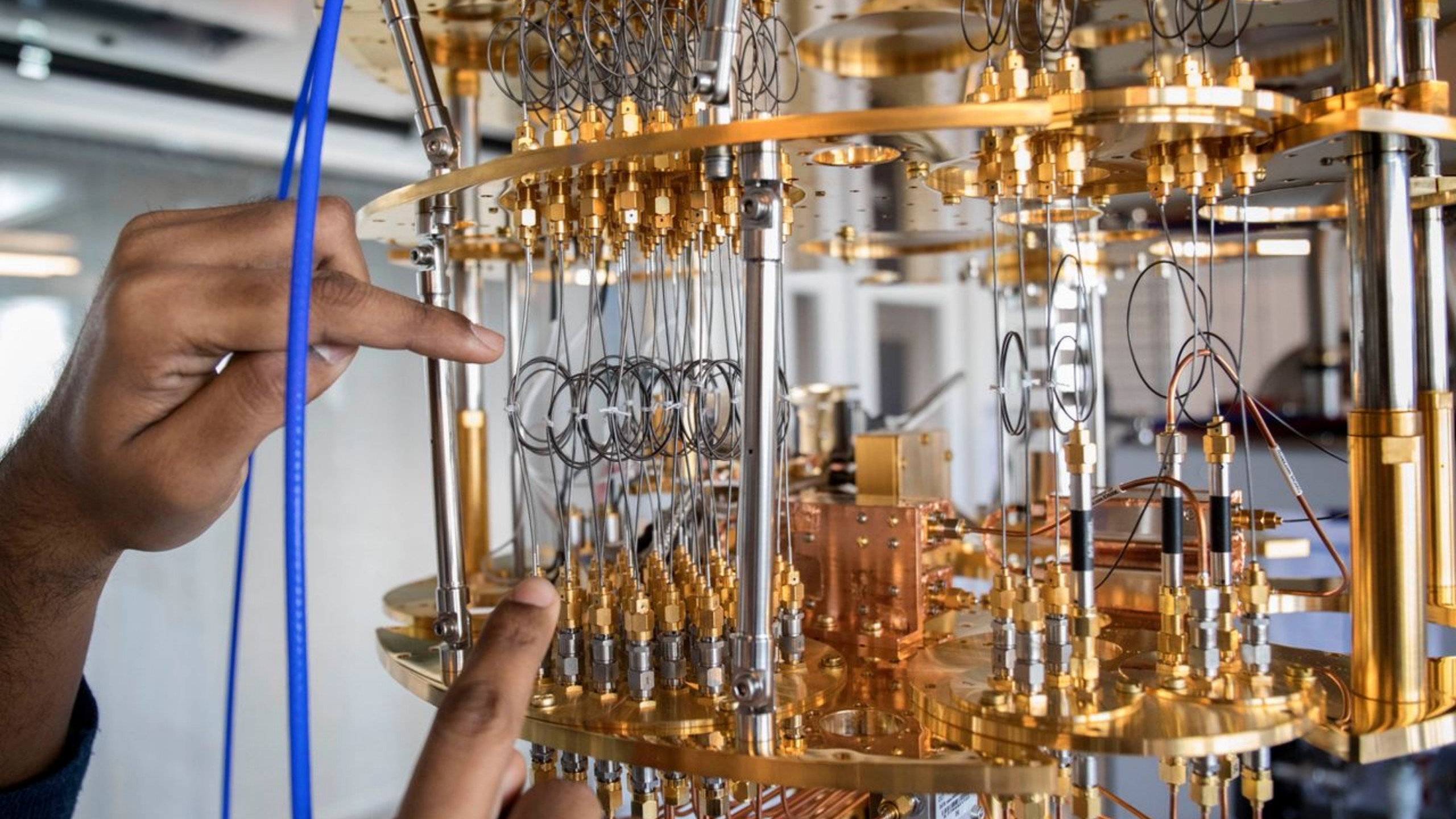
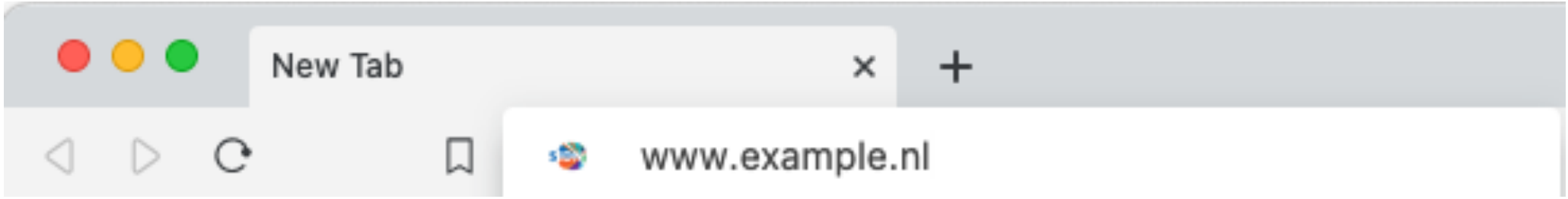
Evaluating Post-Quantum Cryptography in DNSSEC Signing for Top-Level Domain Operators

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

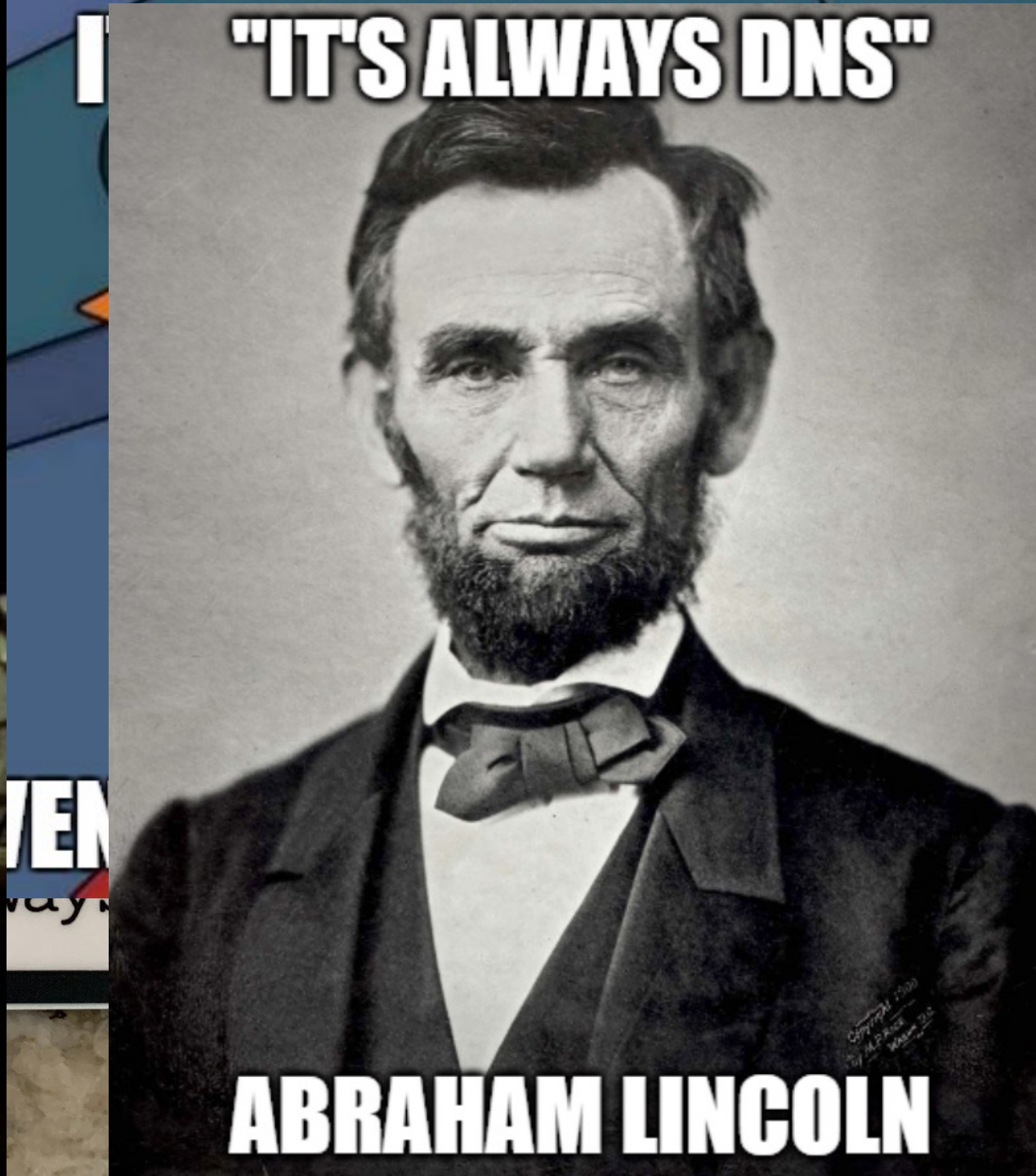
13 June 2025





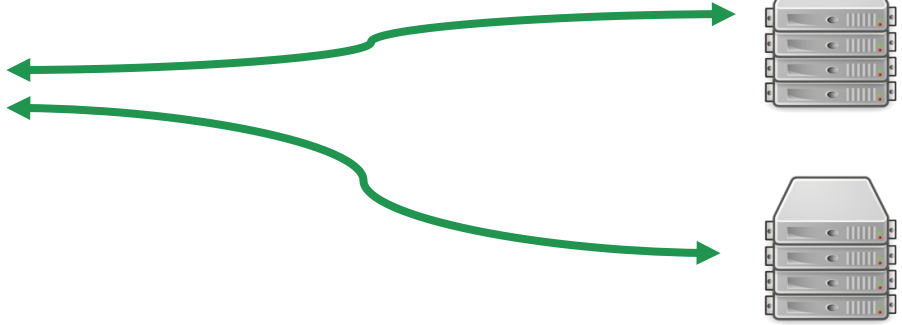
2a00:d78:0:712:94:198:159:35


Why is it when something happens, it's always you three?
DNS
BGP
DHCP


"IT'S ALWAYS DNS"
ABRAHAM LINCOLN

User

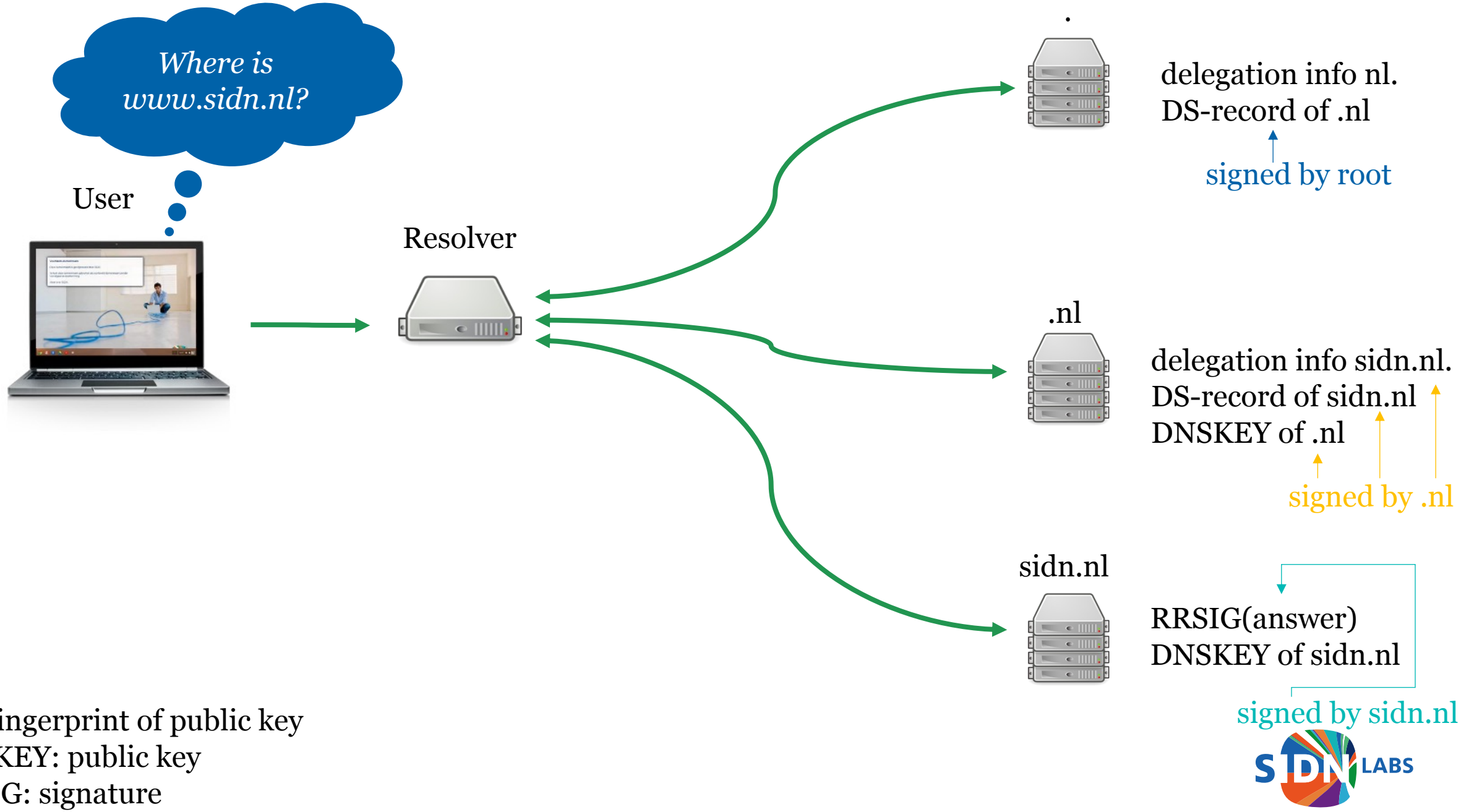
Resolver



DoH, DoT, DNScrypt

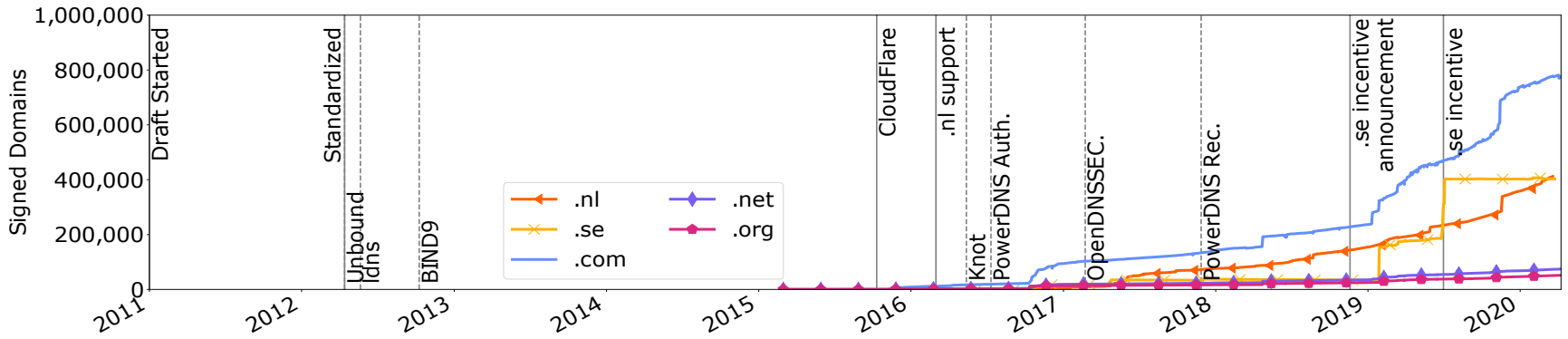
DNSSEC

SIDN LABS



DS: fingerprint of public key
DNSKEY: public key
RRSIG: signature

Time to deploy new algorithm in DNSSEC, +- 10 years



Timeline showing deployment of ECDSA256, from '*Making DNSSEC Future Proof*' by dr. Moritz Müller.

Post-quantum Algorithms Testing and Analysis for the DNS

Algorithm	Public key size	Signature size
RSA-1280	162*	160
ECDSA-P256	64	64
Falcon-512	897	666
MAYO-2 (R1)	4912	186

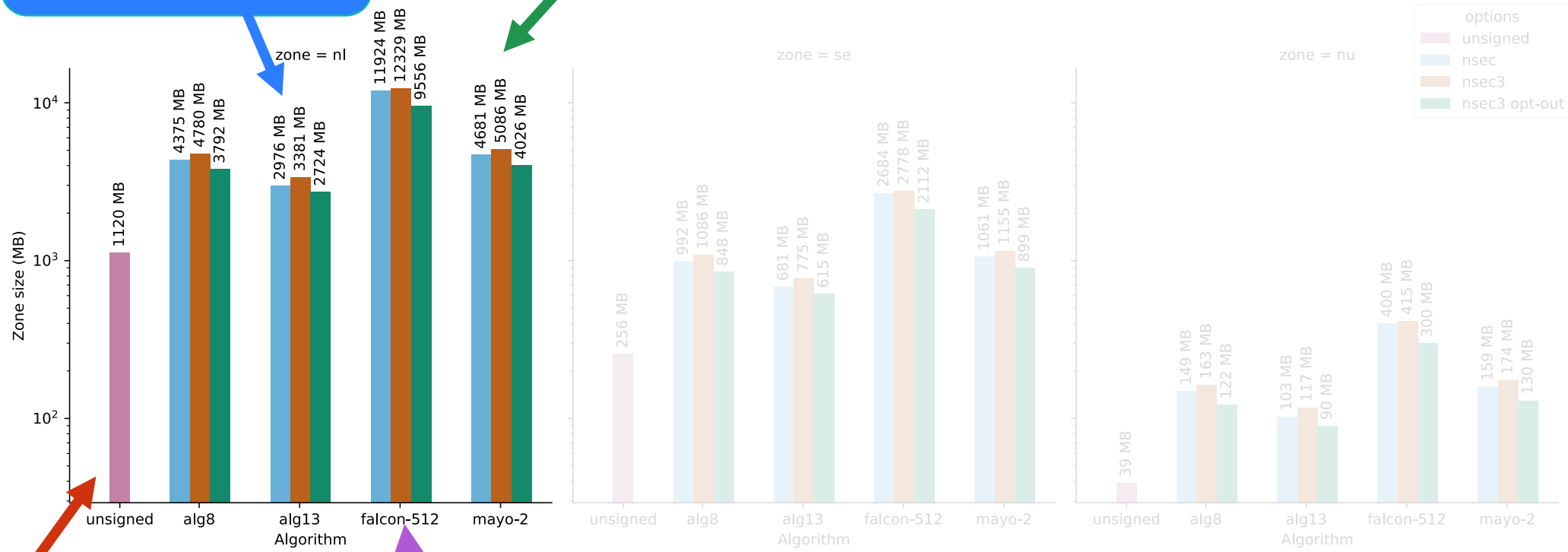
all numbers are in bytes

Hardware support (AVX2)	Proof of nonexistence
4 algorithms	3 zonefiles

Zone sizes

ECC (alg 13)
~3 GB

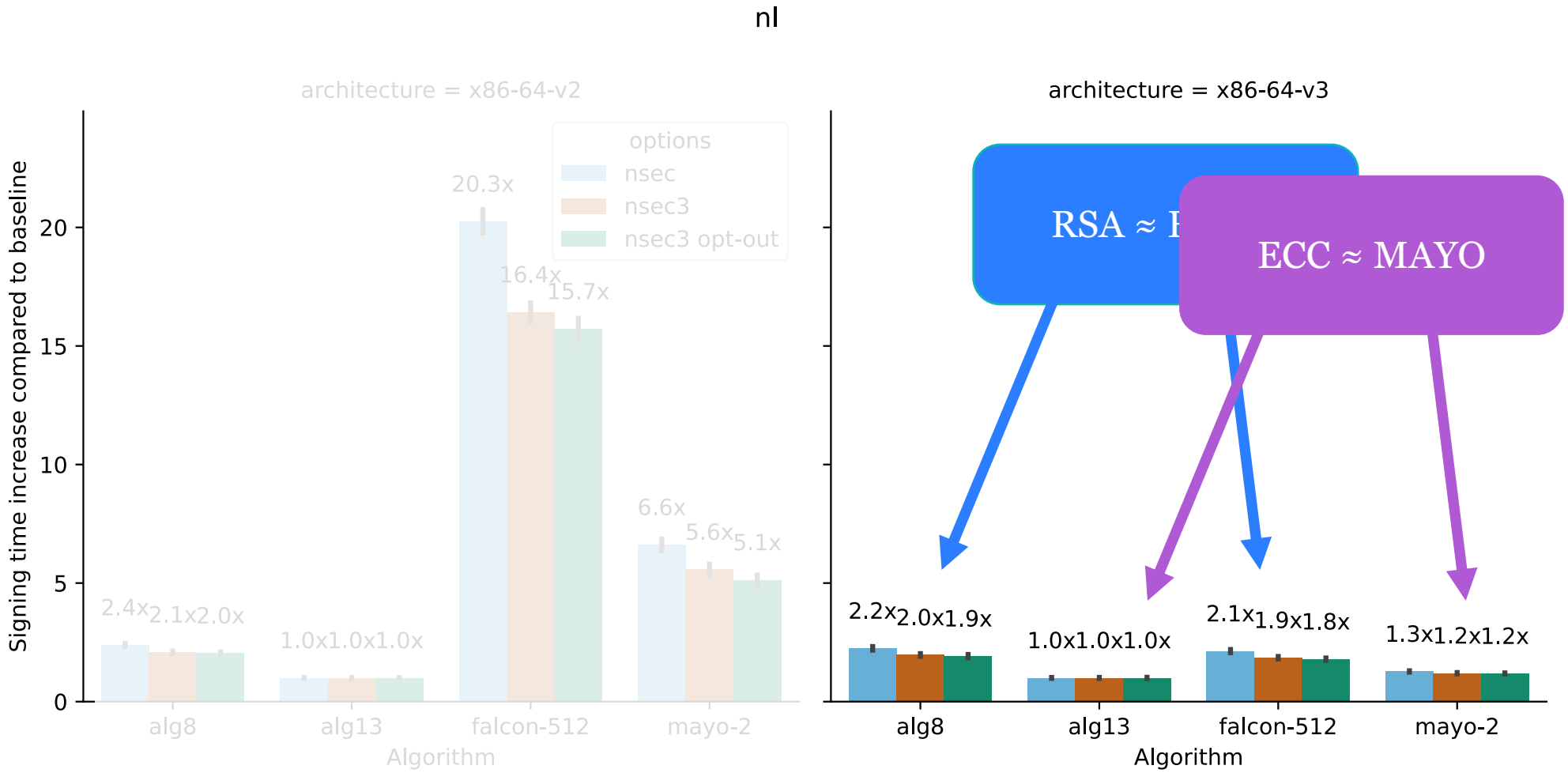
Mayo ~5 GB



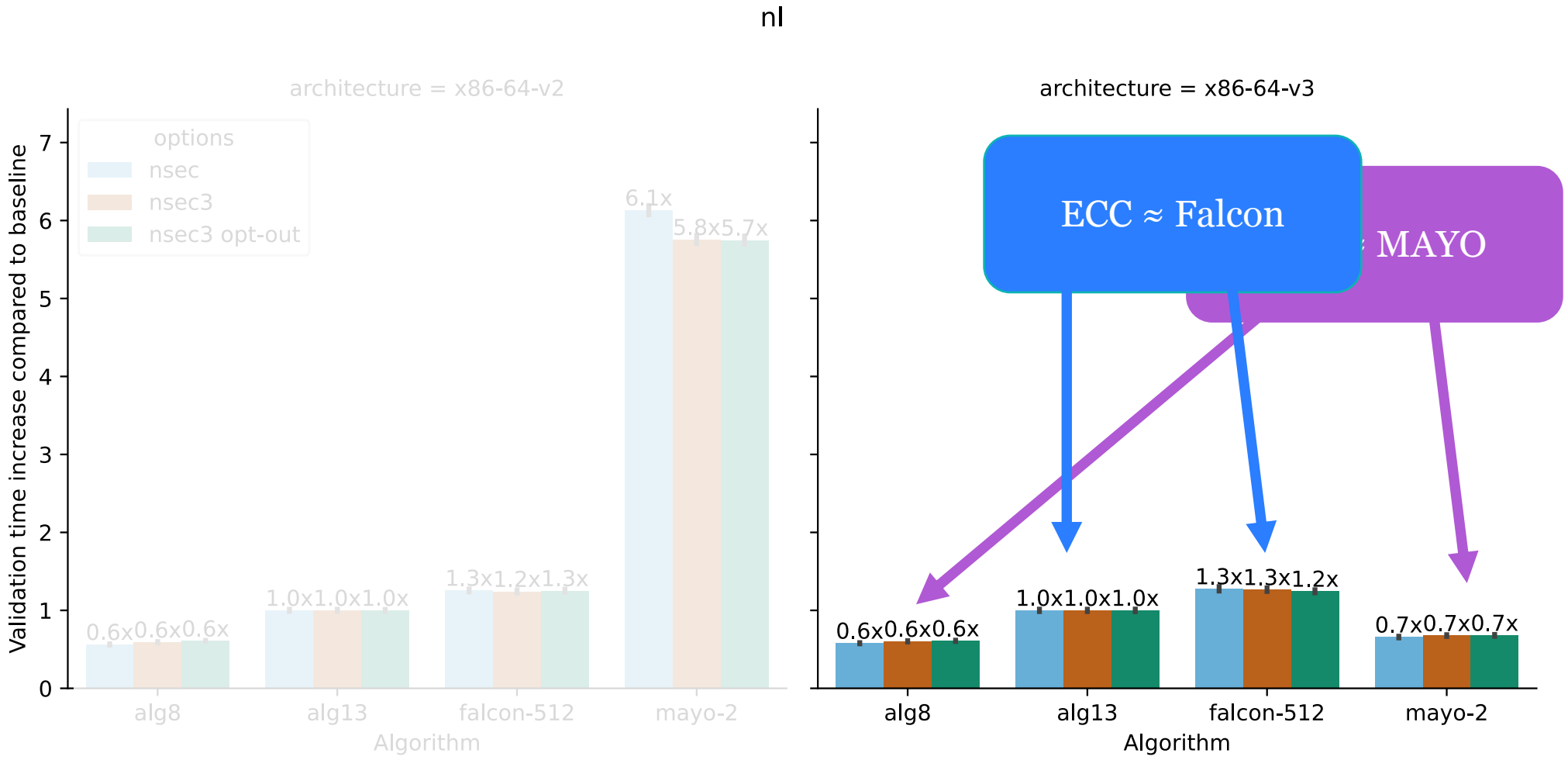
Unsigned ~1 GB

Falcon ~12 GB

Signing time of entire .nl zone



Validating the entire .nl zone




CAN WE FIX IT ?
YES WE CAN!!


WHAT'S
NEXT?

Download and enable PQC for DNS yourself

https://patad.sidnlabs.nl

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

https://github.com/SIDN/OQS-bind

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