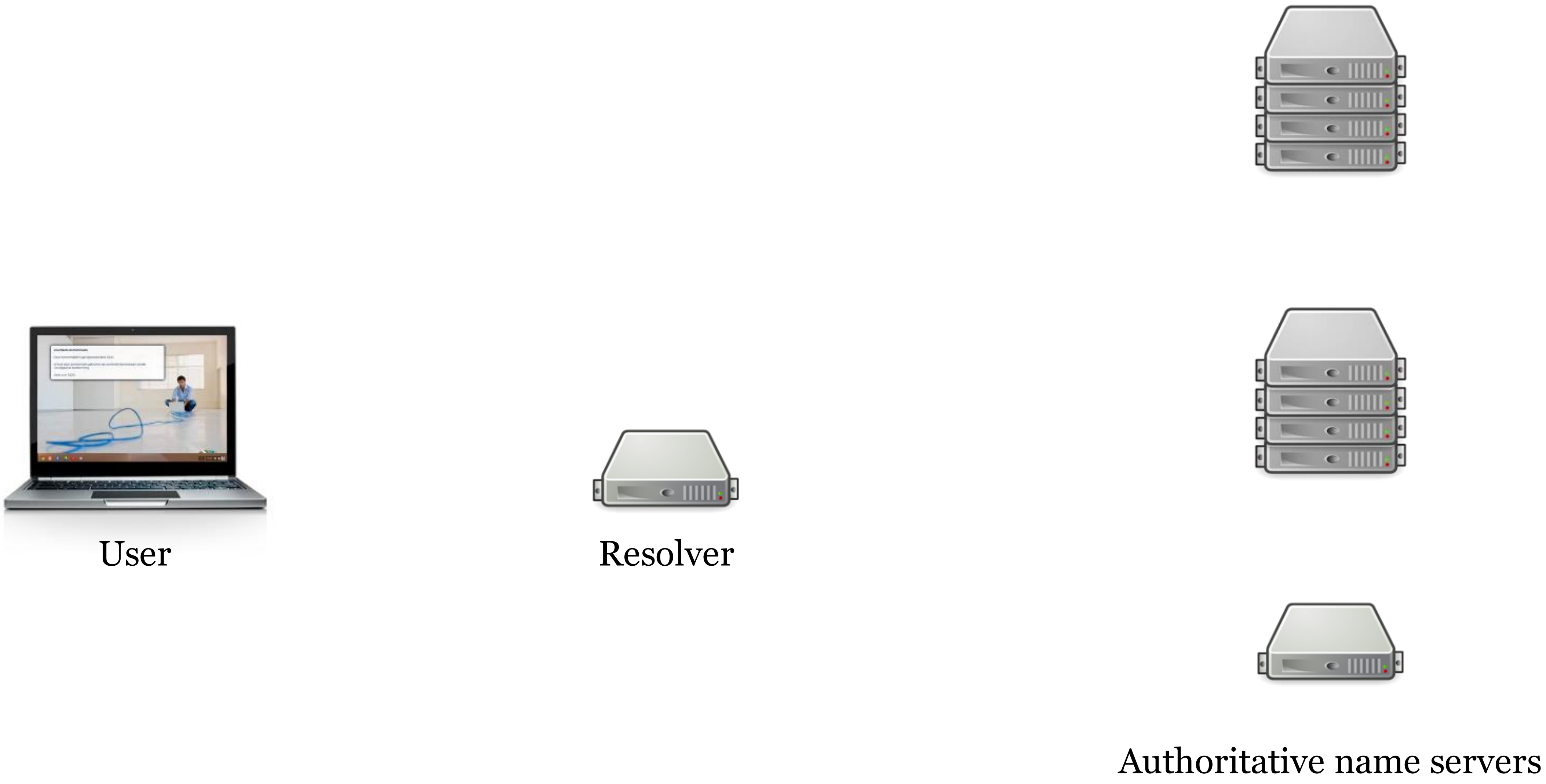
A testbed for evaluating post-quantum algorithms for the DNS

Caspar Schutijser | CENTR R&D (online)
14 February 2024

A testbed for evaluating post-quantum algorithms for the DNS

SIDN LABS



User

Resolver

Authoritative name servers

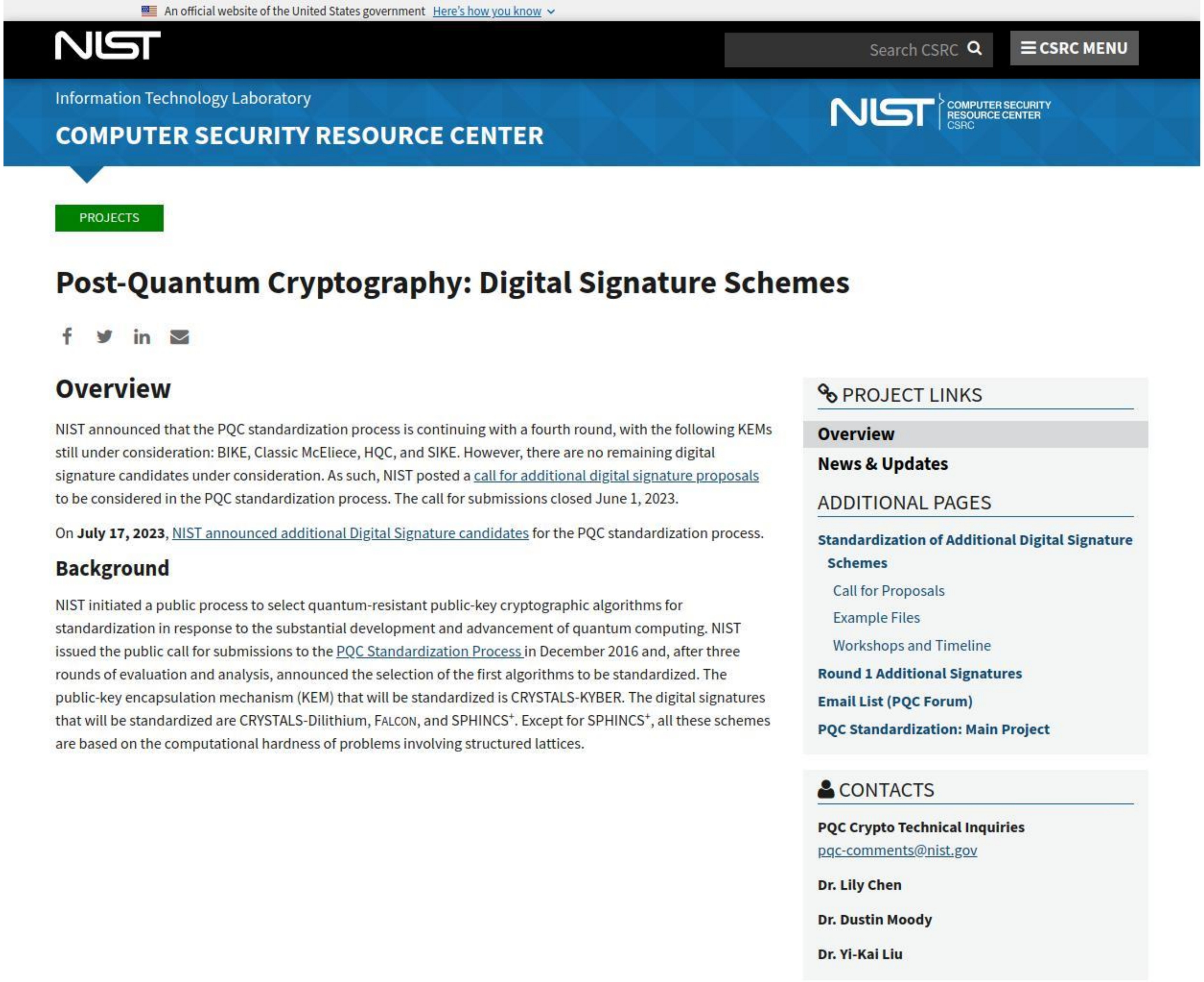
DoH, DoT, DNScrypt
https://dns4all.eu/

X25519Kyber768

DNSSEC

A testbed for evaluating post-quantum algorithms for the DNS

Source: https://www.flickr.com/photos/ibm_research_zurich/51248690716


An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PROJECTS

Post-Quantum Cryptography: Digital Signature Schemes

Overview

NIST announced that the PQC standardization process is continuing with a fourth round, with the following KEMs still under consideration: BIKE, Classic McEliece, HQC, and SIKE. However, there are no remaining digital signature candidates under consideration. As such, NIST posted a call for additional digital signature proposals to be considered in the PQC standardization process. The call for submissions closed June 1, 2023.

On **July 17, 2023**, NIST announced additional Digital Signature candidates for the PQC standardization process.

Background

NIST initiated a public process to select quantum-resistant public-key cryptographic algorithms for standardization in response to the substantial development and advancement of quantum computing. NIST issued the public call for submissions to the PQC Standardization Process in December 2016 and, after three rounds of evaluation and analysis, announced the selection of the first algorithms to be standardized. The public-key encapsulation mechanism (KEM) that will be standardized is CRYSTALS-KYBER. The digital signatures that will be standardized are CRYSTALS-Dilithium, FALCON, and SPHINCS$^+$. Except for SPHINCS$^+$, all these schemes are based on the computational hardness of problems involving structured lattices.

CONTACTS

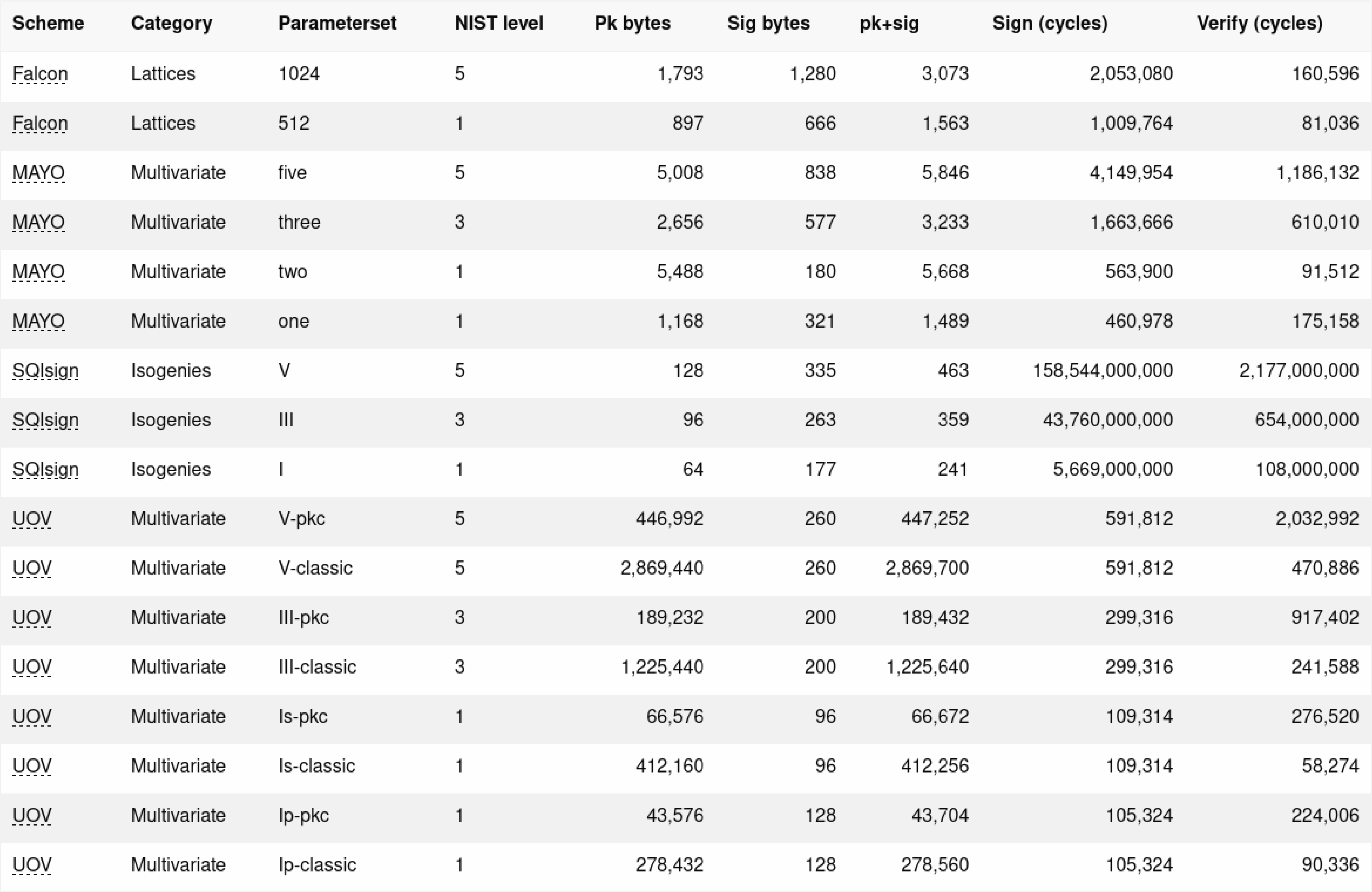
PQC Crypto Technical Inquiries
pqc-comments@nist.gov

Dr. Lily Chen

Dr. Dustin Moody

Dr. Yi-Kai Liu

SDN LABS

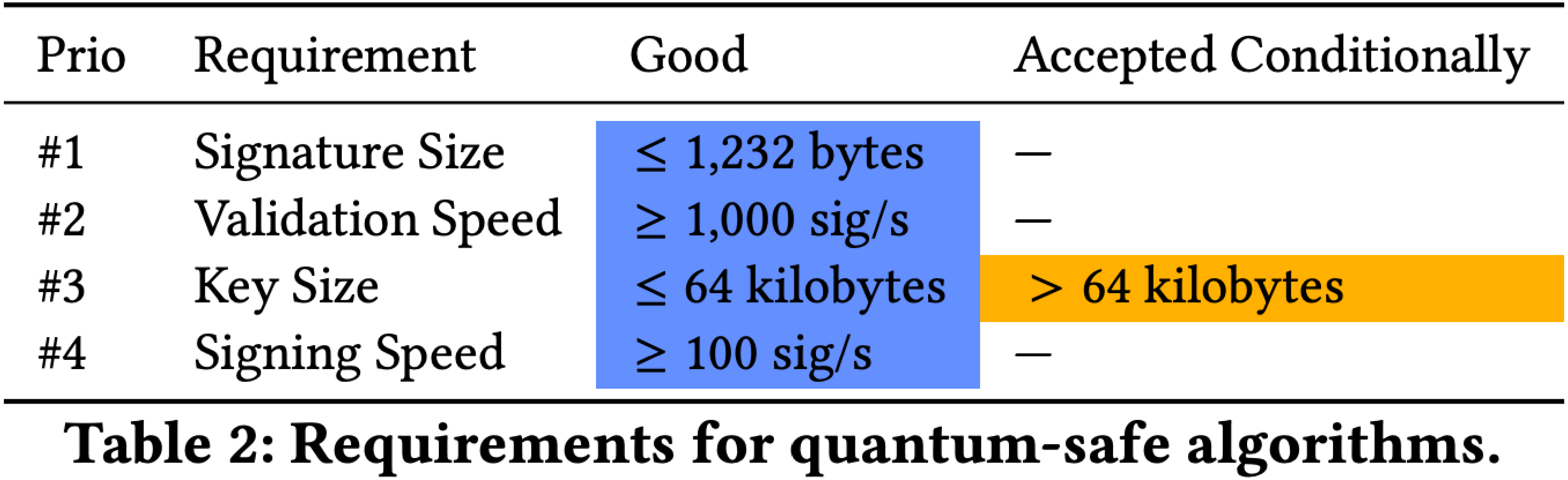


Scheme	Category	Parameterset	NIST level	Pk bytes	Sig bytes	pk+sig	Sign (cycles)	Verify (cycles)
Falcon	Lattices	1024	5	1,793	1,280	3,073	2,053,080	160,596
Falcon	Lattices	512	1	897	666	1,563	1,009,764	81,036
MAYO	Multivariate	five	5	5,008	838	5,846	4,149,954	1,186,132
MAYO	Multivariate	three	3	2,656	577	3,233	1,663,666	610,010
MAYO	Multivariate	two	1	5,488	180	5,668	563,900	91,512
MAYO	Multivariate	one	1	1,168	321	1,489	460,978	175,158
SQIsign	Isogenies	V	5	128	335	463	158,544,000,000	2,177,000,000
SQIsign	Isogenies	III	3	96	263	359	43,760,000,000	654,000,000
SQIsign	Isogenies	I	1	64	177	241	5,669,000,000	108,000,000
UOV	Multivariate	V-pkc	5	446,992	260	447,252	591,812	2,032,992
UOV	Multivariate	V-classic	5	2,869,440	260	2,869,700	591,812	470,886
UOV	Multivariate	III-pkc	3	189,232	200	189,432	299,316	917,402
UOV	Multivariate	III-classic	3	1,225,440	200	1,225,640	299,316	241,588
UOV	Multivariate	Is-pkc	1	66,576	96	66,672	109,314	276,520
UOV	Multivariate	Is-classic	1	412,160	96	412,256	109,314	58,274
UOV	Multivariate	Ip-pkc	1	43,576	128	43,704	105,324	224,006
UOV	Multivariate	Ip-classic	1	278,432	128	278,560	105,324	90,336

https://pqshield.github.io/nist-sigs-zoo/

A testbed
for evaluating
post-quantum algorithms
for the DNS

Requirements



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	—

Table 2: Requirements for quantum-safe algorithms.

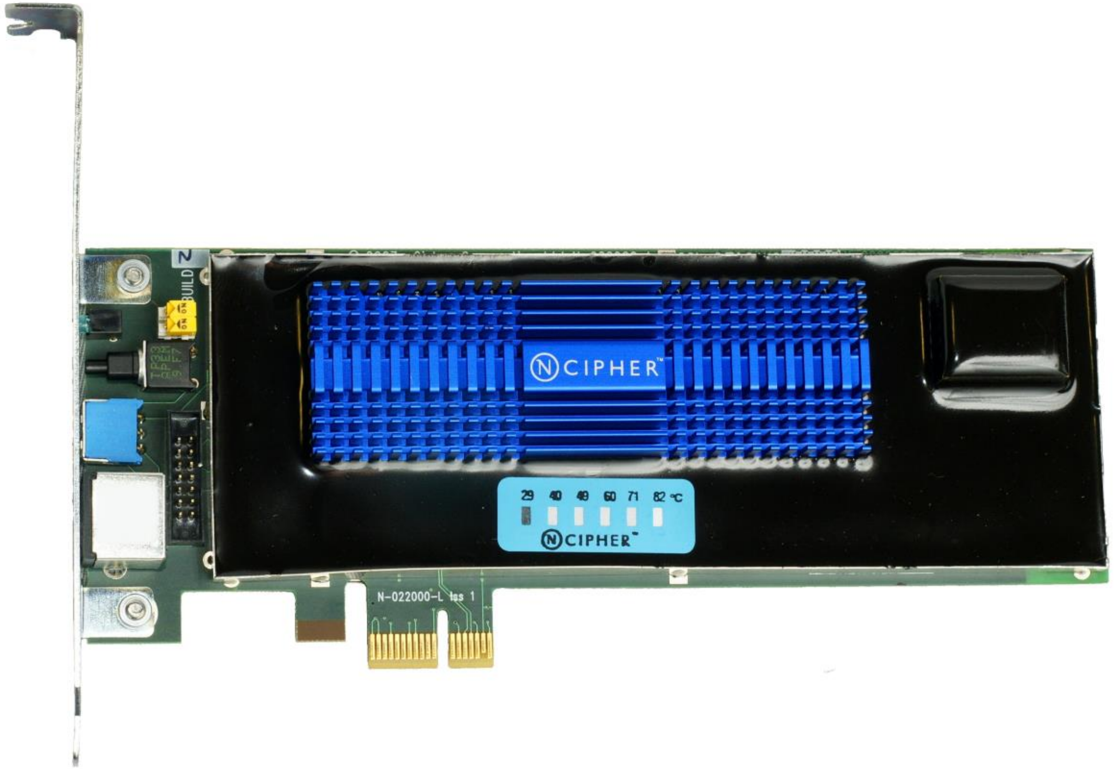
M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

Jürgen Henn – 11foot8.com

CONSOLE
DISK 1
EJECT

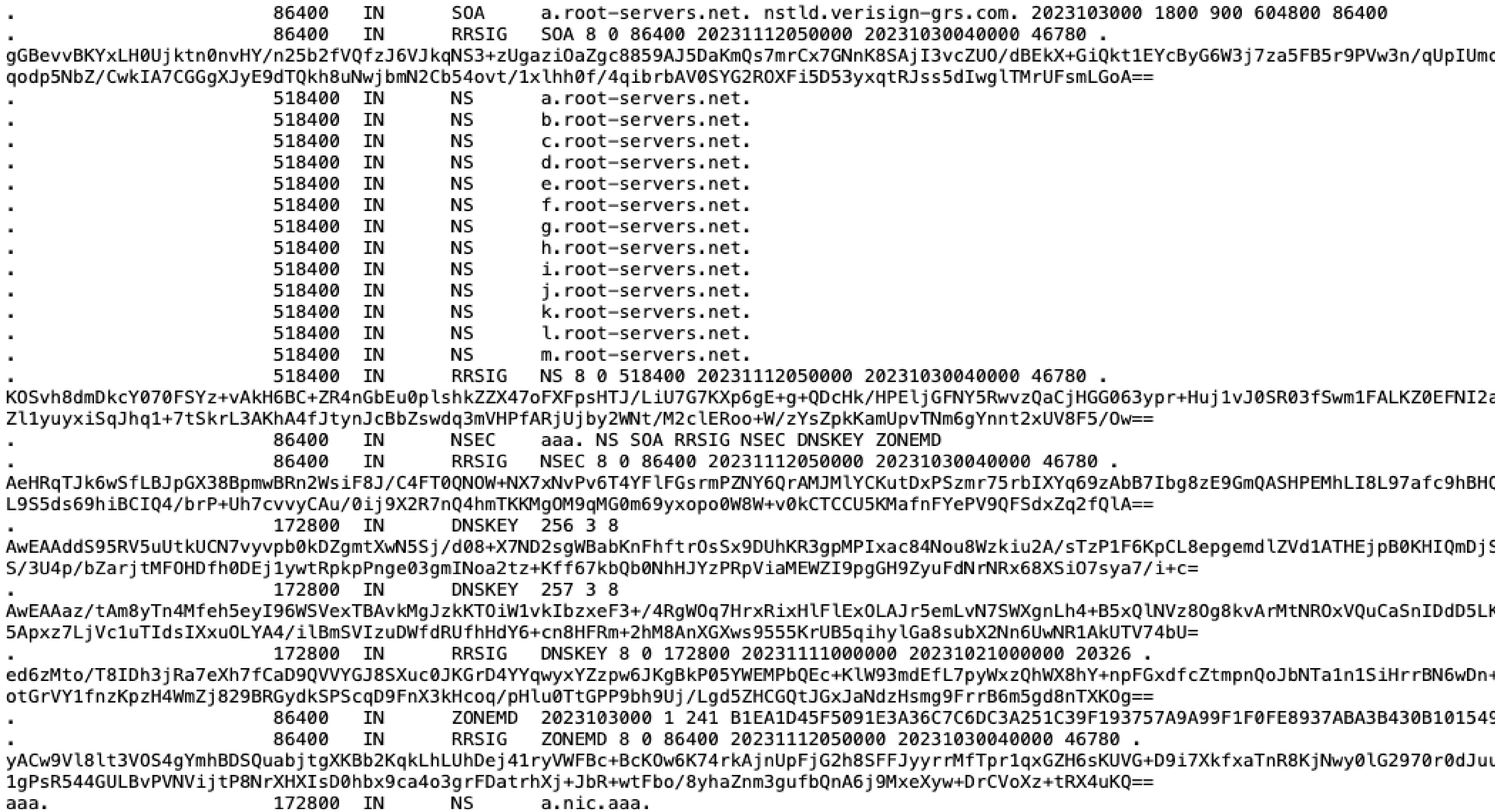
gifbin.com

THALES
THALES


NCIPHER
29 40 49 60 71 82 °C
NCIPHER
N-022000-L Iss 1

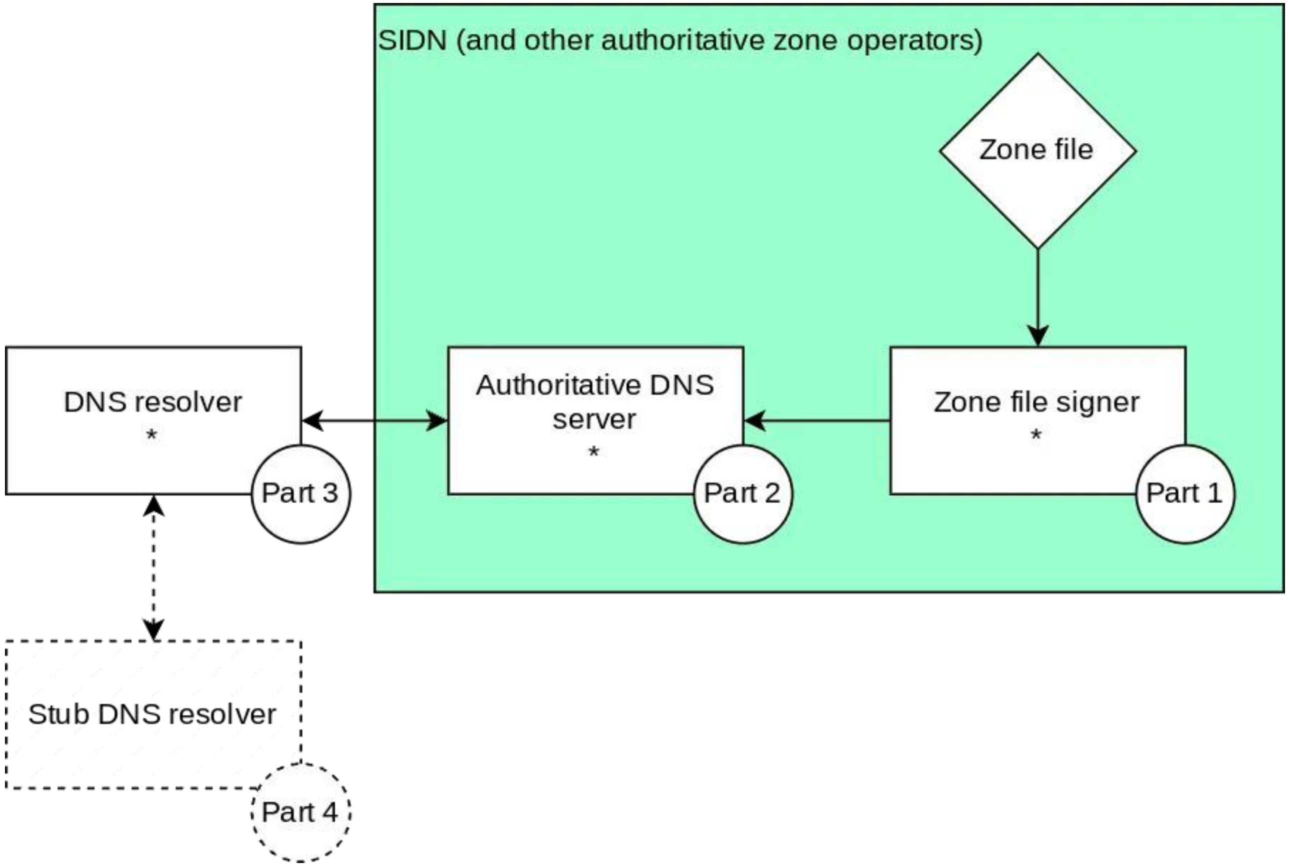
utimaco

A testbed
for evaluating
post-quantum algorithms
for the DNS



```
.                       86400   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023103000 1800 900 604800 86400
.                       86400   IN      RRSIG   SOA 8 0 86400 20231112050000 20231030040000 46780 .
gGBevvBKYxLH0Ujktn0nvHY/n25b2fVQfzJ6VJkqNS3+zUgaziOaZgc8859AJ5DaKmQs7mrCx7GNnK8SAjI3vcZUO/dBEkX+GiQkt1EYcByG6W3j7za5FB5r9PVw3n/qUpIUmo
qodp5NbZ/CwkIA7CGGgXJyE9dTQkh8uNwjbmN2Cb54ovt/1xlhh0f/4qibrbAV0SYG2ROXFi5D53yxqtRJss5dIwglTMrUFsmLGoA==
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      RRSIG   NS 8 0 518400 20231112050000 20231030040000 46780 .
KOSvh8dmDkcY070FSYz+vAkH6BC+ZR4nGbEu0plshkZZX47oFXFpsHTJ/LiU7G7KXp6gE+g+QDcHk/HPEljGFNY5RwvzQaCjHGG063ypr+Huj1vJ0SR03fSwm1FALKZ0EFNI2a
Zl1yuyxiSqJhq1+7tSkrL3AKhA4fJtynJcBbZswdq3mVHPfARjUjby2WNt/M2clERoo+W/zYsZpkKamUpvTNm6gYnnt2xUV8F5/Ow==
.                       86400   IN      NSEC    aaa. NS SOA RRSIG NSEC DNSKEY ZONEMD
.                       86400   IN      RRSIG   NSEC 8 0 86400 20231112050000 20231030040000 46780 .
AeHRqTJk6wSfLBJpGX38BpmwBRn2WsiF8J/C4FT0QNOW+NX7xNvPv6T4YFlFGsrmPZNY6QrAMJMlYCKutDxPSzmr75rbIXYq69zAbB7Ibg8zE9GmQASHPEMhLI8L97afc9hBHQ
L9S5ds69hiBCIQ4/brP+Uh7cvvyCAu/0ij9X2R7nQ4hmTKKMgOM9qMG0m69yxopo0W8W+v0kCTCCU5KMafnFYePV9QFSdxZq2fQlA==
.                       172800  IN      DNSKEY  256 3 8
AwEAAddS95RV5uUtkUCN7vyvpb0kDZgmtXwN5Sj/d08+X7ND2sgWBabKnFhftrOsSx9DUhKR3gpMPIxac84Nou8Wzkiu2A/sTzP1F6KpCL8epgemdlZVd1ATHEjpB0KHIQmDjS
S/3U4p/bZarjtMFOHDfh0DEj1ywtRpkpPnge03gmINoa2tz+Kff67kbQb0NhHJYzPRpViaMEWZI9pgGH9ZyuFdNrNRx68XSiO7sya7/i+c=
.                       172800  IN      DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LK
5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
.                       172800  IN      RRSIG   DNSKEY 8 0 172800 20231111000000 20231021000000 20326 .
ed6zMto/T8IDh3jRa7eXh7fCaD9QVVYGJ8SXuc0JKGrD4YYqwyxYZzpw6JKgBkP05YWEMPbQEc+KlW93mdEfL7pyWxzQhWX8hY+npFGxdfcZtmpnQoJbNTa1n1SiHrrBN6wDn+
otGrVY1fnzKpzH4WmZj829BRGydkSPScqD9FnX3kHcoq/pHlu0TtGPP9bh9Uj/Lgd5ZHCGQtJGxJaNdzHsmg9FrrB6m5gd8nTXKOg==
.                       86400   IN      ZONEMD  2023103000 1 241 B1EA1D45F5091E3A36C7C6DC3A251C39F193757A9A99F1F0FE8937ABA3B430B101549
.                       86400   IN      RRSIG   ZONEMD 8 0 86400 20231112050000 20231030040000 46780 .
yACw9Vl8lt3VOS4gYmhBDSQuabjtgXKBb2KqkLhLUhDej41ryVWFBc+BcKOw6K74rkAjnUpFjG2h8SFFJyyrrMfTpr1qxGZH6sKUVG+D9i7XkfxaTnR8KjNwy0lG2970r0dJuu
1gPsR544GULBvPVNVijtP8NrXHXIsD0hbx9ca4o3grFDatrhXj+JbR+wtFbo/8yhaZnm3gufbQnA6j9MxeXyw+DrCVoXz+tRX4uKQ==
aaa.                    172800  IN      NS      a.nic.aaa.
```

TAKE
AWAY
1
ZURICH



https://www.sidnlabs.nl/en/news-and-blogs/a-quantum-safe-cryptography-dnssec-testbed

What do you think it will take to deploy PQC DNSSEC in your organisation?

Thank you for your attention!

Caspar Schutijser
caspar.schutijser@sidn.nl

https://mstdn.social/@SIDNlabs

https://www.sidnlabs.nl/en