Evaluating Post-Quantum Cryptography for the Domain Name System

SURF Networking dag 2024

02 Dec 2024

SIDN LABS

Requirements for quantum-safe algoritms

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	—

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

Theory: packet size

	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
🙂	SQIsign	I	1	64	177	241
	VOX	128	1	9,104	102	9,206

Post-quantum signatures zoo: https://pqshield.github.io/nist-sigs-zoo

Theory: signing and verification speed

	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
☹️	SQIsign	I	1	5,669,000,000	108,000,000
	VOX	128	1	664,265	168,567

Post-quantum signatures zoo: https://pqshield.github.io/nist-sigs-zoo

PATAD Testbed

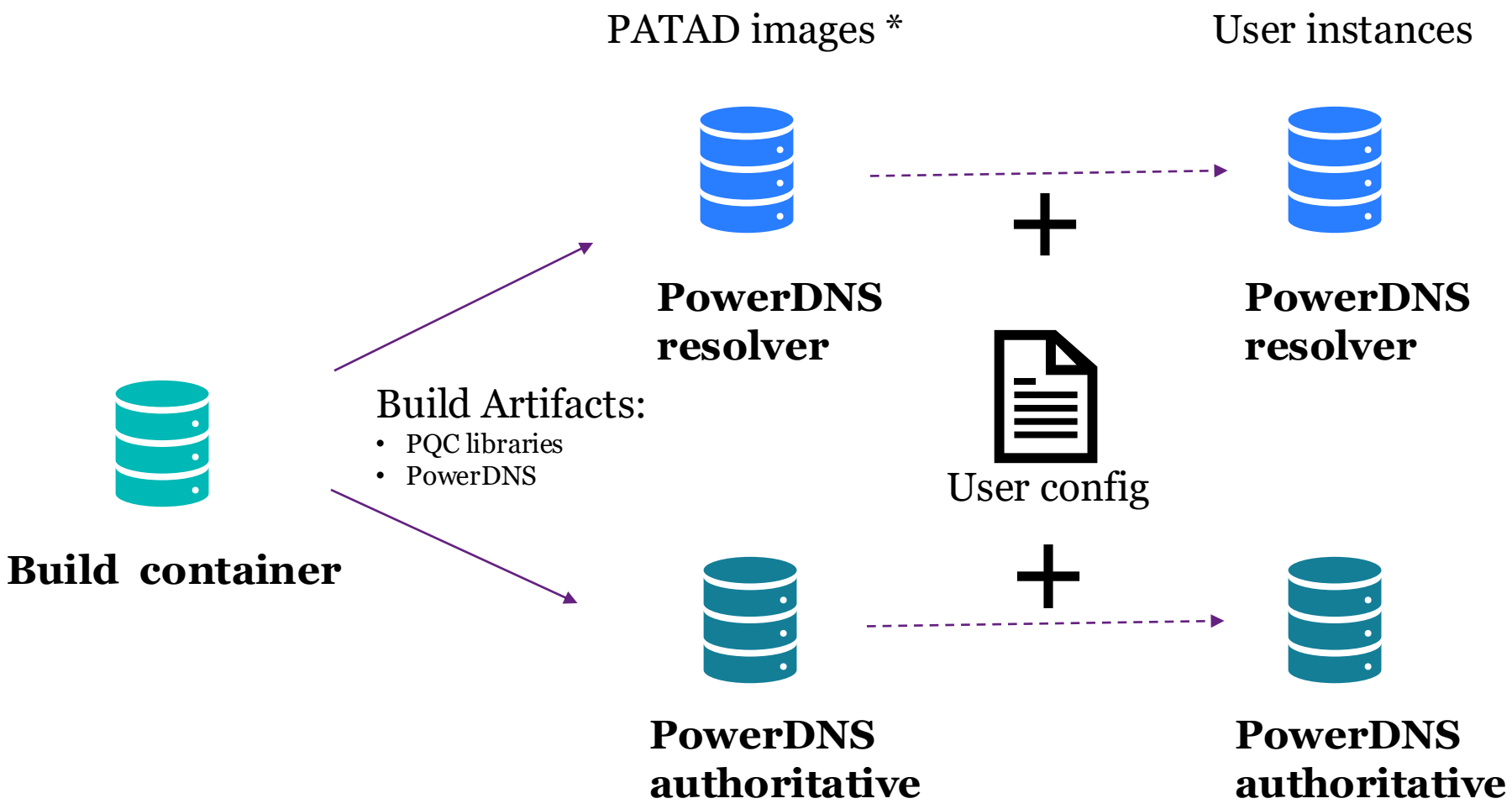
PATAD testbed is available

- Prebuilt docker images plus testbed using docker–compose
  - Specify your own topology.
  - Run your own experiments.

- Supported software:
  - PowerDNS
    - SQIsign-I
    - MAYO-2
    - Falcon-512

SIDN LABS

Container hierarchy



* PATAD images are provided for amd64 and arm64 architectures

Configuring the testbed

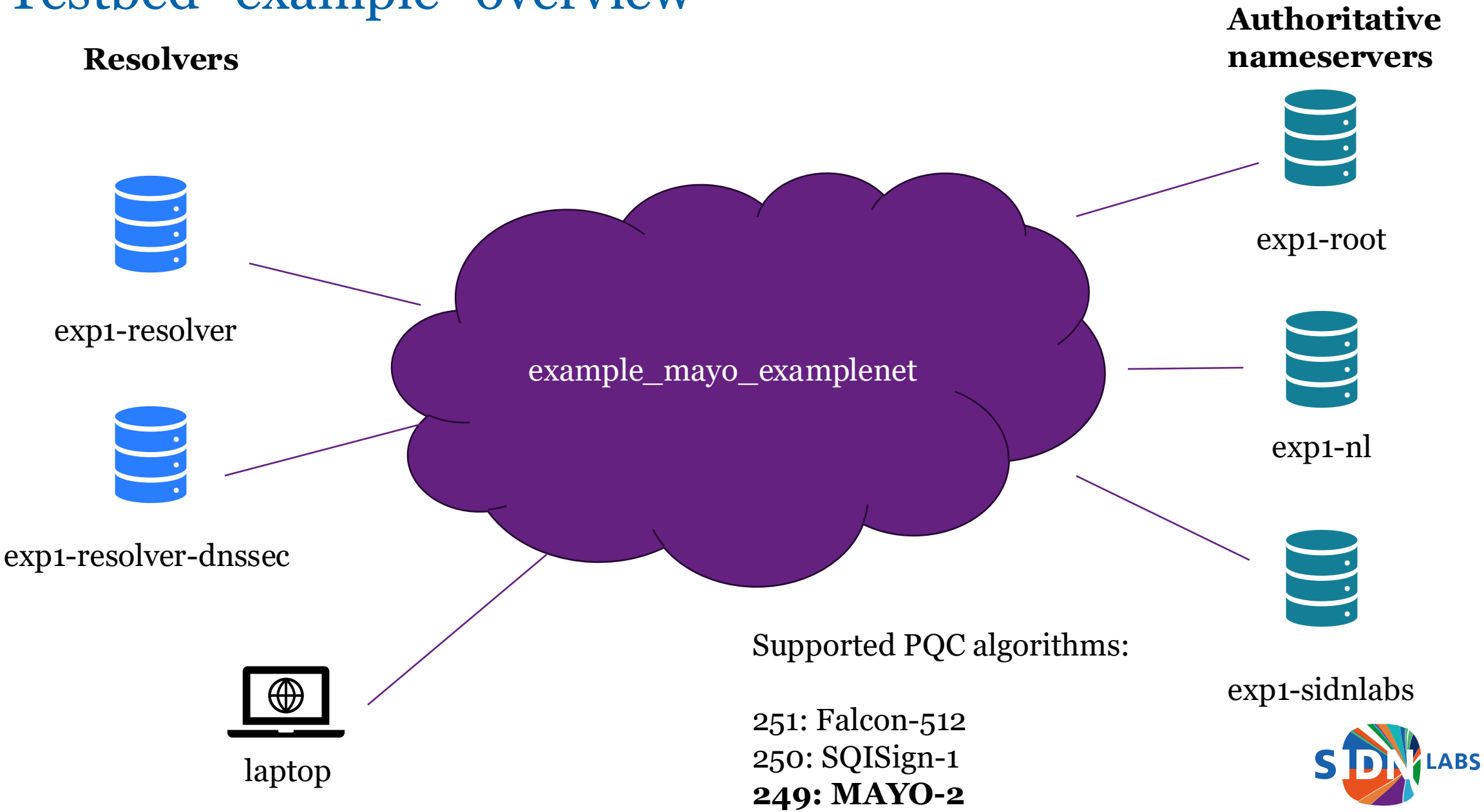
main pqc-testbed / example /

ElmerLastdrager Initial commit

Name	Last commit message
..	
README.md	Initial commit
docker-compose.yml	Initial commit
generate-testbed.sh	Initial commit
named-nl.conf	Initial commit
named-root.conf	Initial commit
named-sidnlabs.conf	Initial commit
pdns.conf	Initial commit
recursor-dnssec.conf	Initial commit

SIDN LABS

Testbed “example” overview



Starting the testbed

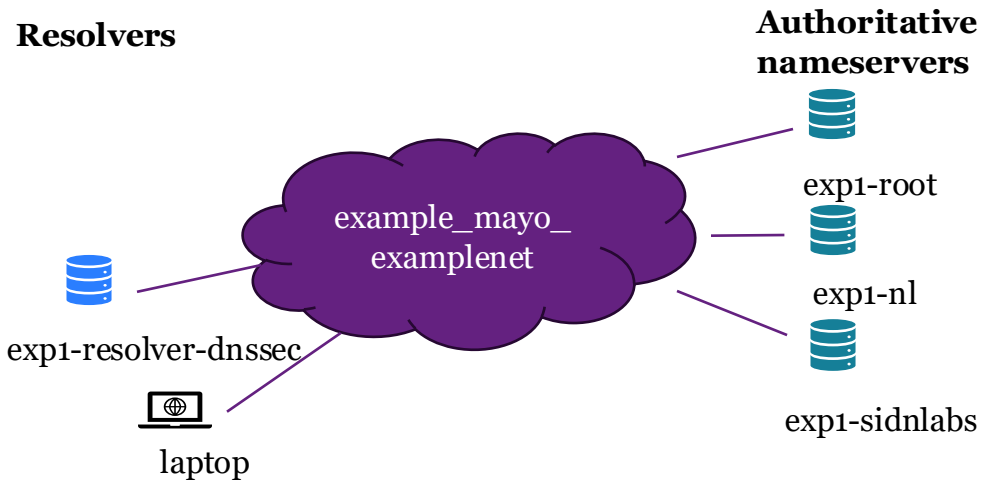
```
patad$ ./generate-testbed
setting up dnssec on root server
Jul 31 12:26:17 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
pub: [omitted] 1
Added a KSK with algorithm = 250, active=0
Jul 31 12:26:19 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
pub: [omitted] 2
Added a ZSK with algorithm = 250, active=0
exporting trust anchor
setting up trust between root and nl
Jul 31 12:26:21 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
pub: [omitted] 1
Added a ZSK with algorithm = 249, active=1
Jul 31 12:26:21 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
nl. IN DS 16434 249 2 [omitted] ; ( SHA256 digest )
nl. IN DS 16434 249 4 [omitted] ; ( SHA-384 digest )
.:         parsed into memory at 2024-07-31 12:26:21 +0000
setting up trust between nl and sidnlabs
Jul 31 12:26:21 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
pub: [omitted] 1
Added a ZSK with algorithm = 251, active=1
Jul 31 12:26:22 [bindbackend] Done parsing domains, 0 rejected, 1 new, 0 removed
sidnlabs.nl. IN DS 11468 251 2 [omitted] ; ( SHA256 digest )
sidnlabs.nl. IN DS 11468 251 4 [omitted] ; ( SHA-384 digest )
nl:        parsed into memory at 2024-07-31 12:26:22 +0000
Forcing root to sign all records
 ... waiting for nameserver
Finished signing root
Forcing sidnlabs.nl to sign all records
Finished signing sidnlabs.nl
```

AXFR to force sign the zone

Verifying the testbed

```
patad$ podman ps --format="{{.Names}} {{.State}} \t {{.Ports}}"

v2_database_1 running
v2_apiserver_1 running                    127.0.0.1:8000->80/tcp
example_exp1-root_1 running               0.0.0.0:5302->53/tcp, 0.0.0.0:5302->53/udp
example_exp1-nl_1 running                 0.0.0.0:5303->53/tcp, 0.0.0.0:5303->53/udp
example_exp1-sidnlabs_1 running           0.0.0.0:5304->53/tcp, 0.0.0.0:5304->53/udp
example_exp1-resolver-dnssec_1 running 0.0.0.0:5311->53/tcp, 0.0.0.0:5311->53/udp
```



Querying the root authoritative

```
patad$ dig . NS -p 5302 @::1

; <<>> DiG 9.18.27 <<>> . NS -p 5302 @::1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60209
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232

;; QUESTION SECTION:
;.                              IN NS

;; ANSWER SECTION:
.                              3600 IN    NS s.root-servers.net.
.                              3600 IN    RRSIG NS 250 0 3600 (
                                          20240808000000 20240718000000 15317 .
                                          [omitted] )

;; ADDITIONAL SECTION:
s.root-servers.net.   3600 IN    AAAA fc01::2
s.root-servers.net.   3600 IN    RRSIG AAAA 250 3 3600 (
                                          20240808000000 20240718000000 15317 .
                                          [omitted] )

;; Query time: 3 msec
;; SERVER: ::1#5302(::1) (UDP)
;; WHEN: Wed Jul 31 14:27:08 CEST 2024
;; MSG SIZE  rcvd: 726
```

AA bit set

250 = SQISign-I

Querying the resolver

```
patad$ dig sidnlabs.nl txt -p 5311 @::1

; <<>> DiG 9.18.27 <<>> sidnlabs.nl txt -p 5311 @::1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31760
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512

;; QUESTION SECTION:
;sidnlabs.nl.                   IN TXT

;; ANSWER SECTION:
sidnlabs.nl.                    3600 IN    TXT "This is the sidnlabs.nl zone"
sidnlabs.nl.                    3600 IN    RRSIG TXT 251 2 3600 (
                                           20240808000000 20240718000000 11468 sidnlabs.nl.
                                           [omitted] )

;; Query time: 57 msec
;; SERVER: ::1#5311(::1) (UDP)
;; WHEN: Wed Jul 31 14:27:19 CEST 2024
;; MSG SIZE  rcvd: 783

patad$
```

AD bit set

251 = Mayo-2

Running PQC testbed yourself

https://patad.sidnlabs.nl

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

PowerDNS with PQC patches:

https://github.com/SIDN/pdns/tree/master-pqc-20240606

Measurements

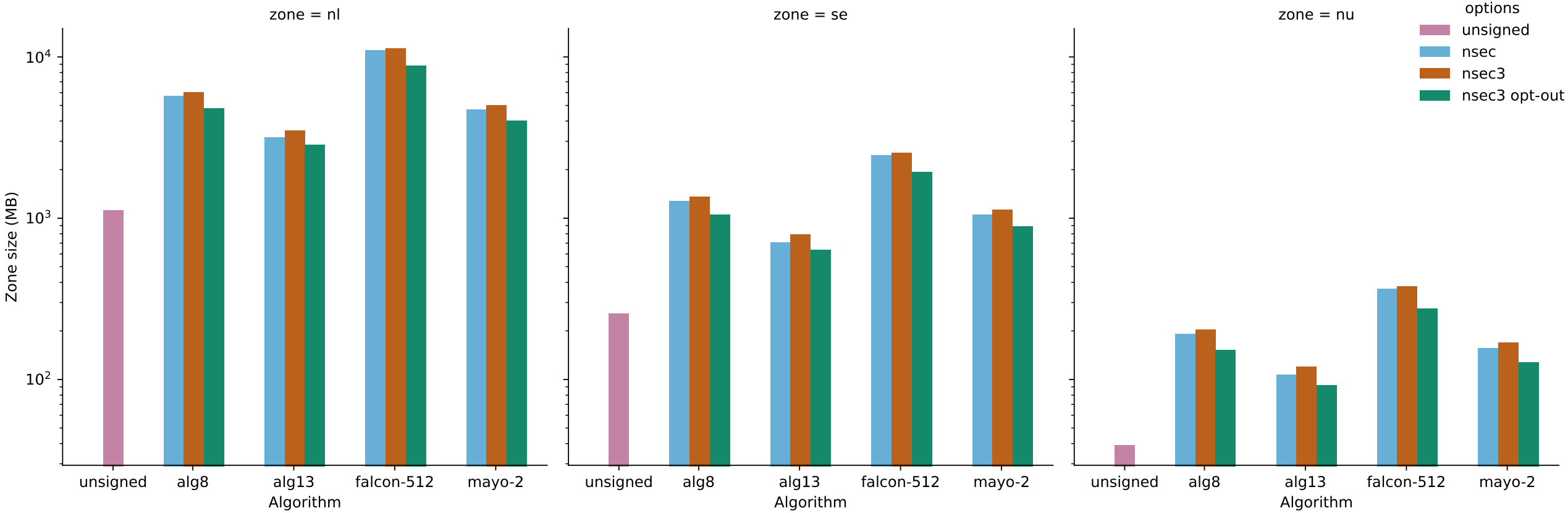
Requirements for quantum-safe algoritms

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	—

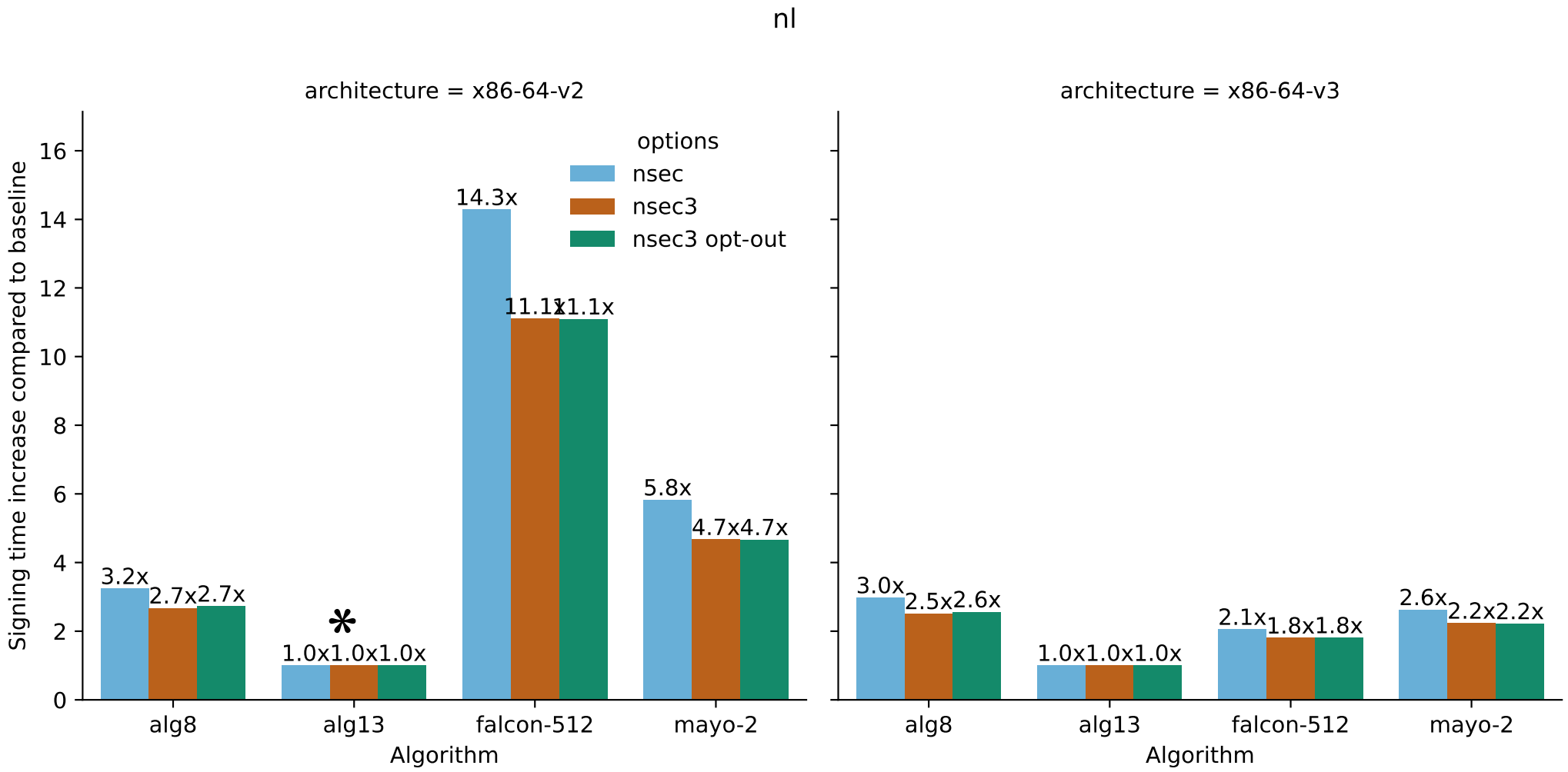
M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

SIDN LABS

Zonefile sizes and increase

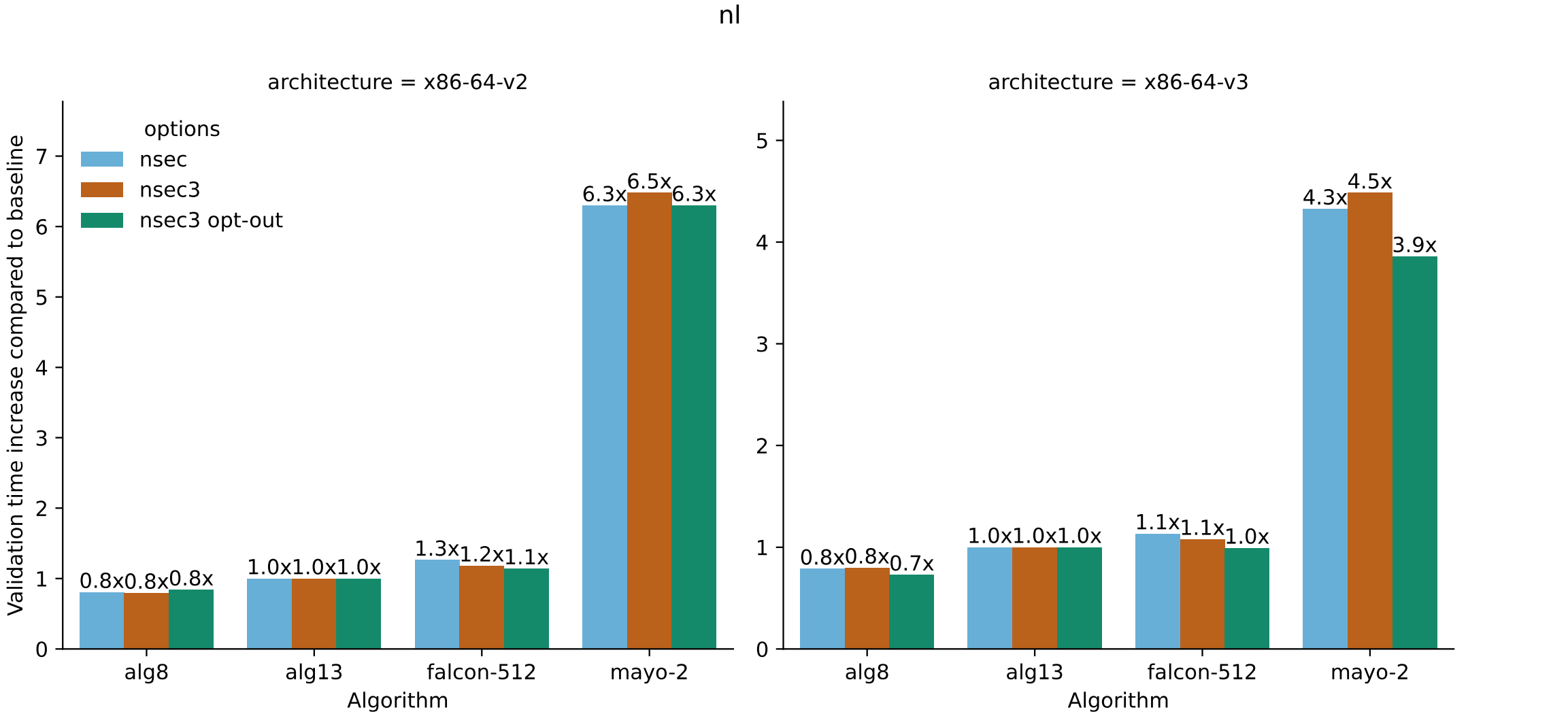


Zone signing times of .nl relative to algorithm 13



- 1.0x approx 1,5 hours of signing using dnspython

Validation time of .nl (full zone) relative to algorithm 13



Conclusions

Falcon-512

- ✅ Larger zone size
- ✅ Zone signing times below alg8
- ✅ Validation time comparable to alg13
- ⚠️ Large signature 10x larger than alg13 (but below threshold)

Mayo-2

- ✅ Smaller zone size
- ✅ Zone Signing times below alg8, slightly higher than falcon512
- ⚠️ Validation takes much (4x) longer than alg13 (and alg8)
- ✅ Signature size comparable to alg13

SIDN LABS

Demo

PATAD testbed demo / query explorer

www.example.nl | PQC | Analyze | Reset

Back | Next

Contacting resolver

The client contacted the selected resolver: `[fc01::100]`

The question that was asked: what is the IP address of `www.example.nl`?

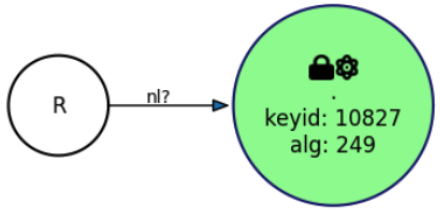
Connection to resolver is secured with PQC using DoH with ML-KEM/Kyber.

After this, the resolver will start searching for the answer.

PATAD testbed demo / query explorer

DEMO: post-quantum algorithms in DNSSEC

www.example.nl | PQC | Analyze | Reset



Back | Next

The root (.) lists all top-level-domains (TLDs) and is the starting point of DNS. In DNSSEC, the root is the trust anchor for validating the chain of trust. The servers are run by many organisations.

DNS query 1

Nameserver for query	.
Query sent	nl.
Transport layer	UDP
DNSSEC	signed
Packet size	287 bytes

DNSSEC: obtain pubkey

Type	DNSKEY
zsk	10827 MAYO-2 (249)
ksk	19828 MAYO-2 (249)
Transport layer	UDP
DNSSEC	signed
Packet size	11260 bytes

DNSSEC: delegation

Type	DS
Key type	35292 MAYO-2 (249)
Key type	35292 MAYO-2 (249)
Transport layer	UDP
DNSSEC	signed
Packet size	370 bytes

Next steps for us.

Work together with SURF and UT to further Measure impact on DNSSEC signing and resolvers: validation timings, response times, packet sizes

Implement and Investigate other Round 2 candidate algorithms:

- SQIsign variant SQIsign2D-West
- SNOVA (24, 5, 4), UOV (Ip-pkc)

Look into other solutions for DNSSEC to support PQC such as merkle-trees and MTL-mode

SIDN LABS

Questions?