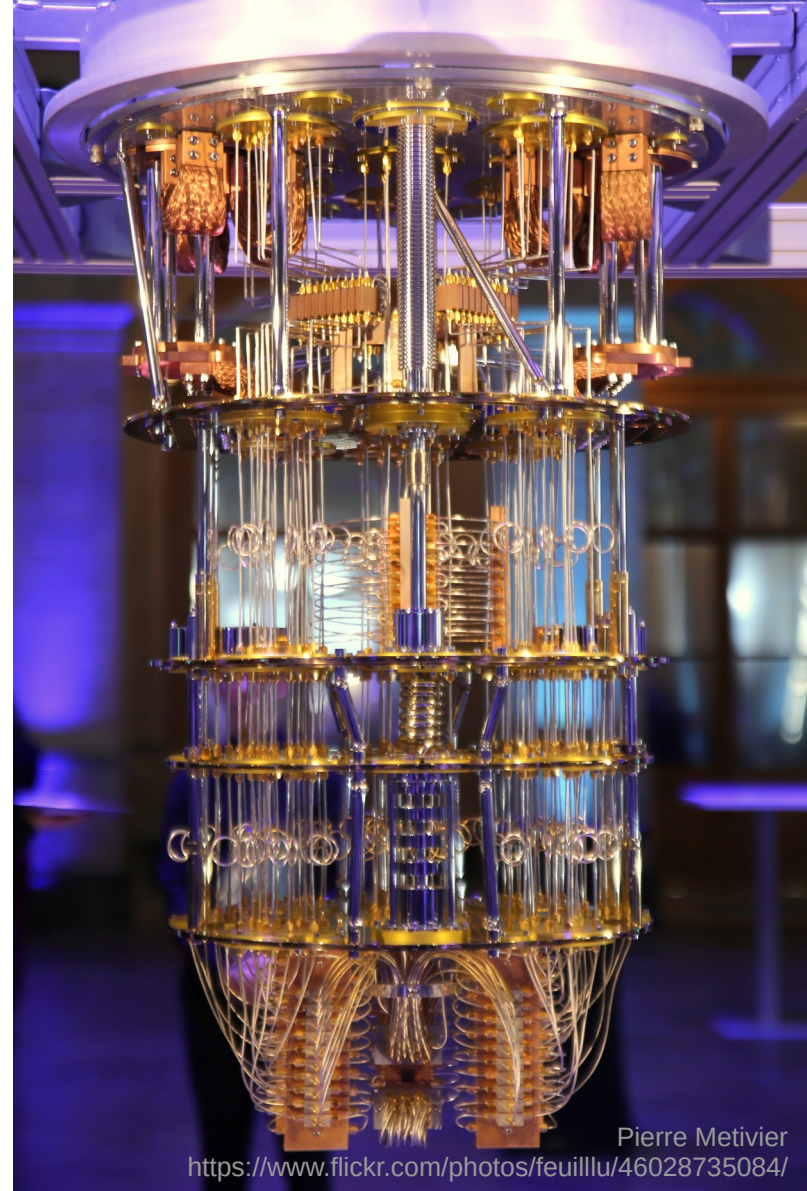


DNSSEC na de quantumapocalyps

Caspar Schutijser (SIDN Labs)
Joeri de Ruiter (SURF)

Quantumapocalyps

- Quantumcomputer kan asymmetrische cryptografie kraken
- Nog niet krachtig genoeg (voor zover we weten)





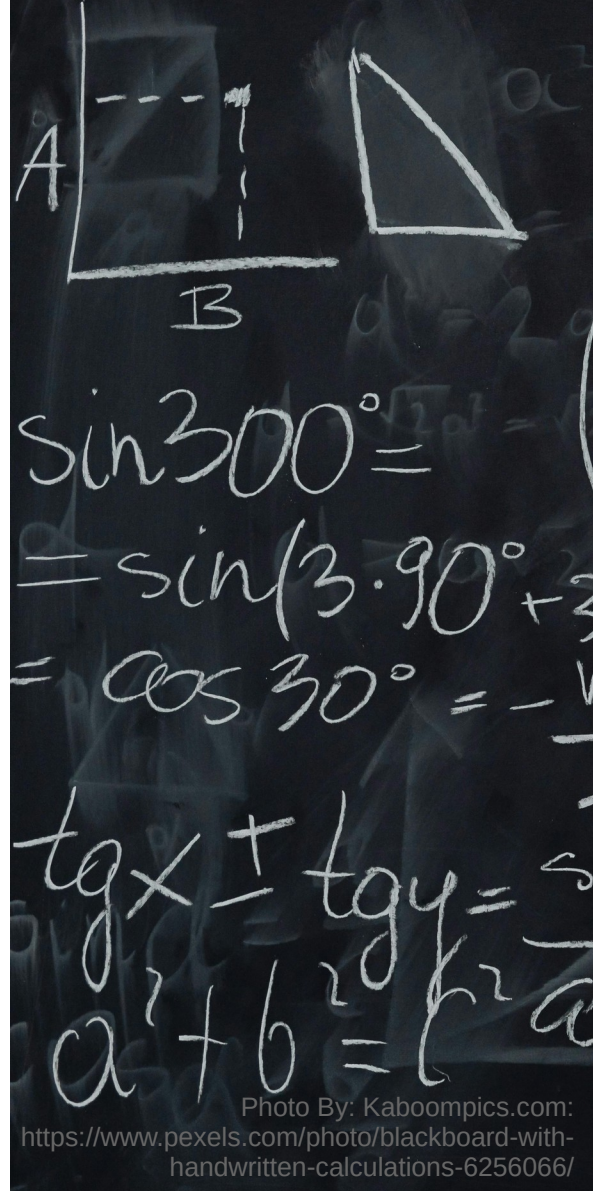
Wanneer is dit een probleem?

Versleuteling: “store now, decrypt later” betekent dat het *nu* al een probleem is

Integriteit: bij het verschijnen van een quantumcomputer die krachtig genoeg is

Postquantum cryptografie

- Nieuwe algoritmes nodig die bestand zijn tegen quantumcomputer
 - Andere wiskundige principes
- Volop in ontwikkeling
- Eerste algoritmes gestandaardiseerd door NIST
- Richtlijnen vanuit BSI



PQC en DNS

- Asymmetrische cryptografie gebruikt voor DNSSEC-handtekeningen
- Geen confidentialiteit binnen DNSSEC
 - Alleen integriteit/authenticiteit
 - Geen last van “store now, decrypt later”
- Wel van trage adoptie
- PQC-TLS al lange tijd onderwerp van onderzoek

Impact op DNS

- Eigenschappen PQC erg anders
- Grotere sleutels en handtekeningen → pakketten groter
 - Fallback van UDP naar TCP
- Berekeningen duren langer
 - Ondertekenen zones op authoritative nameservers
 - Validatie op resolvers

Post-quantum DNSSEC

- Meerdere mogelijkheden
 - Drop-in replacement
 - DNSSEC-protocolwijzigingen
- Wij onderzoeken *drop-in replacement*
 - Eenvoudigere uitrol en adoptie

Query www.sidnlabs.nl

ECC



167 bytes

Falcon-512



760 bytes

Query DNSKEY

ECC



289 bytes

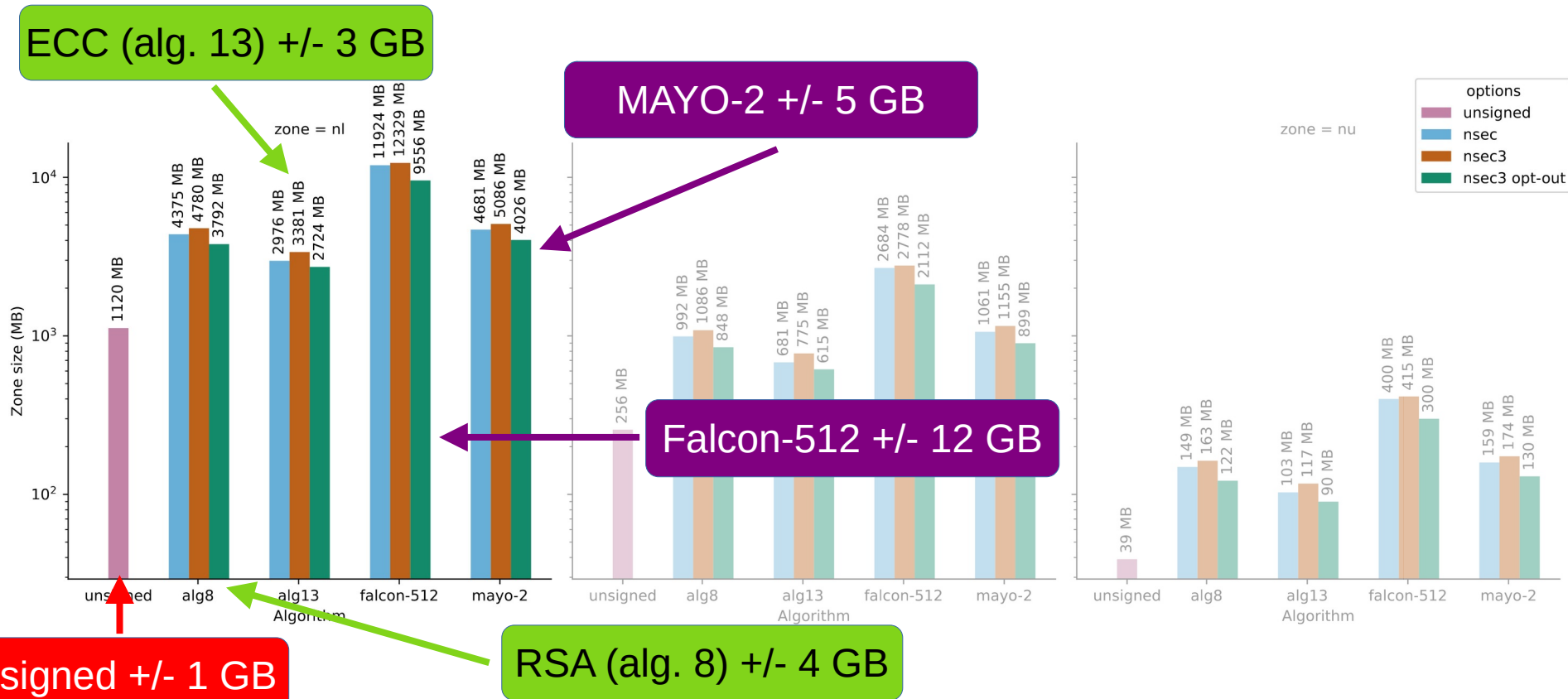
MAYO-2

5749 bytes

Authoritative DNS servers

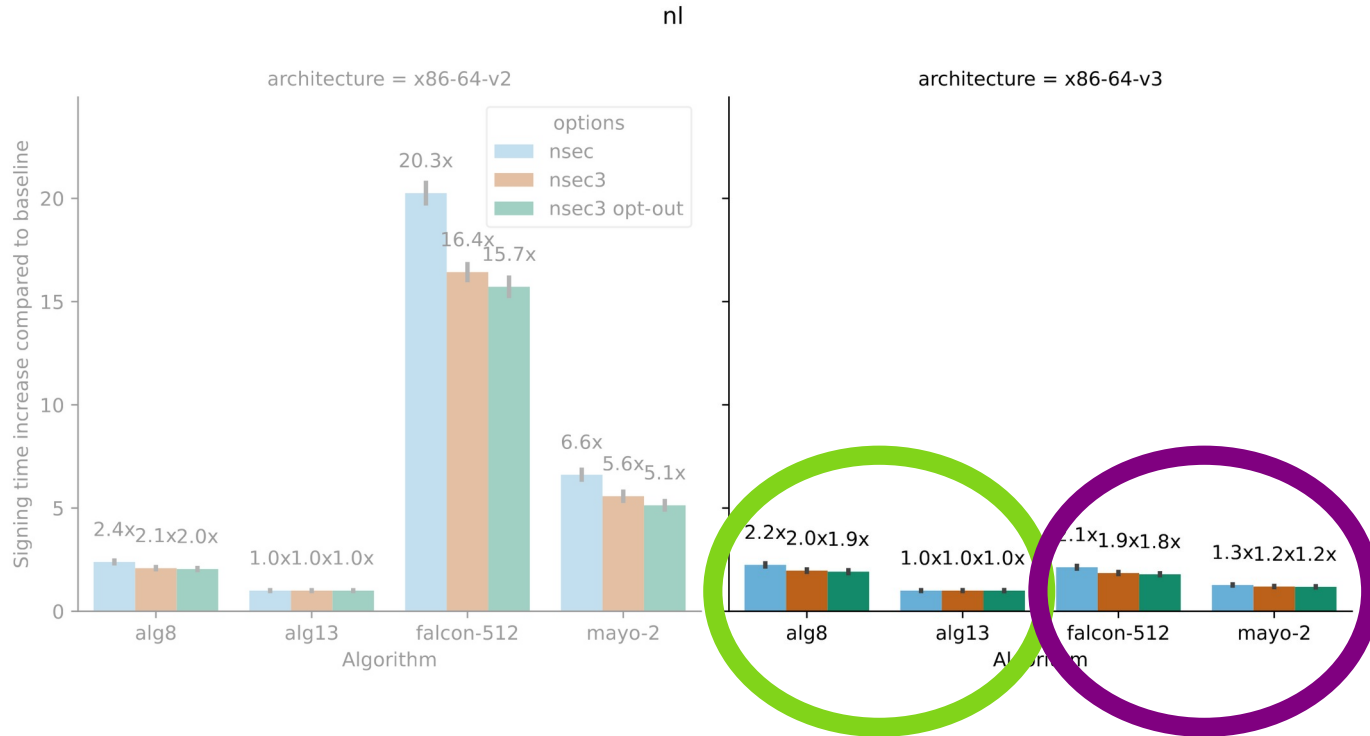
- Onderzoek naar effecten PQC op DNSSEC-signing
 - Voor beheerders van *authoritative DNS servers*
- Gepresenteerd bij *Traffic Measurements and Analysis conference 2025*

Grootte zone files

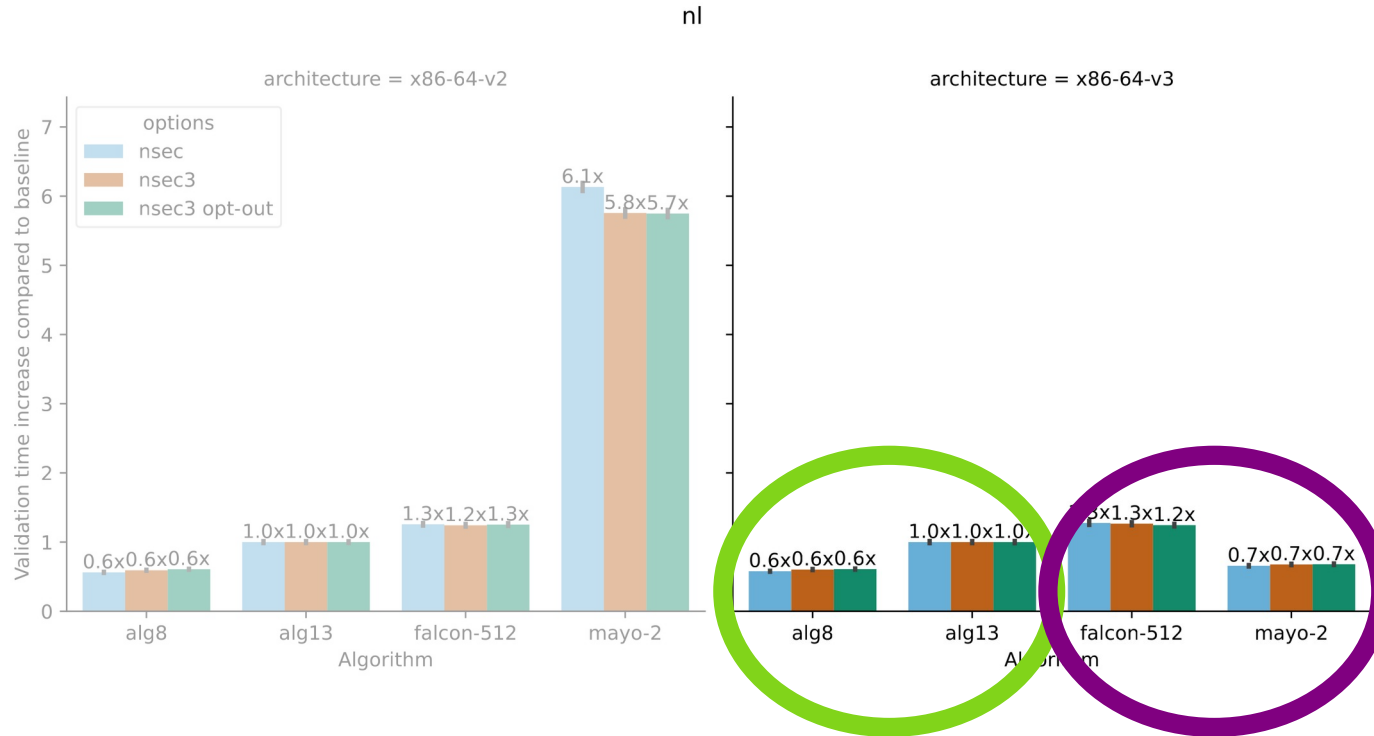


C. Schutijser, R. Koning, E. Lastdrager, C. Hesselman, "Evaluating Post-Quantum Cryptography in DNSSEC Signing for Top-Level Domain Operators", Traffic Measurements and Analysis conference (TMA2025), June 2025

Benodigde tijd ondertekenen



Benodigde tijd validatie



Conclusies onderzoek

- Tijd benodigd voor berekeningen lijkt binnen de perken te blijven met deze algoritmes*[†]
- Ondertekende zonefiles soms wel veel groter
 - Daarom ook de DNS-antwoorden

Wat is het effect op DNS-resolvers?

Gezamenlijk onderzoek

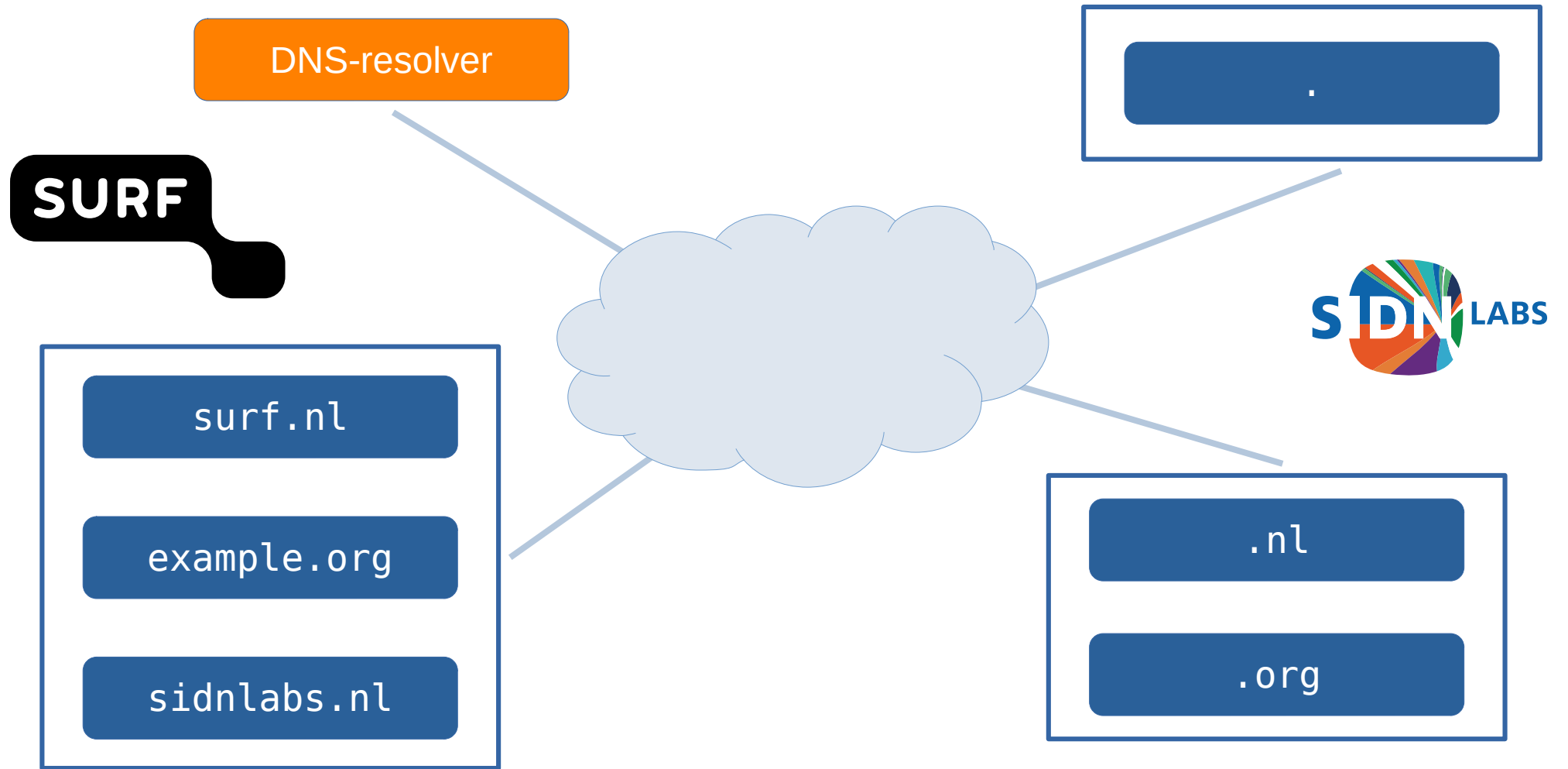
- Impact van gebruik PQC op resolvers in realistische scenario's
- Input vanuit onze eigen rollen
 - SIDN als TLD-beheerder
 - SURF als beheerder van resolvers en authoritative nameservers



Testbed

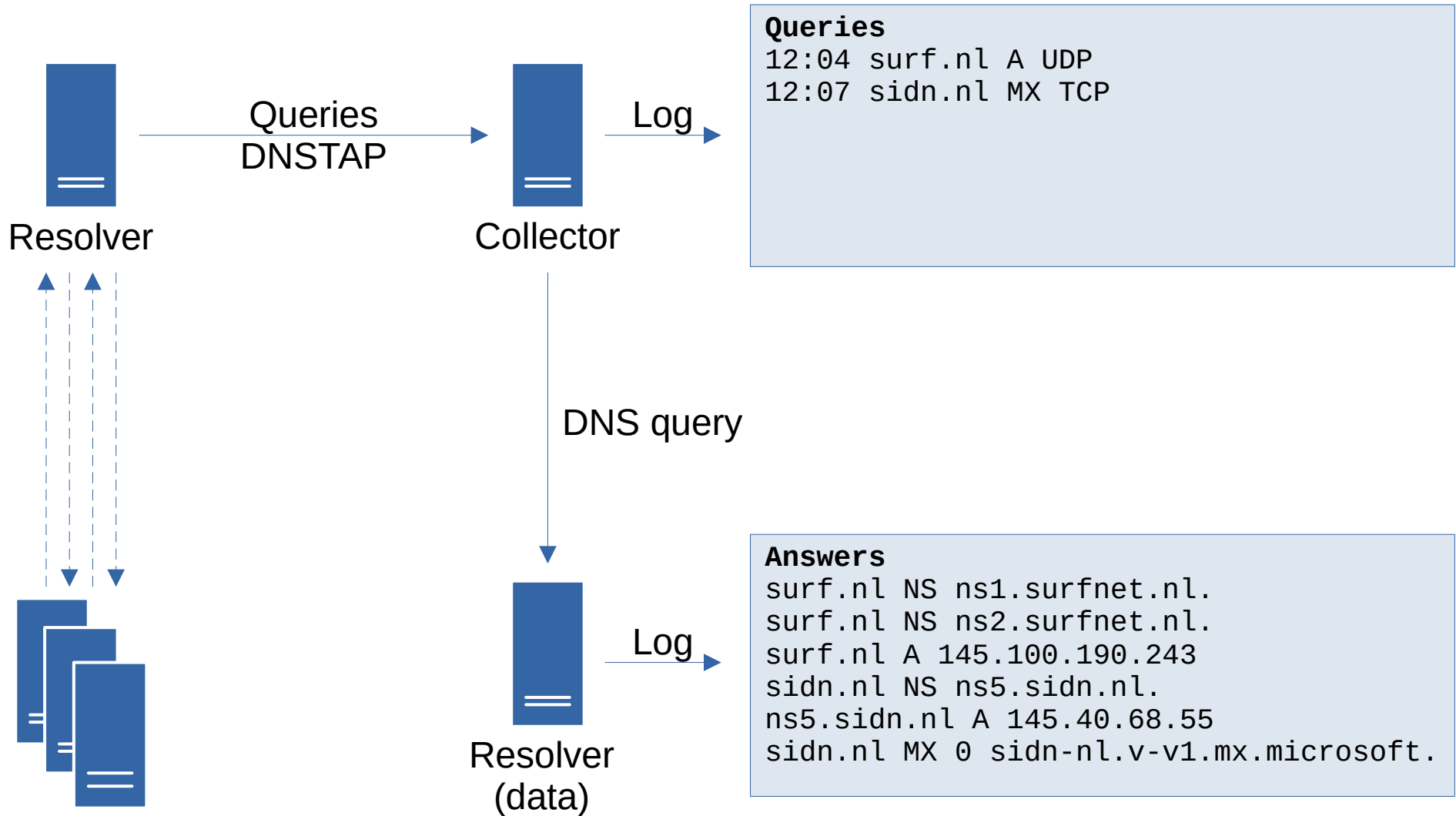
- “Replica van de wereld”
 - Root (.)
 - Top-level domeinen (e.g. .nl)
 - Reguliere DNS-zones (e.g. surf.nl)
- PQC-ondersteuning
 - DNSSEC-signers
 - Resolvers





Realistische scenario's

- Herhalen “echt” verkeer
- Stap 1: queries en antwoorden verzamelen van resolvers
 - Met behulp van DNSTAP
 - Geen informatie clients
- Stap 2: zones herbouwen op basis van antwoorden
 - DNSSEC met PQC
- Stap 3: replay queries
- Data geanonimiseerd
 - Inhoud niet belangrijk
 - Vorm en hoeveelheid wel



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.
```

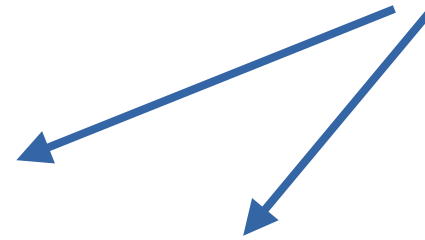


Answers

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

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

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



Metingen

- Verschillende scenario's/algoritmes
- Impact op resolver
 - CPU
 - Memory
 - TCP fallbacks
 - Netwerkverkeer
- Werkt het ongeveer met de huidige server?
- Moeten we de capaciteit verdubbelen?
- Gaat het helemaal niet werken?



Hoe verder?

- Infrastructuur opgezet
- Eerste dataset verzameld
- Volgende stap: meting realistische scenario's

Caspar Schutijser (caspar.schutijser@sidn.nl)
Joeri de Ruiter (joeri.deruiter@surf.nl)

