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

Elmer Lastdrager, in collaboration with Caspar Schutijser, Ralph Koning, and Cristian Hesselman

24 July 2025

Hardware support (AVX2)

Proof of nonexistence

4 algorithms

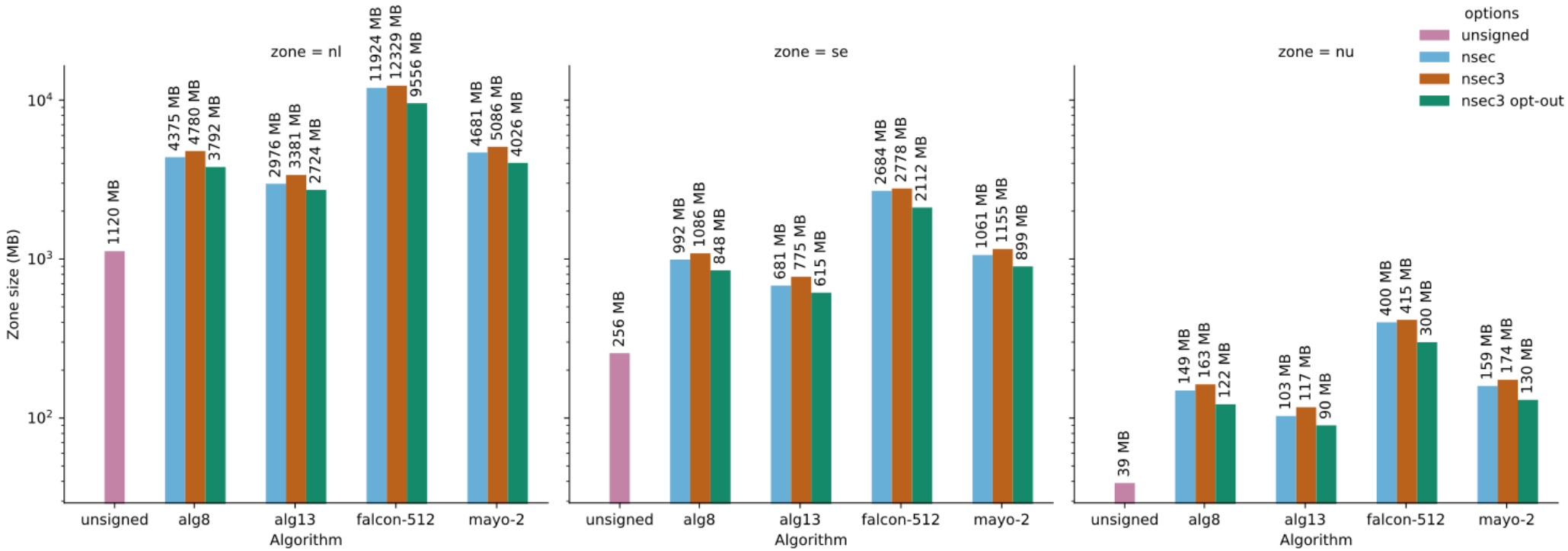
3 zone files

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

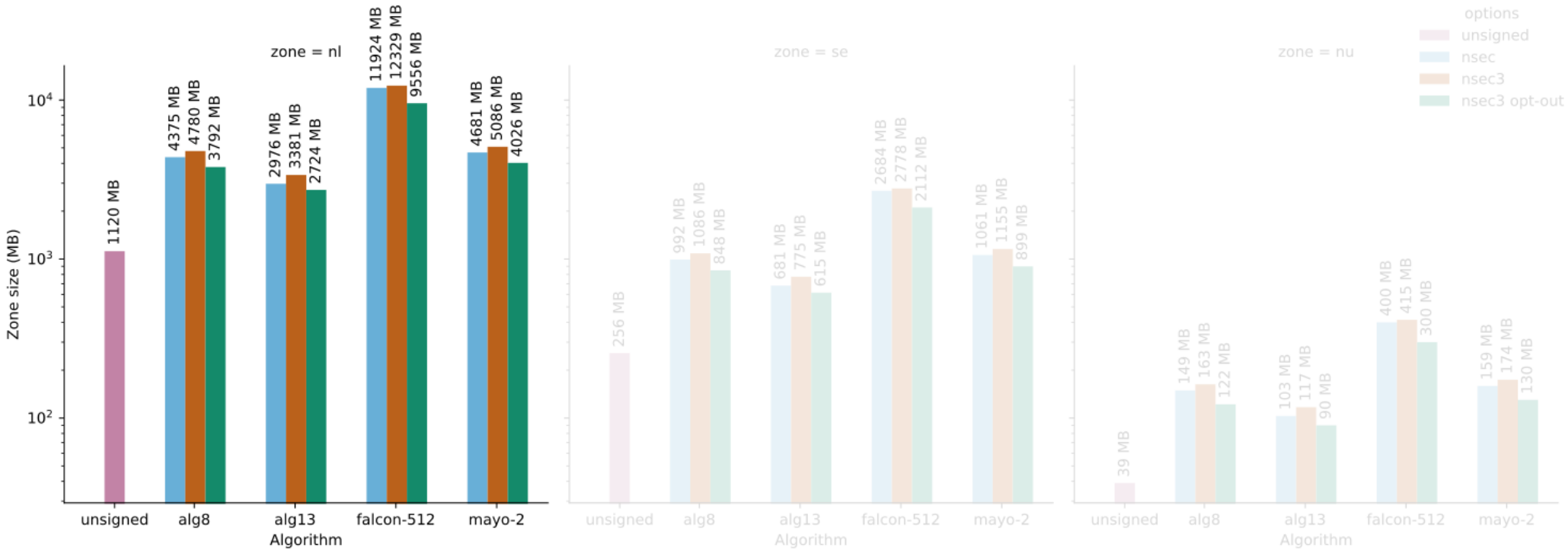
all numbers are in bytes

SIDN LABS

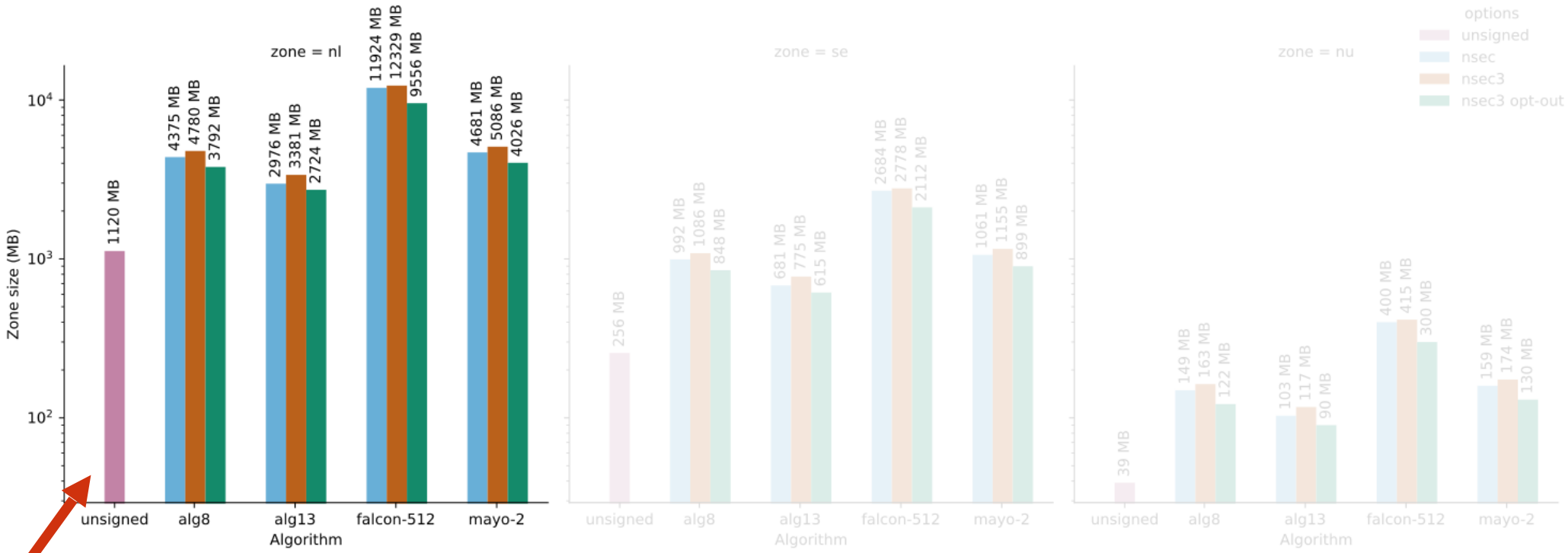
Zone sizes


zone = nl
zone = se
zone = nu
options
unsigned
nsec
nsec3
nsec3 opt-out
Zone size (MB)
10^4
10^3
10^2
1120 MB
4375 MB
4780 MB
3792 MB
2976 MB
3381 MB
2724 MB
11924 MB
12329 MB
9556 MB
4681 MB
5086 MB
4026 MB
256 MB
992 MB
1086 MB
848 MB
681 MB
775 MB
615 MB
2684 MB
2778 MB
2112 MB
1061 MB
1155 MB
899 MB
39 MB
149 MB
163 MB
122 MB
103 MB
117 MB
90 MB
400 MB
415 MB
300 MB
159 MB
174 MB
130 MB
unsigned
alg8
alg13
falcon-512
mayo-2
Algorithm

Zone sizes


zone = nl
zone = se
zone = nu
options
unsigned
nsec
nsec3
nsec3 opt-out
Zone size (MB)
10^4
10^3
10^2
1120 MB
4375 MB
4780 MB
3792 MB
2976 MB
3381 MB
2724 MB
11924 MB
12329 MB
9556 MB
4681 MB
5086 MB
4026 MB
256 MB
992 MB
1086 MB
848 MB
681 MB
775 MB
615 MB
2684 MB
2778 MB
2112 MB
1061 MB
1155 MB
899 MB
39 MB
149 MB
163 MB
122 MB
103 MB
117 MB
90 MB
400 MB
415 MB
300 MB
159 MB
174 MB
130 MB
unsigned
alg8
alg13
falcon-512
mayo-2
Algorithm

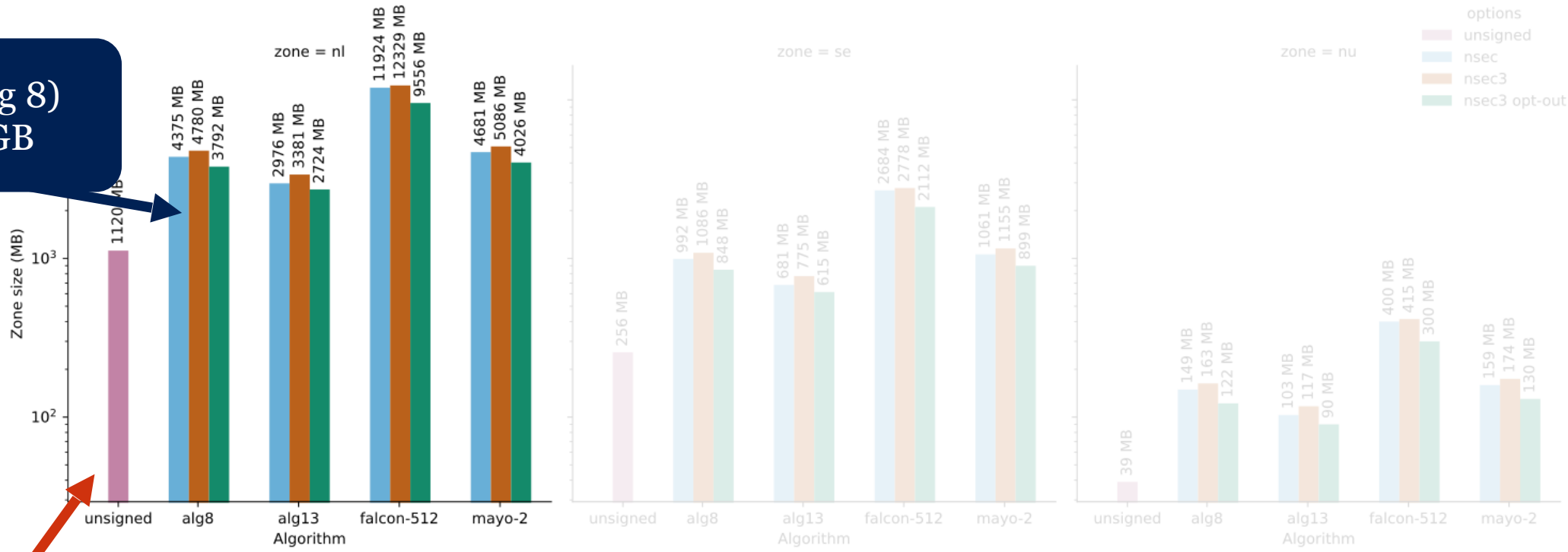
Zone sizes



Unsigned ~1 GB

Zone sizes

RSA (alg 8)
~4.5 GB



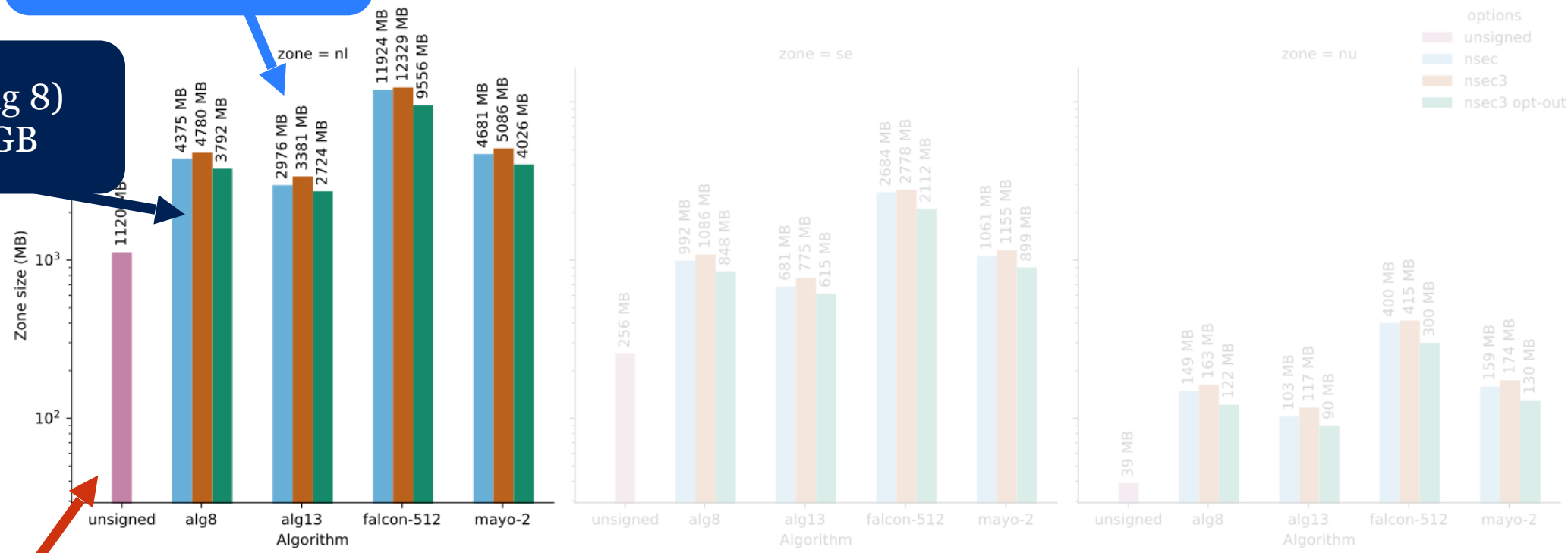
Unsigned ~1 GB

Zone sizes

ECC (alg 13)
~3 GB

RSA (alg 8)
~4.5 GB

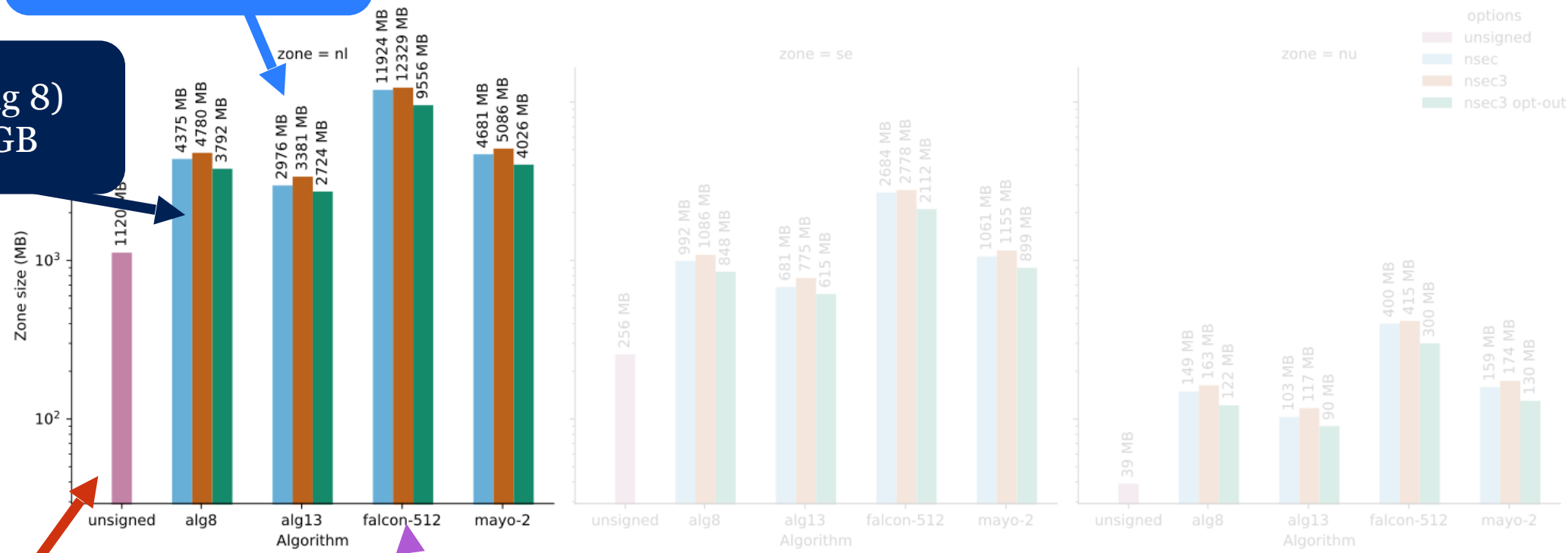
Unsigned ~1 GB



Zone sizes

ECC (alg 13)
~3 GB

RSA (alg 8)
~4.5 GB



Unsigned ~1 GB

Falcon ~12 GB

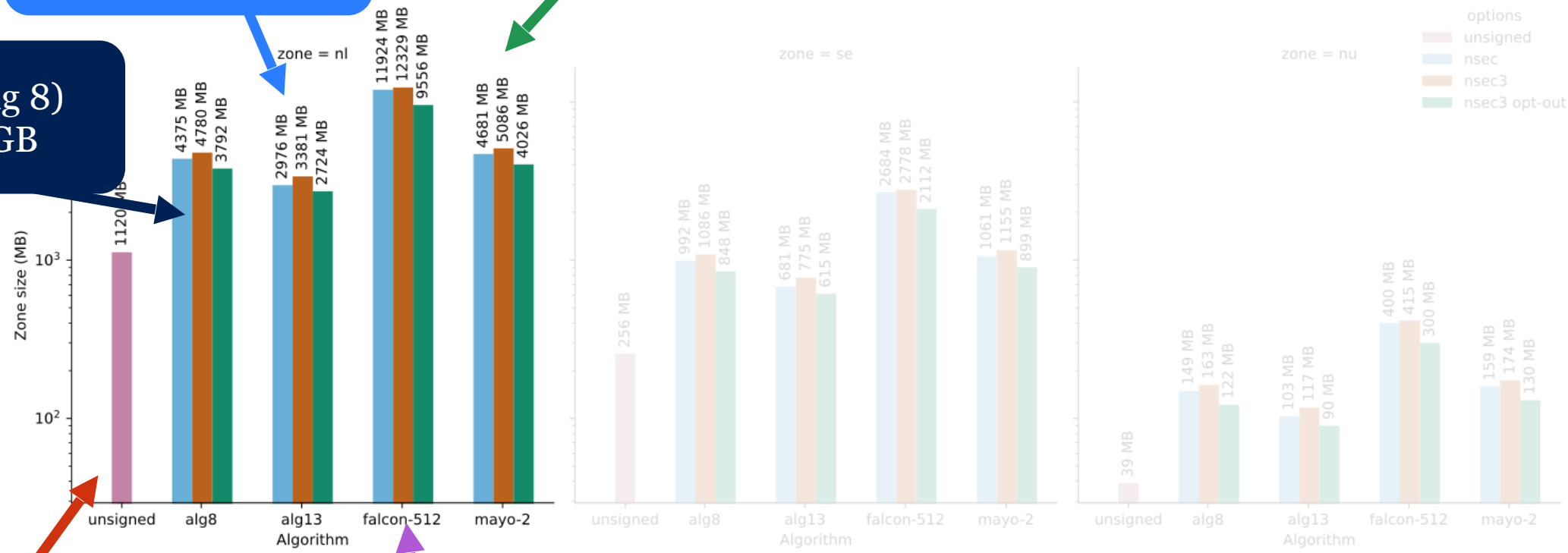
SIDN LABS

Zone sizes

ECC (alg 13)
~3 GB

Mayo ~5 GB

RSA (alg 8)
~4.5 GB

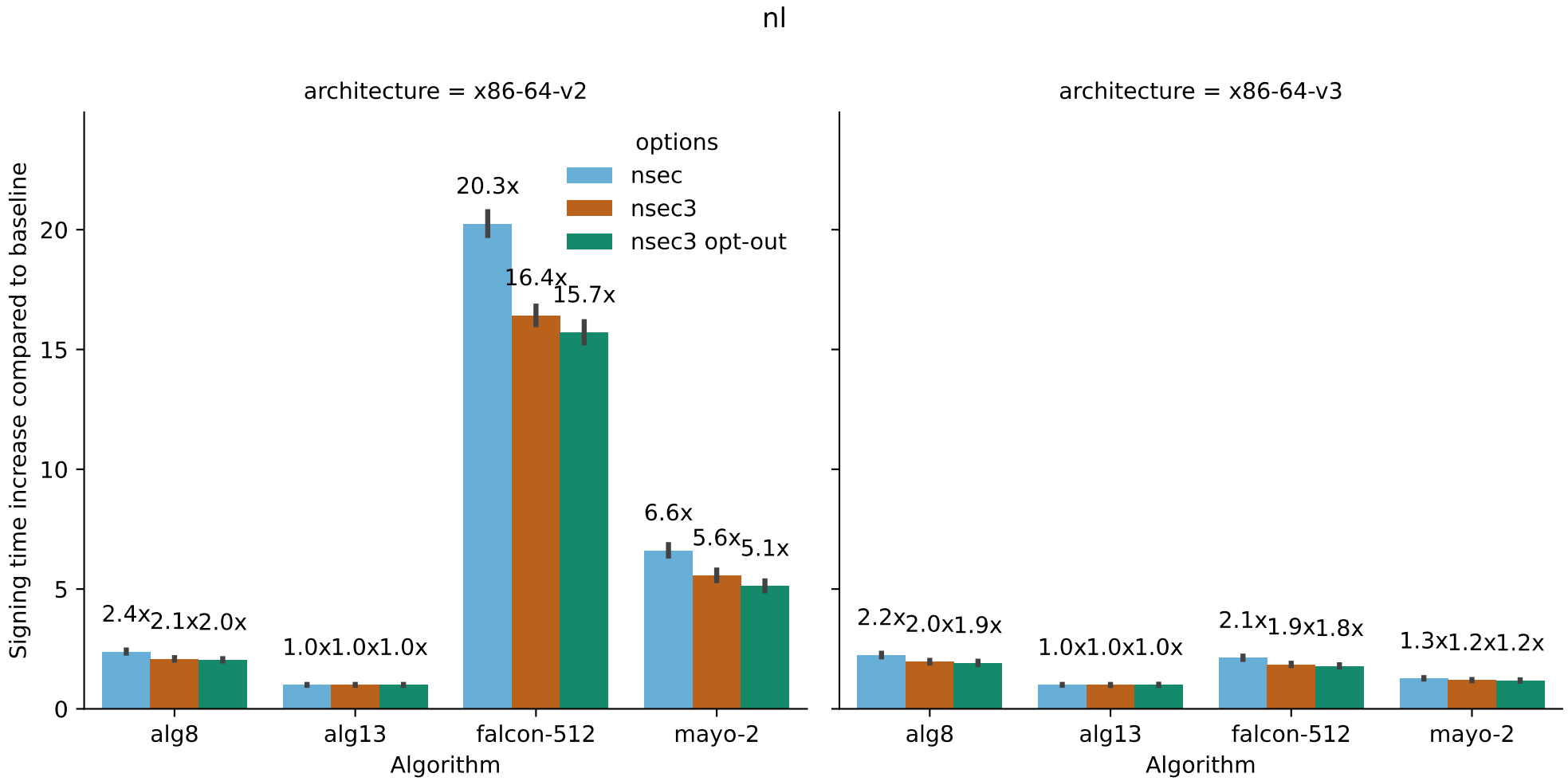


Unsigned ~1 GB

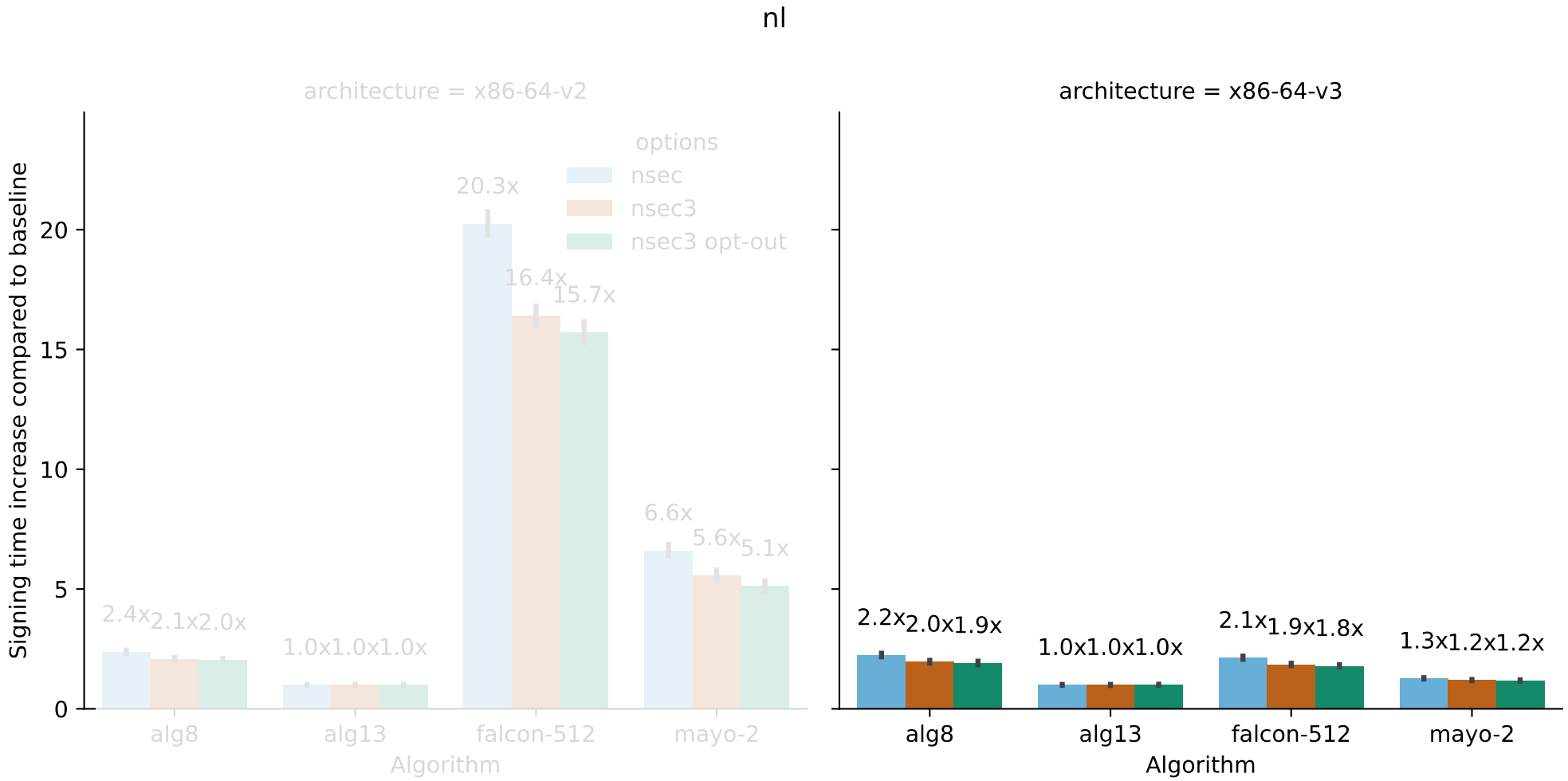
Falcon ~12 GB

SIDN LABS

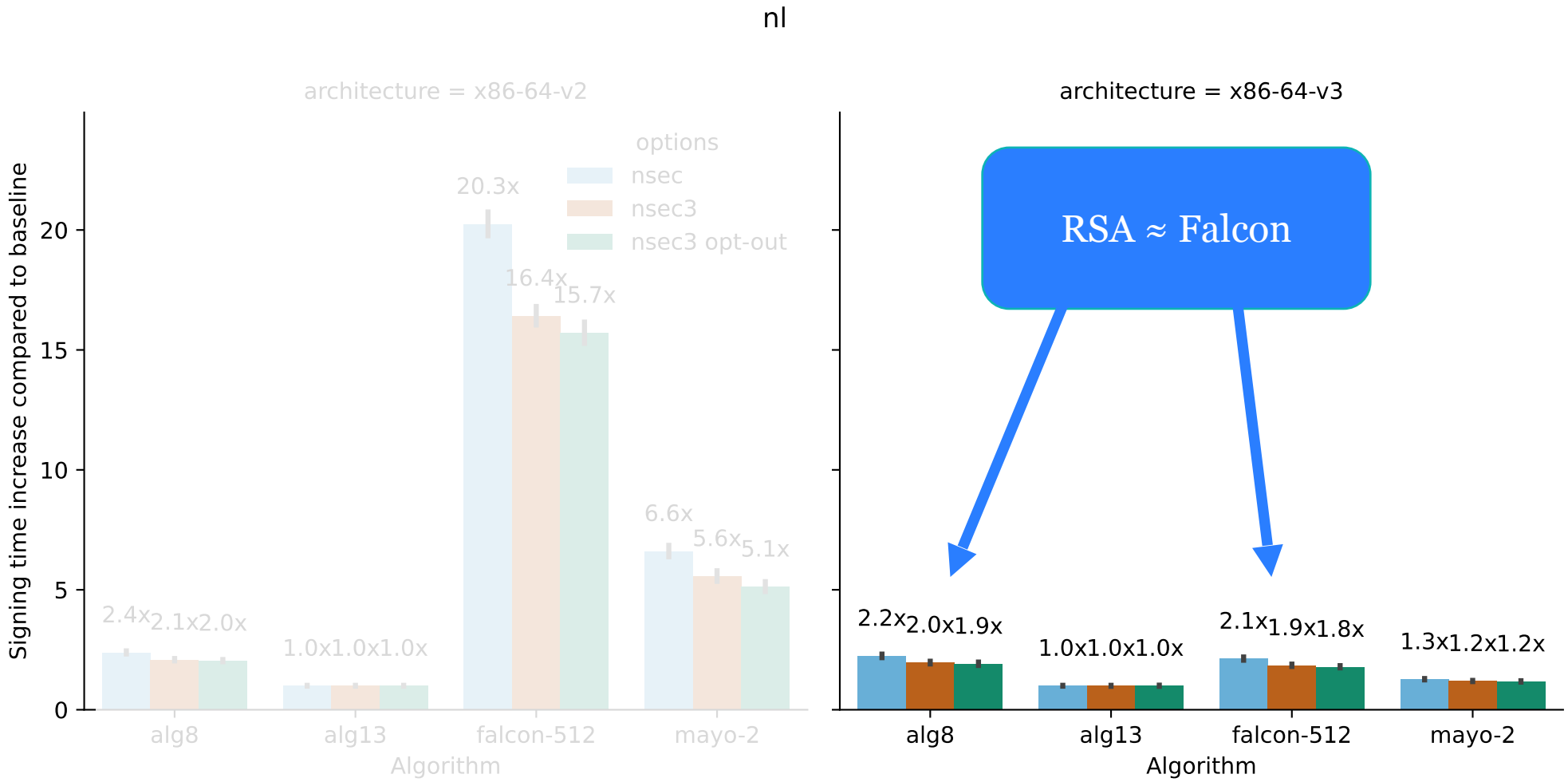
Signing time of entire .nl zone



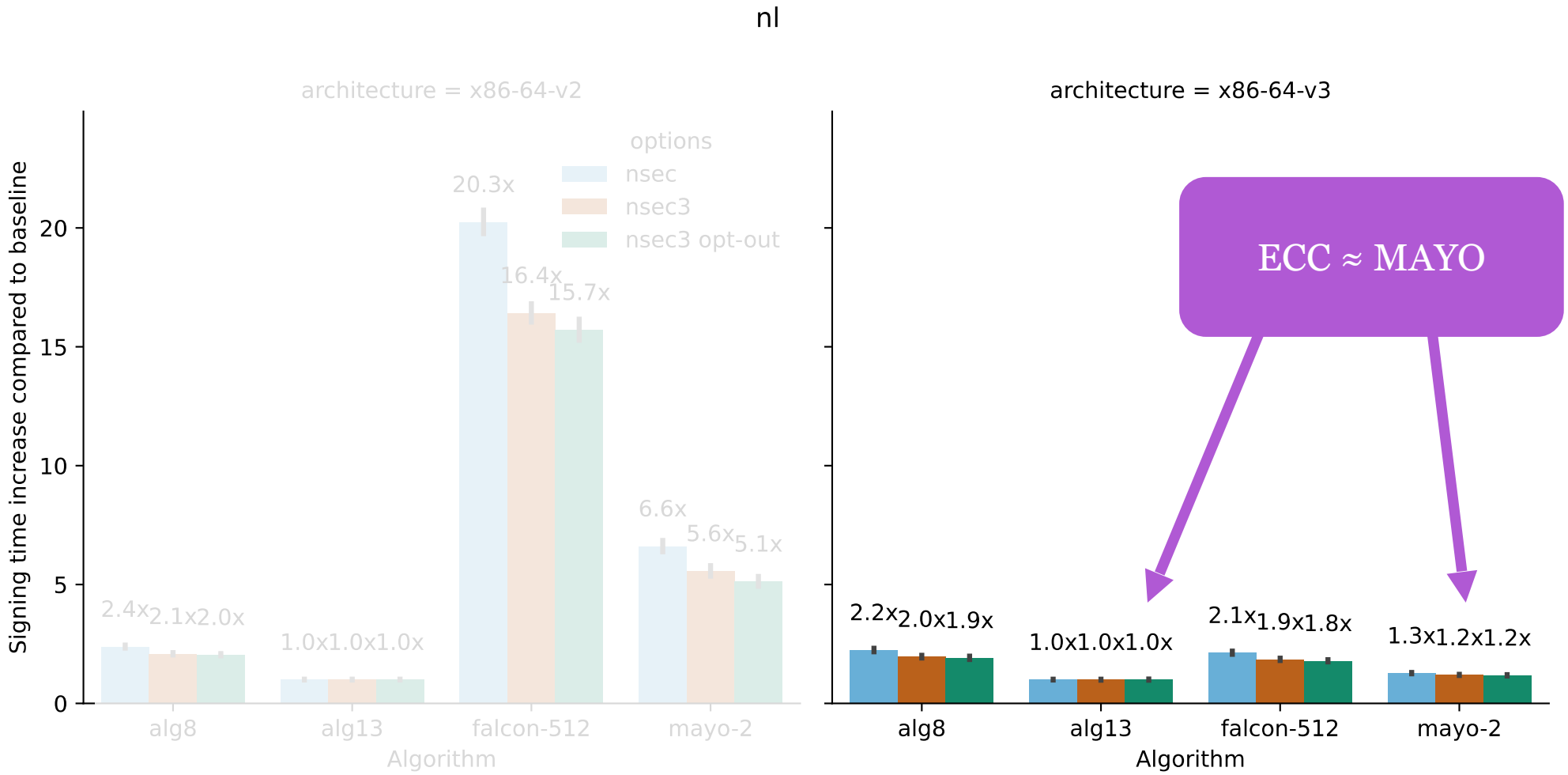
Signing time of entire .nl zone



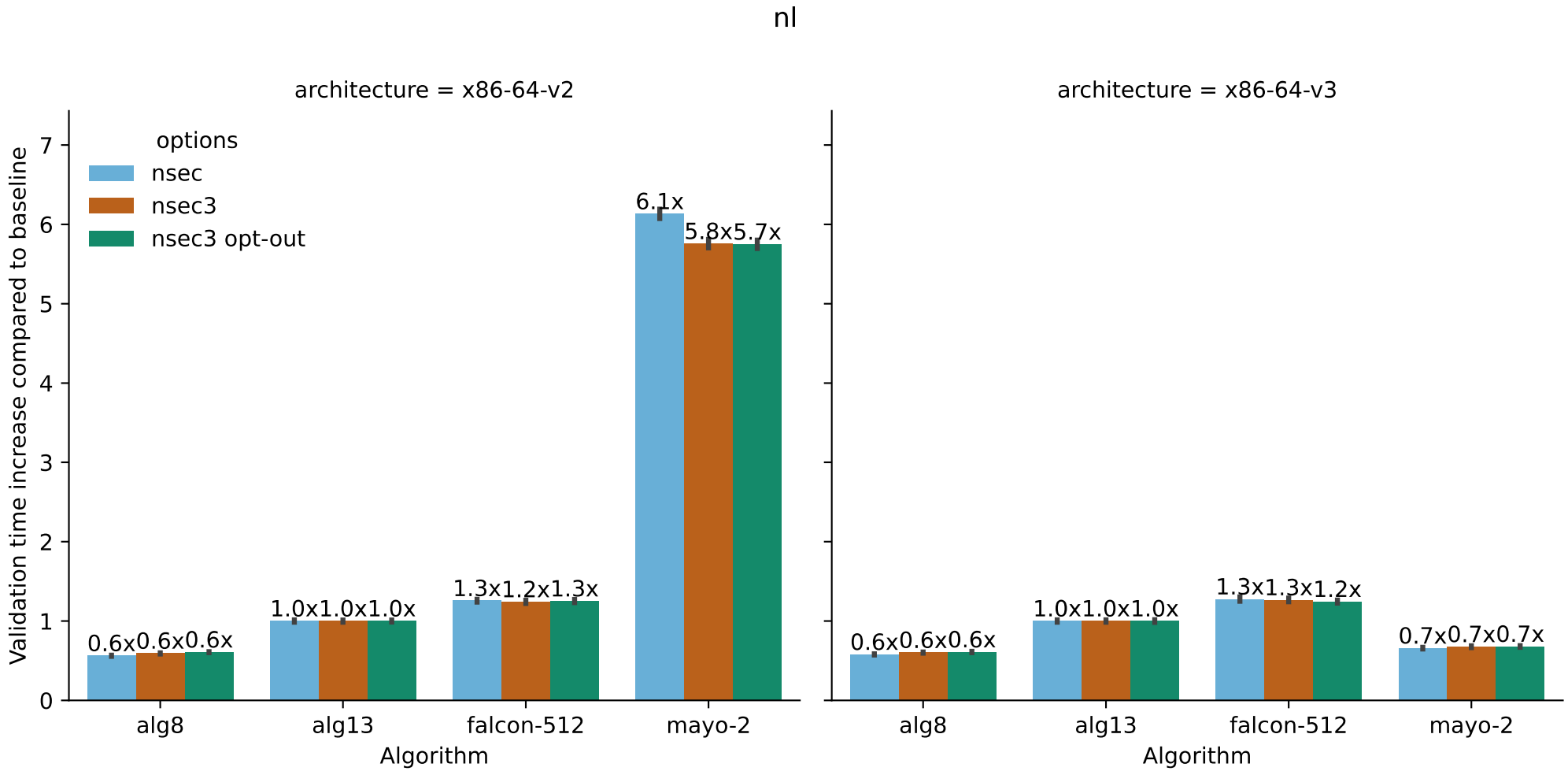
Signing time of entire .nl zone



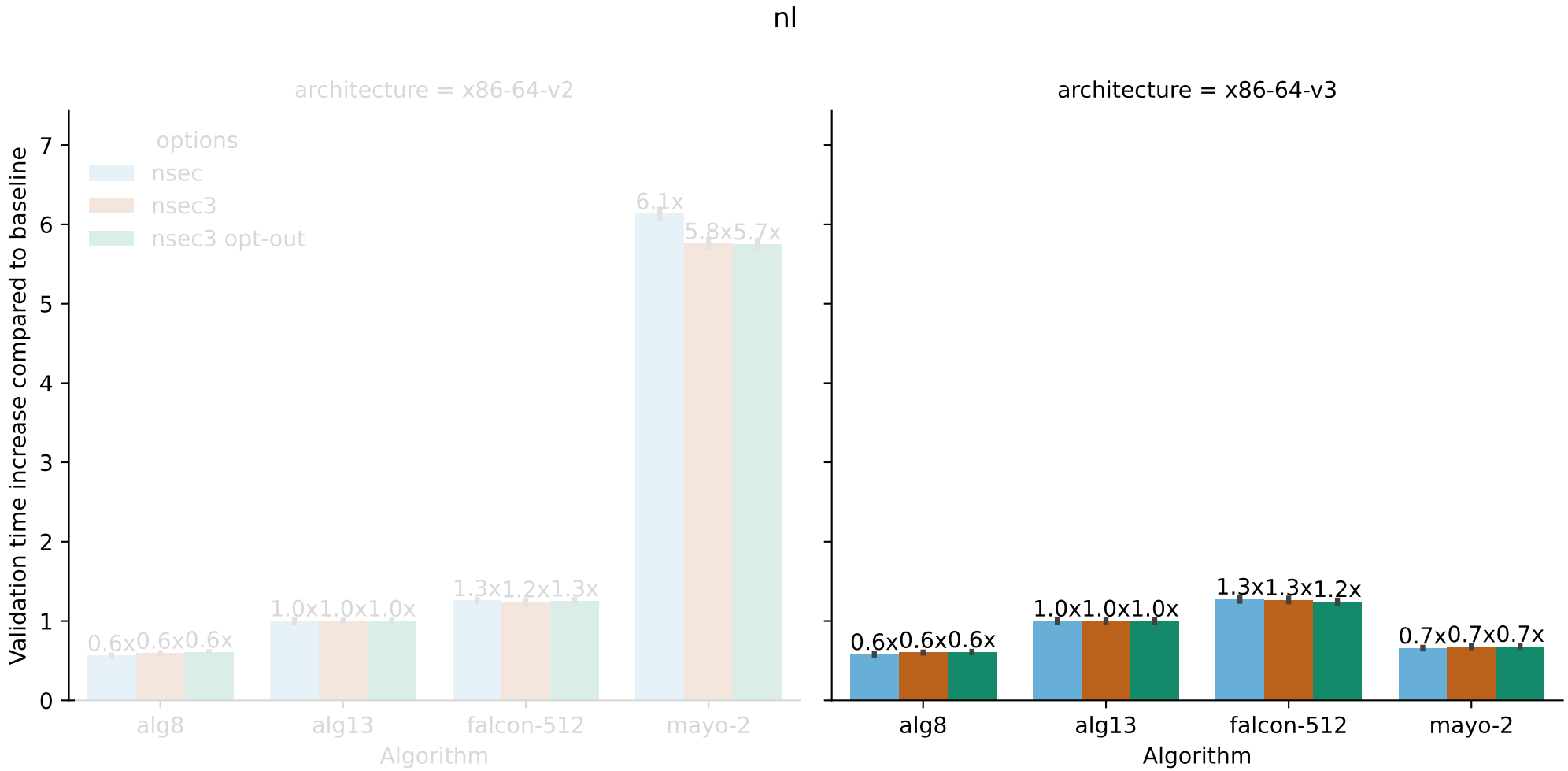
Signing time of entire .nl zone



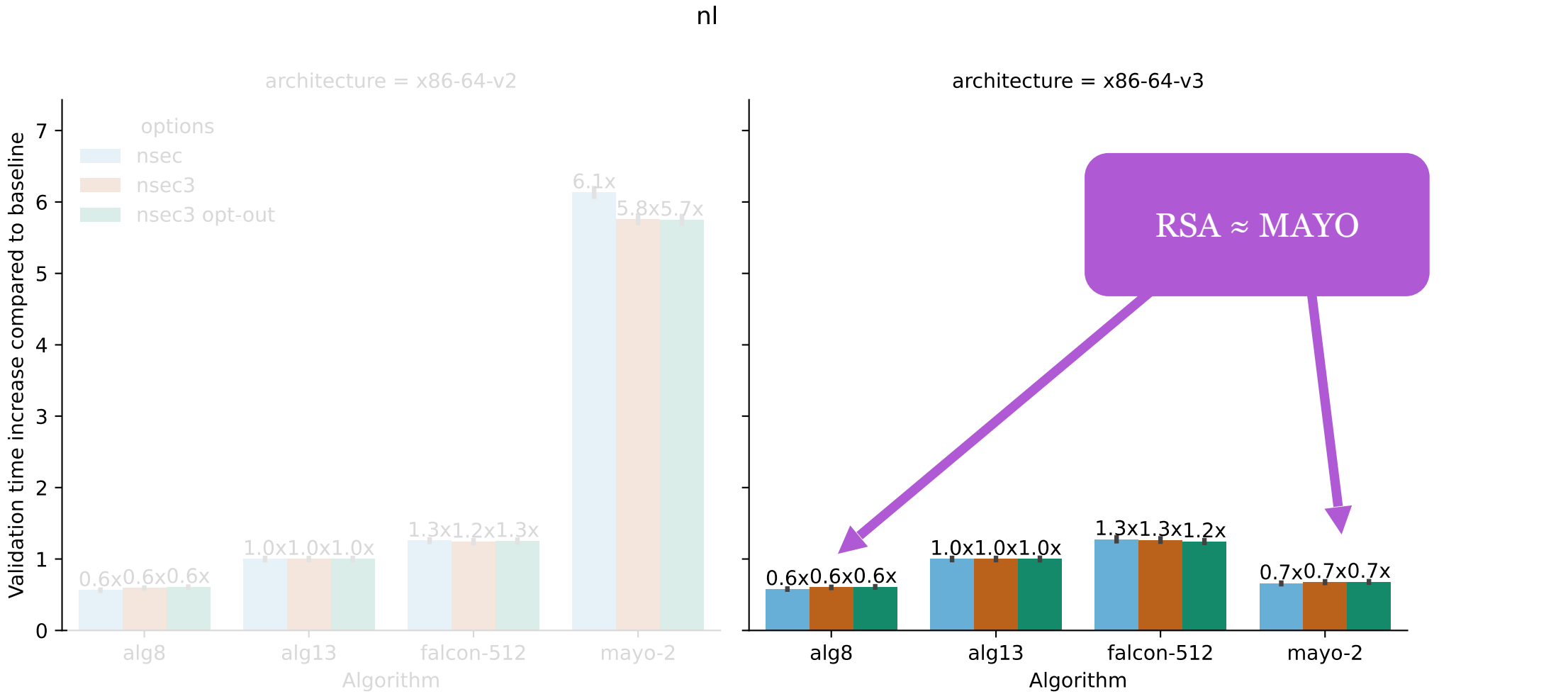
Validating the entire .nl zone



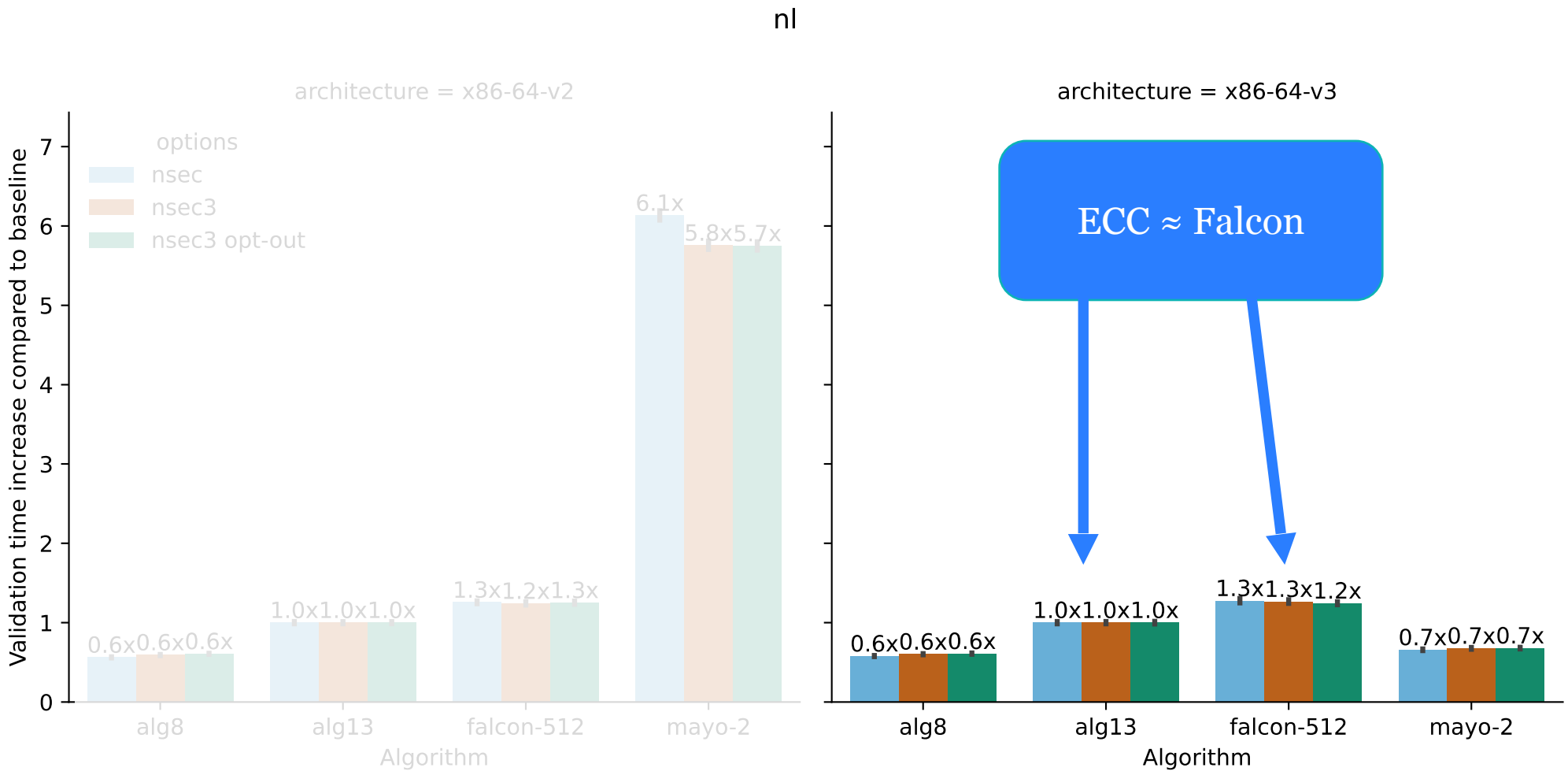
Validating the entire .nl zone



Validating the entire .nl zone



Validating the entire .nl zone

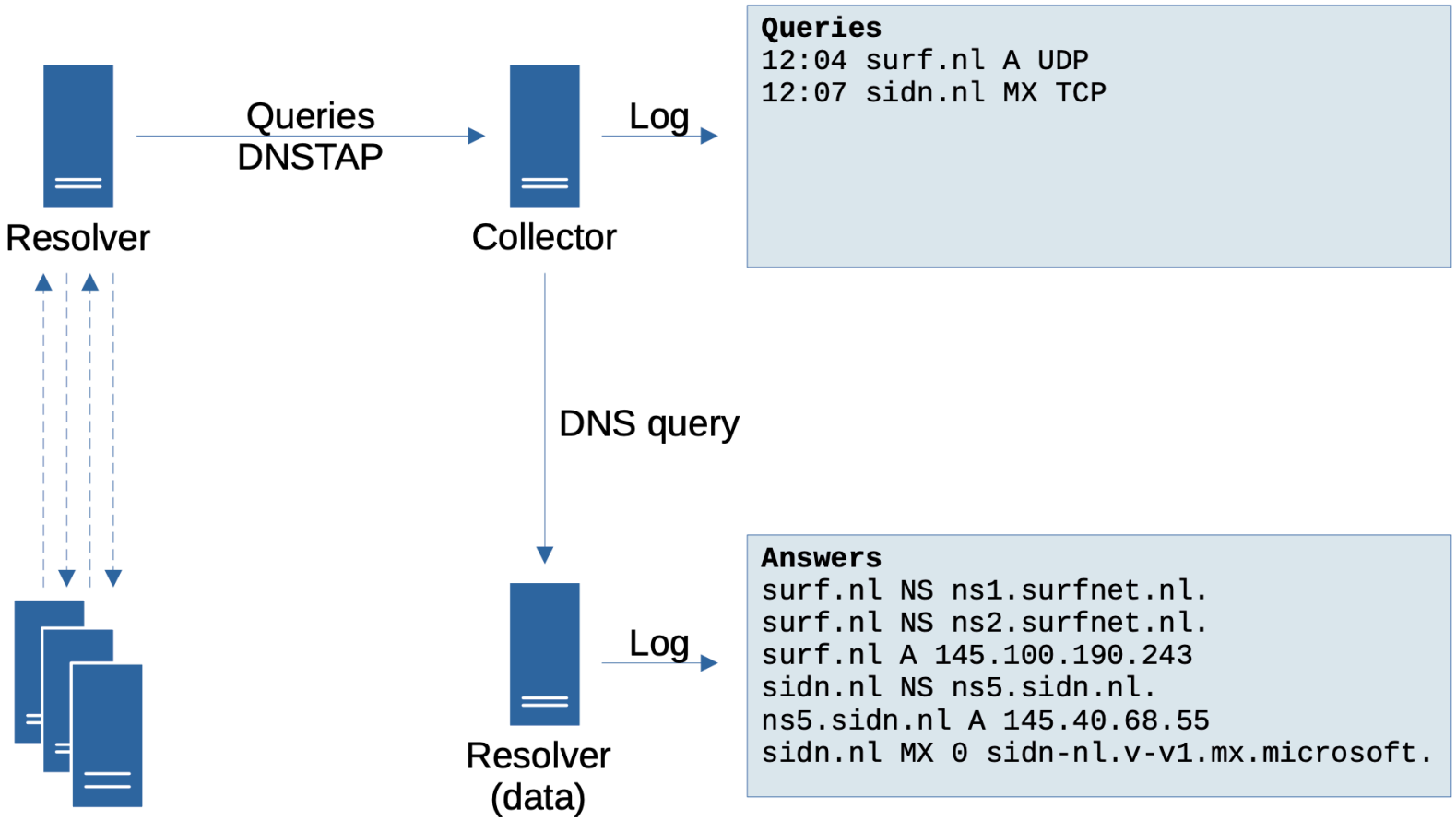



CAN WE FIX IT ?
YES WE CAN!!


WHAT'S
NEXT?

Impact of more TCP on authoritative nameservers

Measuring impact on resolvers



Add more algorithms to our testbed

About QR-UOV

The QR-UOV is an efficient signature scheme for the UOV scheme by using a polynomial quotient ring. The polynomial multiplication is embedded in a special matrix for fast processing.

MTL

MTL Reference Library Implementation based on draft-harvey-cfrg-mtl-mode-00

Dependencies

- libcrypto from openssl version 3.1.0 or newer (or substitute crypto operations t functions)
- liboqs version 0.7.2 or newer (for the examples). To include the liboqs library as change the -loqs to -l:*path*/liboqs.a in the examples/Makefile.am.
- Applications using the MTL Reference Library should also link with the C math

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

Elmer Lastdrager
Research Engineer SIDN Labs
elmer.lastdrager@sidn.nl