DNS Quantum Computing

Ulrich Wisser
Technical Engagement Manager, Europe

15th October 2024

ICANN

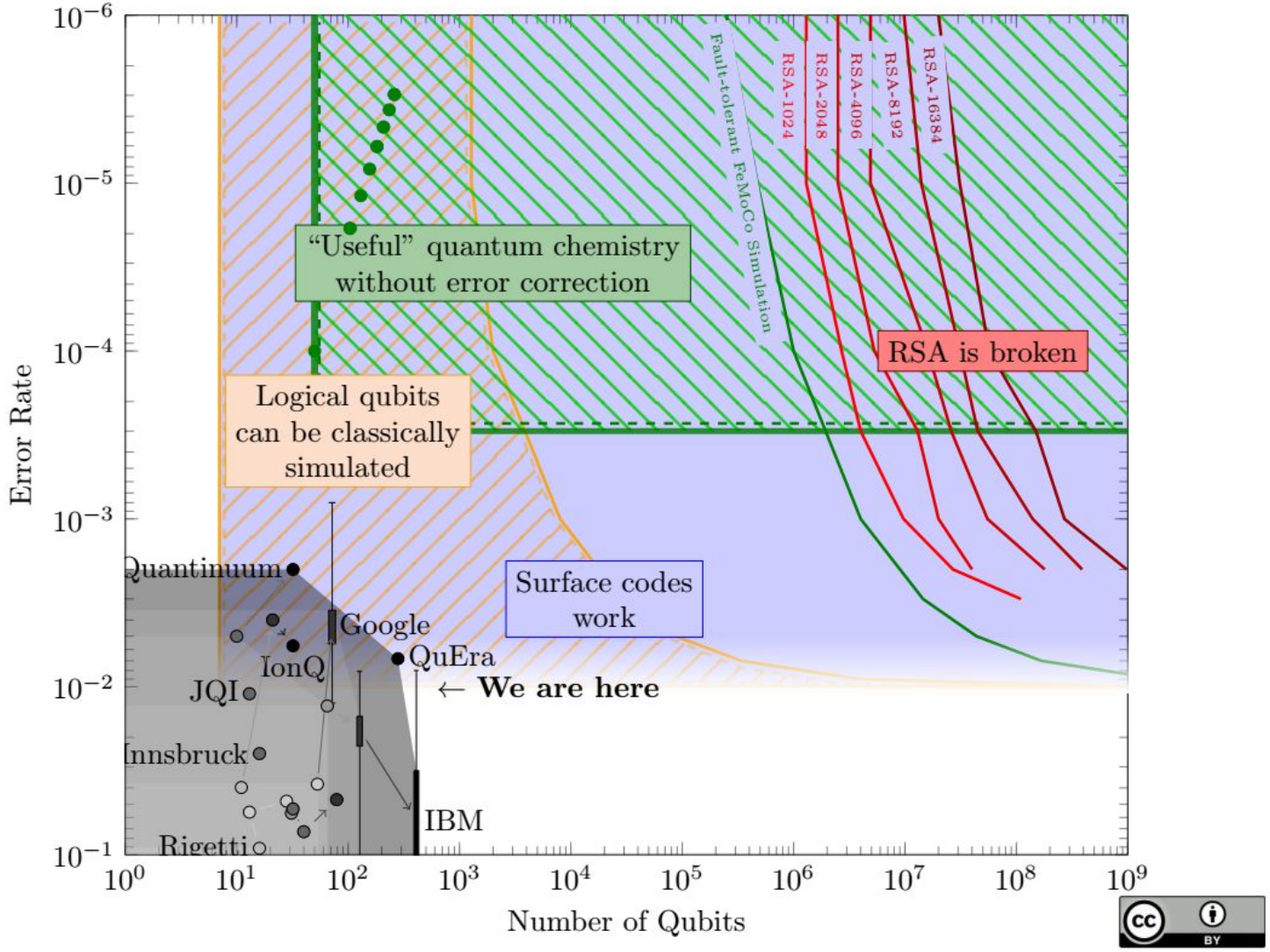
First, the disclaimer:

"If you think you understand quantum mechanics, you don't understand quantum mechanics."

Prof. Richard Feynman (Nobel physicist)

DNS Quantum Computing

CRQC



CC: Samuel Jaques, UNIVERSITY OF WATERLOO, https://sam-jaques.appspot.com/quantum_landscape_2023

Crypto Agility

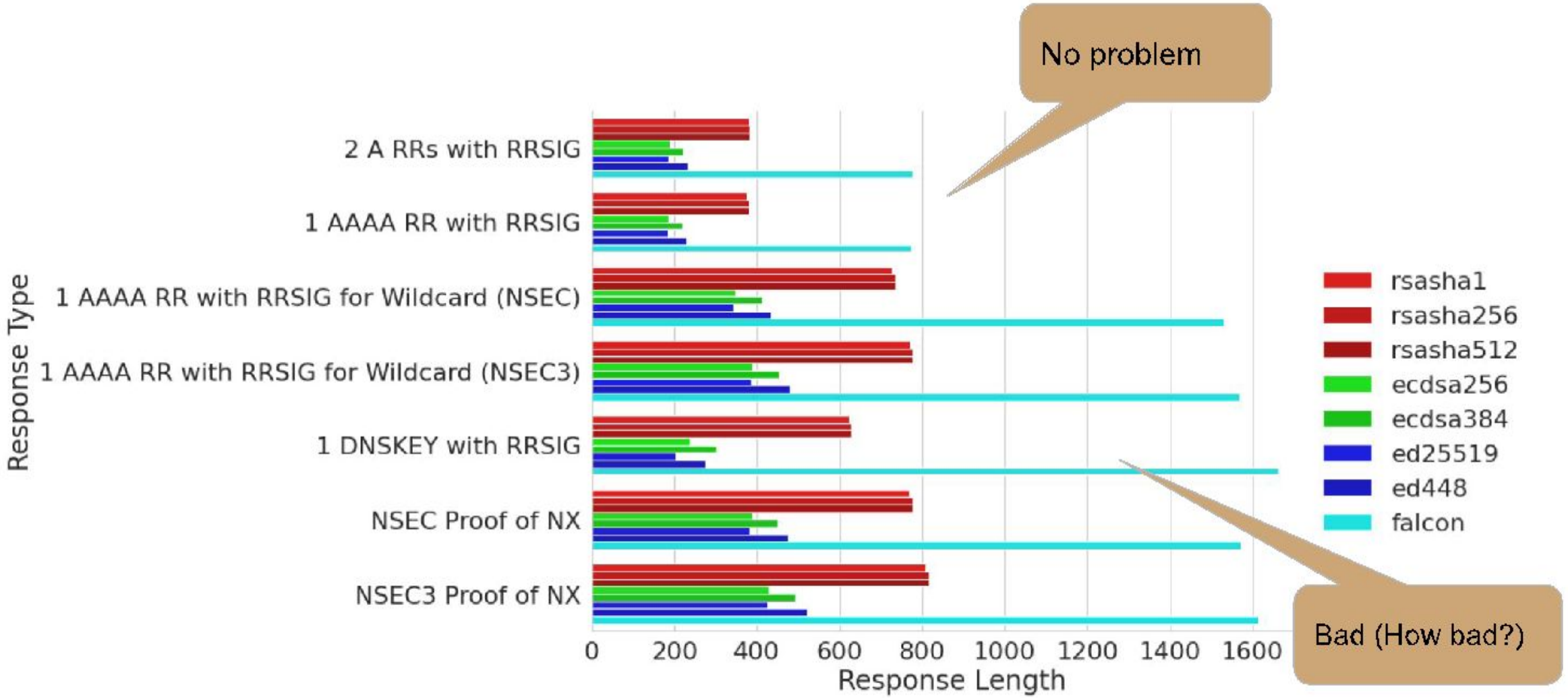
DNSSEC

Signature Sizes

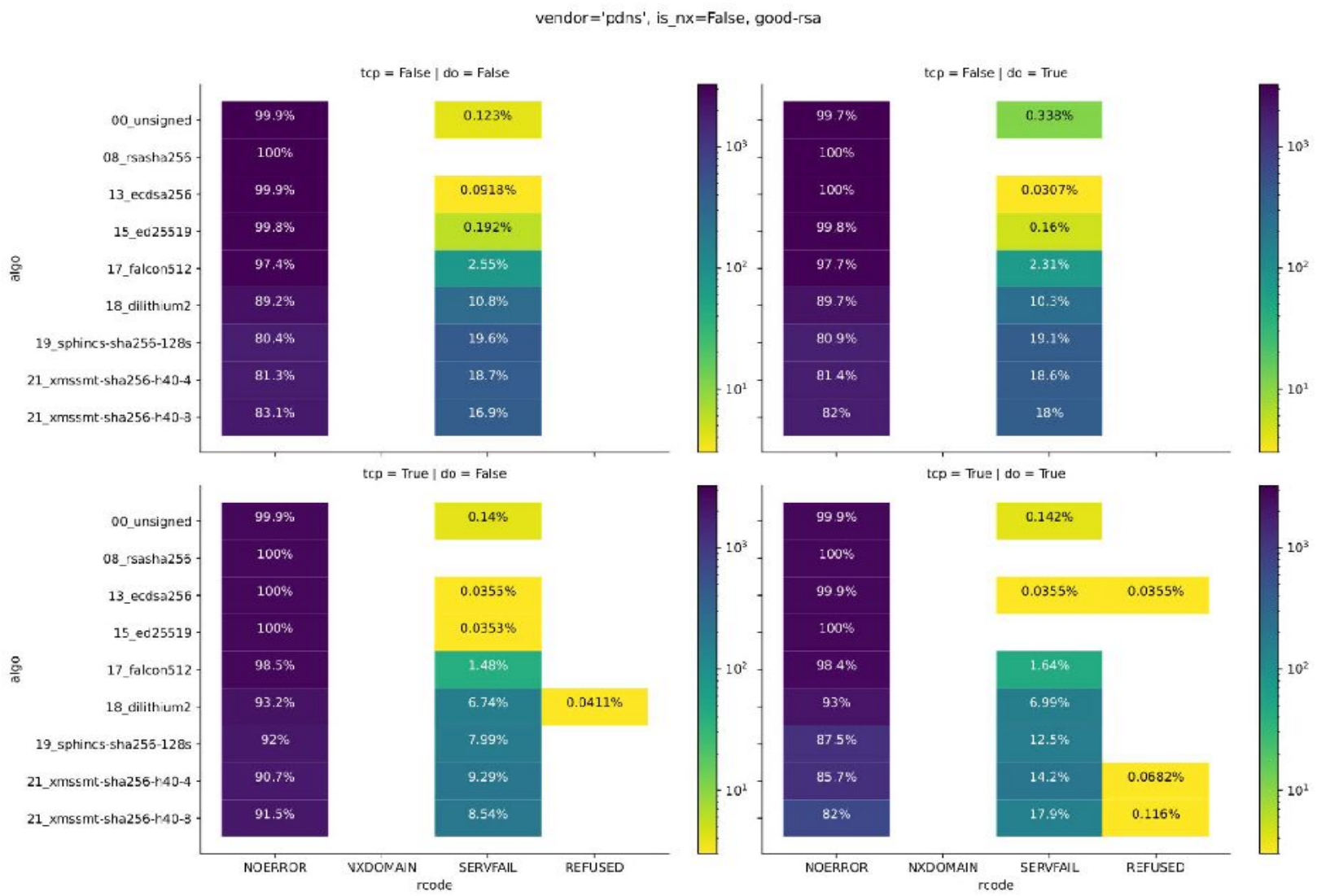
	Public key	Private key	Signature
Crystals Dilithium 2	1312	2528	2420
Crystals Dilithium 3	1,952	4000	3293
Crystals Dilithium 5	2,592	4864	4595
Falcon 512	897	1281	690
Falcon 1024	1,793	2305	1330
Sphincs SHA256-128f	32	64	17088
Sphincs SHA256-192f	48	96	35664
Sphincs SHA256-256f	64	128	49856
ECDSA-P256			64
RSA-SHA256 2048			256

Algorithm	NIST Verdict	Approach	Private key	Public key	Signature	Sign/s	Verify/s
Crystals-Dilithium-II [29]	Finalist	Lattice	2.8kB	1.2kB	2.0kB		
Falcon-512 [31]	Finalist	Lattice	57kB	0.9kB	0.7kB	3,307	20,228
Rainbow-I_a [56]	Finalist	Multivariate	101kB	158kB	66B	8,332	11,065
RedGeMSS128 [16]	Candidate	Multivariate	16B	375kB	35B	545	10,365
Sphincs$^+$-Haraka-128s [11]	Candidate	Hash	64B	32B	8kB		
Picnic-L1-FS [17]	Candidate	Hash	16B	32B	34kB		
Picnic2-L1-FS [17]	Candidate	Hash	16B	32B	14kB		
EdDSA-Ed22519 [12]		Elliptic curve	64B	32B	64B	25,935	7,954
ECDSA-P256 [12]		Elliptic curve	96B	64B	64B	40,509	13,078
RSA-2048 [12]		Prime	2kB	0.3kB	0.3kB	1,485	49,367

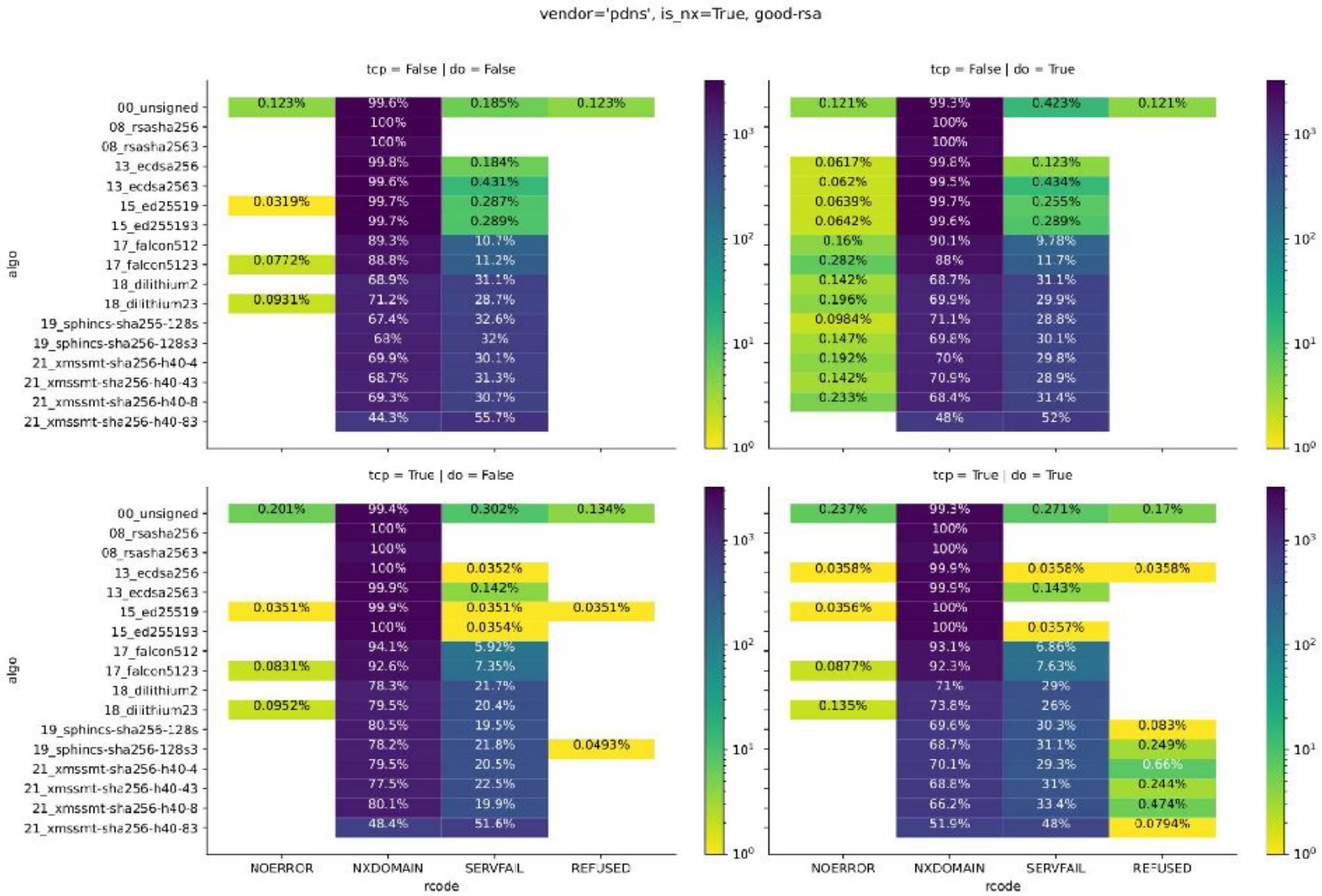
Packet Sizes



Run Time


vendor='pdns', is_nx=False, good-rsa
tcp = False | do = False
tcp = False | do = True
tcp = True | do = False
tcp = True | do = True
algo
00_unsigned
08_rsasha256
13_ecdsa256
15_ed25519
17_falcon512
18_dilithium2
19_sphincs-sha256-128s
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-8
99.9%
100%
99.9%
99.8%
97.4%
89.2%
80.4%
81.3%
83.1%
0.123%
0.0918%
0.192%
2.55%
10.8%
19.6%
18.7%
16.9%
99.7%
100%
100%
99.8%
97.7%
89.7%
80.9%
81.4%
82%
0.338%
0.0307%
0.16%
2.31%
10.3%
19.1%
18.6%
18%
99.9%
100%
100%
100%
98.5%
93.2%
92%
90.7%
91.5%
0.14%
0.0355%
0.0353%
1.48%
6.74%
7.99%
9.29%
8.54%
0.0411%
99.9%
100%
99.9%
100%
98.4%
93%
87.5%
85.7%
82%
0.142%
0.0355%
0.0355%
1.64%
6.99%
12.5%
14.2%
17.9%
0.0682%
0.116%
10^3
10^2
10^1
NOERROR
NXDOMAIN
SERVFAIL
REFUSED
rcode

Run Time


vendor='pdns', is_nx=True, good-rsa
tcp = False | do = False
tcp = False | do = True
tcp = True | do = False
tcp = True | do = True
algo
00_unsigned
08_rsasha256
08_rsasha2563
13_ecdsa256
13_ecdsa2563
15_ed25519
15_ed255193
17_falcon512
17_falcon5123
18_dilithium2
18_dilithium23
19_sphincs-sha255-128s
19_sphincs-sha256-128s3
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-43
21_xmssmt-sha256-h40-8
21_xmssmt-sha256-h40-83
NOERROR
NXDOMAIN
SERVFAIL
REFUSED
rcode

The DNSSEC Community Does Not Need to Consider Post-Quantum Cryptography at This Time

DNS Protocols That Also Use TLS or QUIC Should Update to Post-Quantum Cryptography in Alignment with Web Protocols

Further Reading

- ICANN OCTO-031v2 Quantum Computing and the DNS https://www.icann.org/en/system/files/files/octo-031-22apr24-en.pdf
- ICANN SSAC workshop https://www.icann.org/en/blogs/details/security-and-stability-advisory-committee-

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann