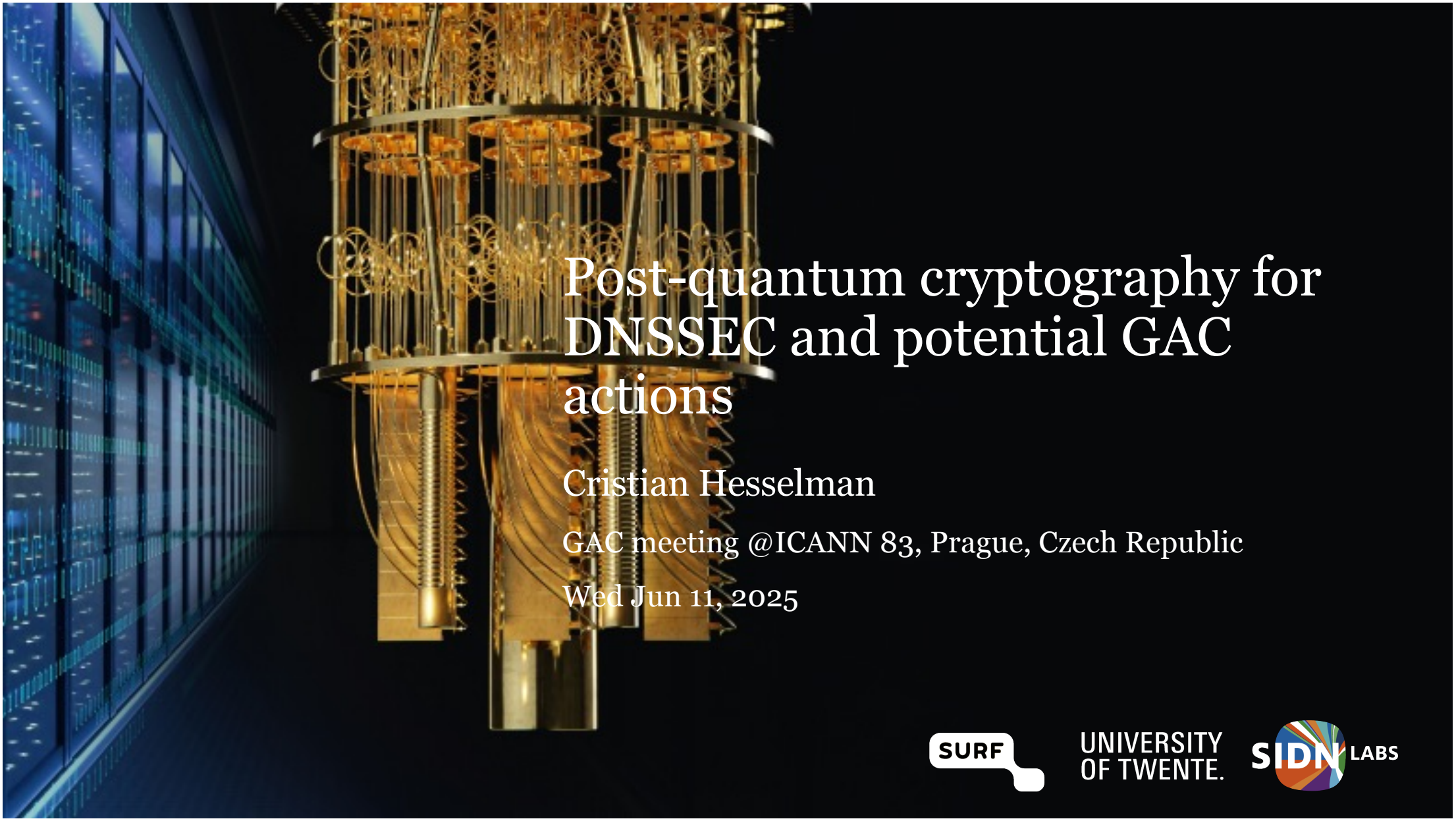


Post-quantum cryptography for DNSSEC and potential GAC actions

Cristian Hesselman

GAC meeting @ICANN 83, Prague, Czech Republic

Wed Jun 11, 2025

SURF

UNIVERSITY OF TWENTE.

SIDN LABS

What are the expectations of quantum computers?

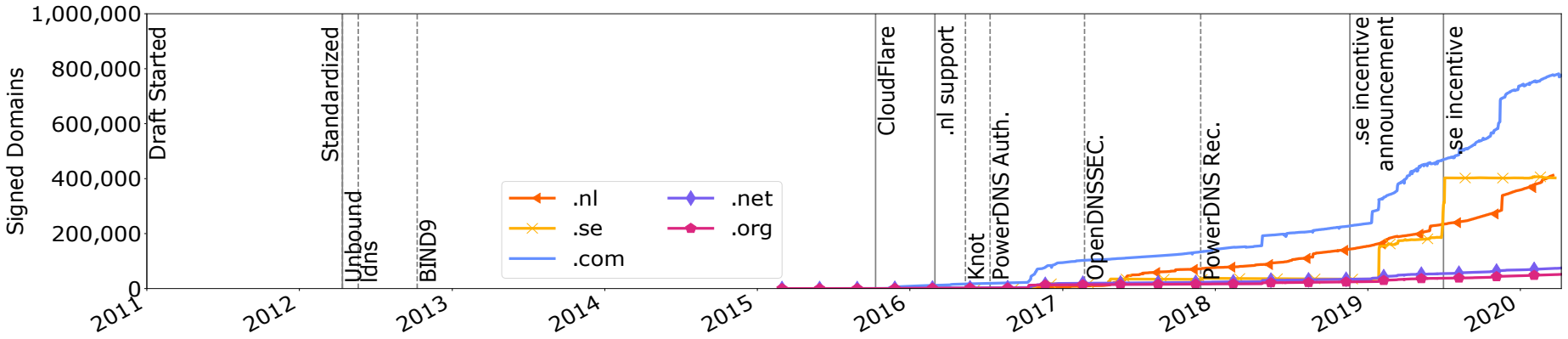
- Accelerated drug discovery, improved machine learning, development of revolutionary materials

- Downside: could break current cryptography
  - Such as the algorithms that DNSSEC uses to protect the authenticity and integrity of DNS responses
  - Sign “evil” DNS messages, redirecting people or software programs to sites they’re not supposed to go to
  - “In-post quantum era” attack, not store-now-decrypt later

- Experts think this won’t happen for another 10-15 years, but…

“The race to find the quantum hotspot”, Nature, May 2023
R. de Wolf, “The potential impact of quantum computers on society”, Ethics and Information Technology, 2017

Deploying new crypto for DNSSEC takes a long time

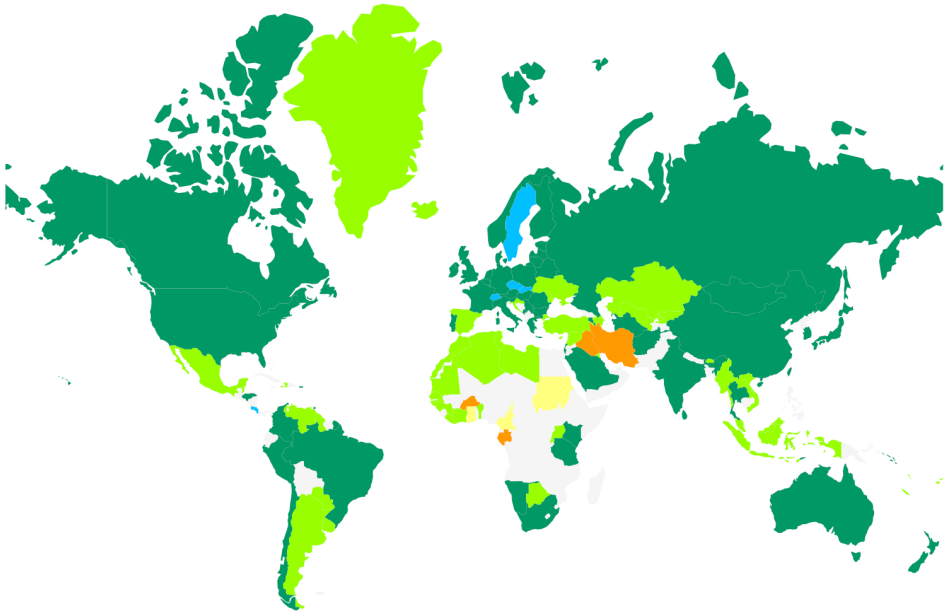


Domains signed with ECDSA256 and resolvers able validating this algorithm

M. Müller, "Making DNSSEC Future Proof", Ph.D. thesis, University of Twente, Sep 2021

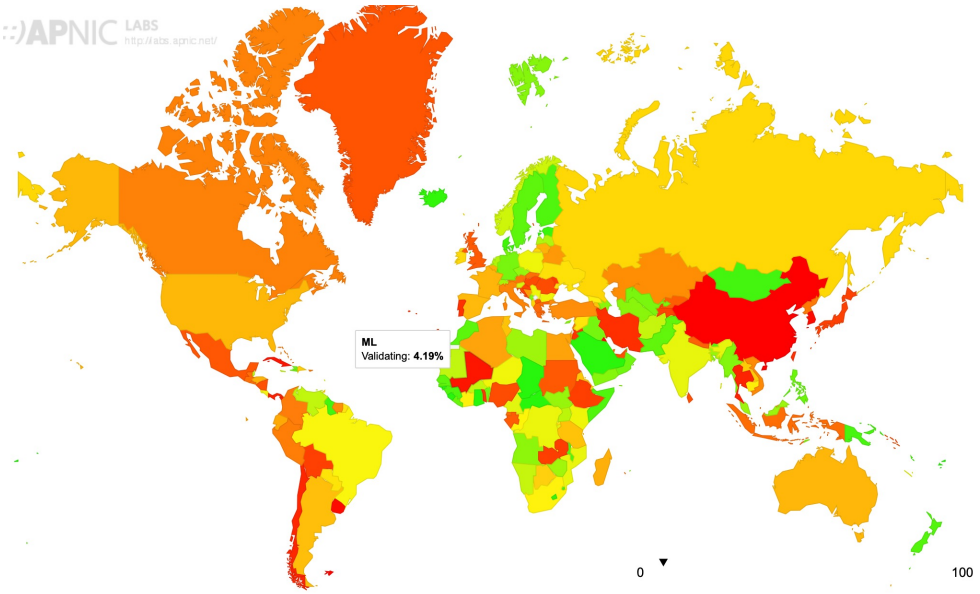
Significant global DNSSEC deployment

Signing (adding signatures)



https://maps.dnssec.gmu.edu

Validation (checking signatures)



https://stats.labs.apnic.net/dnssec

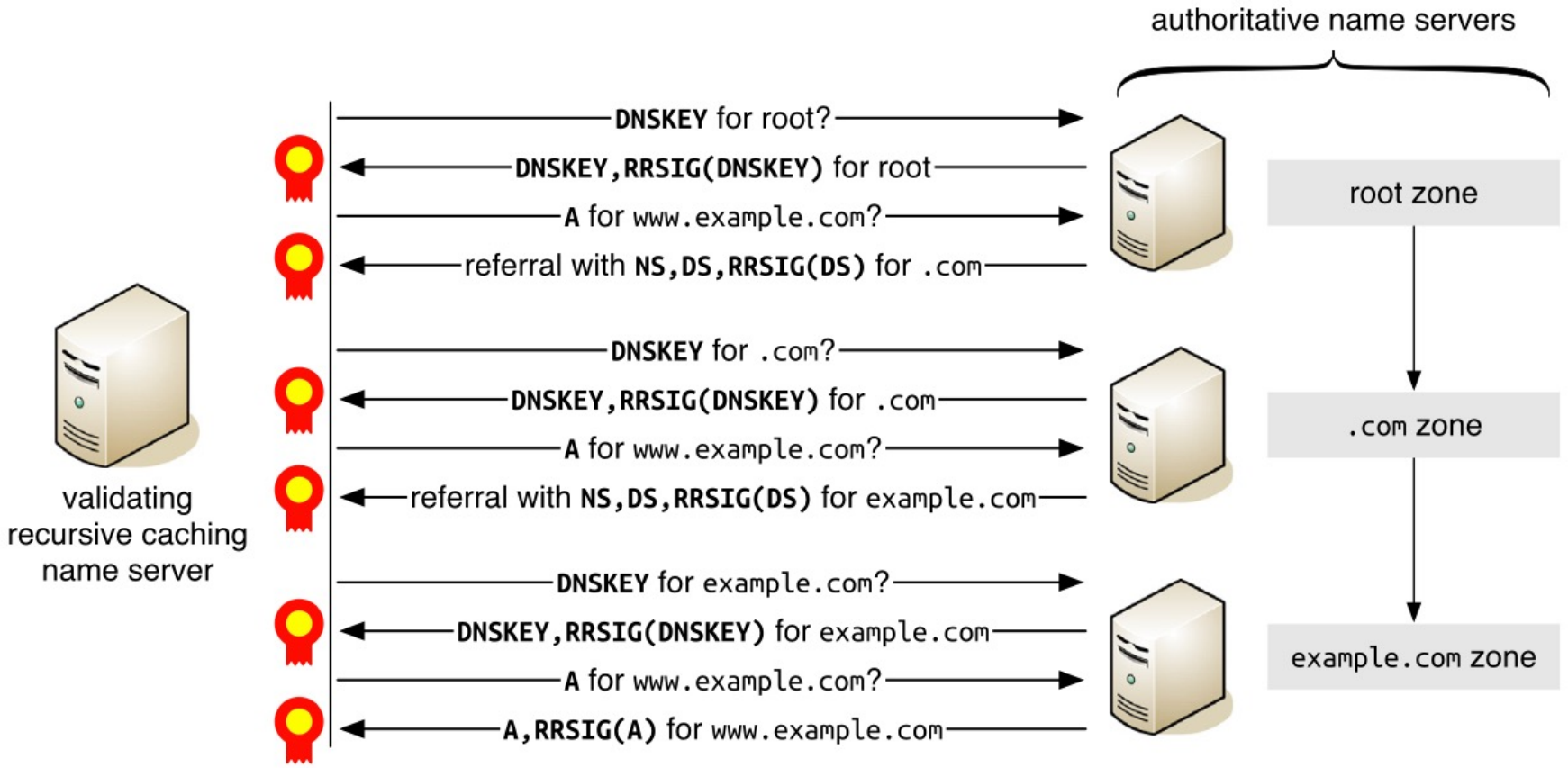
SIDN LABS

So, need to start protecting DNSSEC's crypto today

Strategy	Pros	Cons
Replace: drop-in replacement of current DNSSEC algoritms	• Relatively easy to implement and standardize • "Quick fix"	• Operational risks because of differenent algoritm properties • Would benefit from collaboration with NIST, which adds complexity
Redesign: change DNSSEC to accommodate PQC algorithms	• "Clean slate" to reduce operational risks (no legacy) • Size and computational costs spread across multiple messages (MTL) • Could encourage more people to deploy DNS security	• Requires community support to get standardized and adopted • Requires widely deployed support by DNS software • Will likely take years to develop, test, and standardize
Retire: consider DNSSEC "lost": stop using and supporting it	• Reduces overhead in the DNS • Low impact for some TLDs (e.g., only 5% of .com has been signed)	• DNS open to old attacks, no support for authentication and veirification • Impacts protocols that depend on DNSSEC, such as DANE • High impact for some TLDs (e.g., 62% of .nl has been signed)

SIDN LABS

Change public keys and signatures



O. van der Toorn, M. Müller, S. Dickinson, C. Hesselman, A. Sperotto & R. van Rijswijk-Deij, "Addressing the challenges of modern DNS: a comprehensive tutorial", Computer Science Review, June 2022

Examples of public keys and signatures

example.nl. 3595 IN DNSKEY 257 3 13 (
DfvVT9W9/MuL6HwX18rU3W5Jv2YvdNkWfz/GpxNPY/OZ
o+b31ltiZD7LenCC2iHRaOOzwKE/MUtMegHclrkGqg==
) ; KSK; alg = ECDSAP256SHA256 ; key id = 21532

sidnlabs.nl. 237 IN DNSKEY 256 3 251 (
CS/9zNAFZTYeFn1mGSJRonlASnlCrxWstBQvwotbPo4m
tBnwaQr7toekjk31dBO03OdO0AviwOsvRJ1CkVWdpTLS
pjPdJUxKAuqZLC0LBvaBe3YNiFvJNKn/TTKrtl+Twmb1
CggWOzuOrqtNthA168VYjQzF5sC2ai0pw+LR2rrmiTvs
2BW5+tczbhOzETDhRJvdqBiEuSEqwwZwLTeX7g65i3J8
yPbtb4warSSpSmRl8DdGu1NtYIoj+vPRLIGtgRt/Dbki
auFn14esSyKaUSfn2Boi9MjYjgSpxSsViUOmb2r39N3B
ZUgKvKI35wGfZuyDom2jm2BguDTj7lX6TaByXmeMGMOz
ZcUrolVidXqdQBpOK1TCBK4RdOK6bdt1Q9G5a8AP65Zq
RzobkgmotIERH634NJYukU6OFX29QtVZyXNp9h/z0EL9
lSnrdvFmHiM1PyIFHhtdkuXH1cTJdsK3YPRfCaophUXm
qQGuBoWKWtt8asAR6fUCAFSu39t0AGYHmOHC5YtZHcBh
oIPLBmM4+nCBwLZw4ltWGV8ug4jKcF90BGE67vXZi4la
okVrlR3Hbzgw+tkEniccPctxz+VRFthxkyA0pUCLwmtM
ig3h4Buuy0S8xjRnfEWoDCi2+ABmDAux1teeF7CtfmBp
DCXkIlxAVGNlCQ5uAyIIVMB0WtNjTAw/bI09UoYmv7x2
M7v0wP96DeH2yKIVTPjho74ut09iPPjyAqcsmB93WSuy
i8jv1VrsGQYWbtY73BsGsW21jw1gseUBqdRe3qMWxlmm
n+SmdlLzjMG5SiENRdZcwStIBzVNifkI0trVny5VSREY
wmGBHpNQE6NJWJWymGsjIKFbdeGTQYpPQqKo75dfoe8H
qDzR9pKbab6J9OQUVbqtdiI+qc1siDlzRIFRFDox0oZf
TLy58lssCihavo/icNwvviHlQtdR054K+6UzlWWQejIF
dtJbh2DywYkaJo+CJCPyn3NZ8Ib1ph9X0onF81QV0BqO
q3rjQN9zImC2rRe8A8J32/iKyhFtHgHboGxDMcwpYQBE
ccHRcPvUWwHkYIAh7dlqZLUp82GmBDlulRkRbTPU4bpV
zOUrHNCltQkLLBm8thZBS10g36YOA2ol5johYA0Le4wv
WJHgmlmCmZSnnuSTNjOjKRpKOW1Z8Y+YGCnQvQfACbSq
UV5DES/Y
) ; ZSK; alg = 251 ; key id = 7629

example.nl. 3595 IN RRSIG DNSKEY 13 2 3600 (
20250619080303 20250605072829 21532 example.nl.
GZTrA3y+CkSfoVX9173dxv+hQL7bm094FZKV1zwN+Fum
RtzB5zWPHyl5dzUpbIpgvenOujmLdfWGi+uj9YZ+uA==)

sidnlabs.nl. 3600 IN RRSIG TXT 251 2 3600 (
20250619000000 20250529000000 7629 sidnlabs.nl.
OehawaGN8Vd7T1MewNCZvo38ykzqgAtuU6dqMKketrsm
/XLLUXTzB/qAIDCJA5kaHSglI0bBOeZjHtJHmvQ0j5vX
qc9cpMvSkowoyFx0z2emO/nMfZav5CM4N8pfg1OiZl4j
Z17bMirOEBuLRVTb97yLuZCiaDEvBE2uHPcb3ycsGVbO
YVRyZeiokw89/OMXonXp89iUKdtEv+DK0gph3KcitU5j
k8LFuJjpc0R1dfonHKryOwY21jaqDmVQhGFD//CiJguT
jSITCICG0FAC189s9RMJm22cZb6d3QRTqlFwkvZP5oYw
S3uDLtl48FstdovmkSWaGFM/FqPm6XIJ4ISjftMujVuq
Be4gkcBfLE/ZVEHJG+85b55sMkNQldBEkMktfQOq2OVe
Fv0M8DiIn/6kuaa0QxhNkAwVdqPX2JPoWnnwUa2QKWFb
5/w1ZtdFfr6wcqYdXLkz0P/au++n4+kwJN0XYtLyJE/b
dWs5BaLdMpKrXFpfBB0Ij992zEjvKFwLWGkW/gOY0DnT
XCJc1RocpD0YbCWKLJnIbI52ieFyVzYUjU0zhFIt9LBz
JLC0IiC8s46DuRRIYI05A/RQ6KwPc+XLkkgaZM8gMJE6
9vLZB5rNNiQoyc2xLkNLtlRJtXvJNvFe4fIGDiLuIfY2
Dd14iVKUck2f8cfWT+lxVnsTwUNi3lPzkErKflGXerxs
GXBB810pvmGzpM2ddVIejdnzBO1t0jWL5DNFLewZJRUJ
SK08kvLgP0Y2/vQp+Hw/CwMNUjD48grENC3tvQj2Hcx6
PYw4bJFBq9HalQMvtOtSTdb8i1fv1orGASaf3kdWAoSJ
idubIWRr2PvbkaQekOfZv3+d+2nTXAvCBRU6lJyx)

Current algorithm (ECDSA-256)

PQC algorithm (Falcon)

SIDN LABS

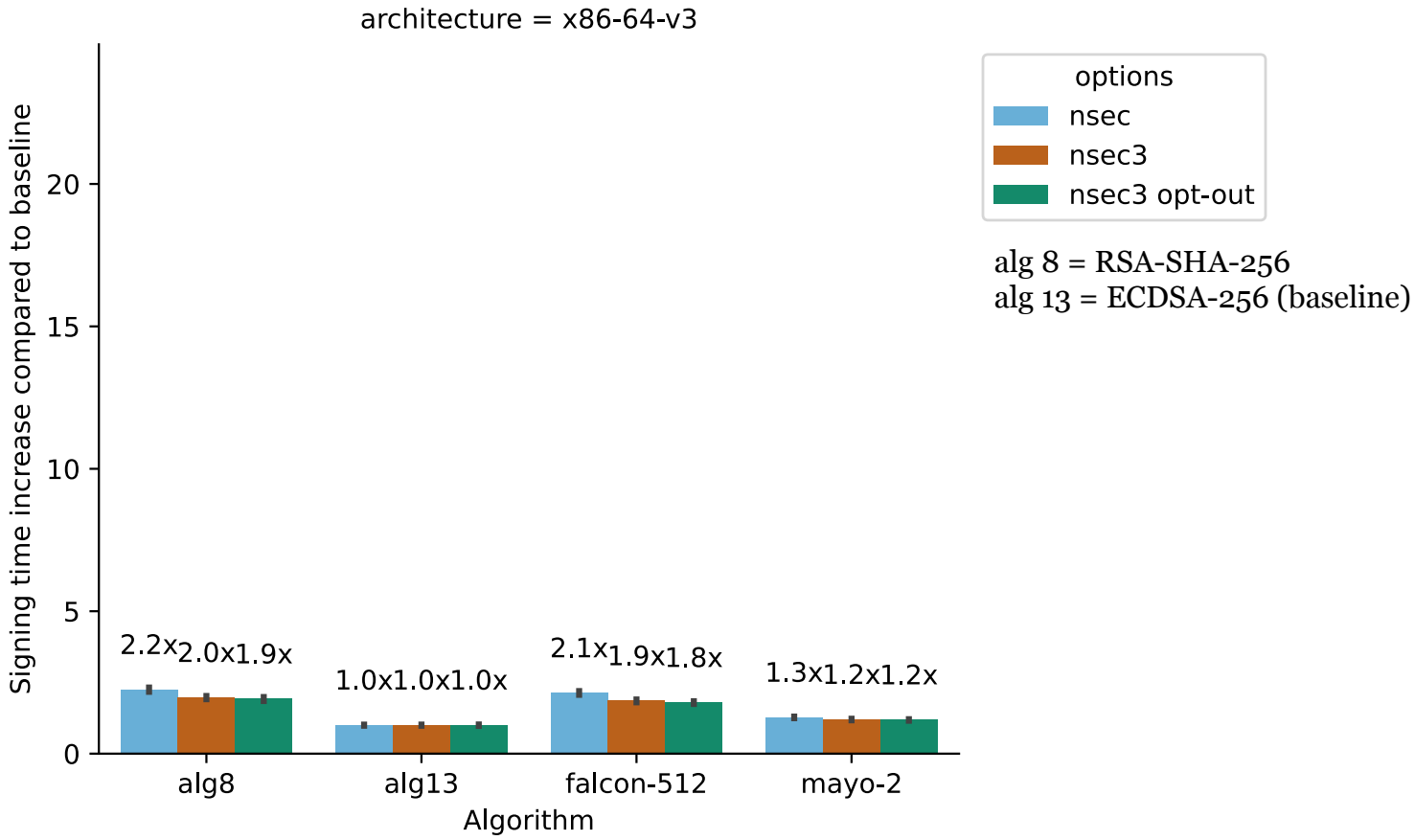
Trade-offs for quantum-safe algoritms

PQC algorithm	ECC (13)	MAYO	Falcon	SQSign
Signature size	😄😄	😄	😡	😄😄
Validation speed	😄	😄	😄	😡😡
Key size	😄😄	😡	😄	😄😄
Signing speed	😄	😄	😄	😡😡

More post-quantum algorithms: https://pqshield.github.io/nist-sigs-zoo

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

First result: signing performance looking good (.nl)



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

Next steps: further explore operational risks

- More state on authoritative name servers because of TCP fallback
- Larger responses during keyrolls
- Resolver validation times with realistic traffic and the role of caching
- Truncated responses not coming through (middleboxes)

Suggested actions for the GAC

- Work with NIST (US government agency) to explore how to align the PQC algorithms coming out of their contest with the DNS' requirements
- Incentivize development of PQC open source software for DNS components via national initiatives, such as via NLnet (NL) or Sovereign Tech Fund (DE)
- Stimulate deployment, perhaps by supporting sites like internet.nl or a future version of security auditing schemes like MANRS+ (routing) to incorporate PQC
- Support research to further assess operational impact of (new) PQC algorithms on the DNS and its operators, such as for the root zone

SIDN LABS

Questions and feedback

https://patad.sidnlabs.nl

Contact person: elmer.lastdrager@sidn.nl

Cristian Hesselman
Director of SIDN Labs
cristian.hesselman@sidn.nl
+31 6 25 07 87 33