Field Experiments on Post-Quantum DNSSEC

Jason Goertzen <jason.goertzen@sandboxaq.com>
Peter Thomassen <peter@desec.io>
Nils Wisiol <nils@desec.io>

ICANN 80 – DNSSEC and Security Workshop – June 10, 2024

Motivation

- Shor's Algorithm breaks all today's DNSSEC signature schemes
  - Problem: Suitable quantum computer could be available in the future
  - Less pressing than in TLS case (which protects private contents)
  - DoH/DoT/DoQ don't solve this (does not provide data origin authentication)

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

ICANN OCTO-031v2: Quantum Computing and the DNS

→ Low urgency, but important to **be prepared**

Let's Give it a Try

- … actually, already did in 2022
- **Requirements:**
  - fast validation
  - short signatures
  - short-ish keys

  → **Falcon**
- **Internal study** only
  - Local benchmarks (e.g., keygen time)
  - Local DNS transactions (e.g., DNS resolution in Docker network)
  - Implemented/conducted with PowerDNS (credits: N. Wisiol, deSEC; M. Grillere, TU Berlin)
- Results: https://blog.powerdns.com/2022/04/07/falcon-512-in-powerdns

Mission

- Broader experiments with **multiple PQC algorithms**
- Create **public deployment** on the Internet, from “real” clients
- Goals:
  - Investigate behavior of non-PQC-aware resolvers typically used by clients
  - Investigate behavior of PQC-aware resolvers
- Implemented **both signing and validation**, for both **BIND9** and **PowerDNS**
- Additional test parameters:
  - Name existence and NSEC vs. NSEC3
  - UDP vs. TCP
  - DO bit

Algorithm Considerations

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

Müller, M. et al.: Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. SIGCOMM Comput. Commun. Rev. 50, 49–57 (2020)

- Selected algorithms with public keys and signatures < 10 KB
- Plus: a stateful hash-based algorithm (XMSS)

Steps Taken

- Facilitated by NLnet Foundation and collaboration with Sandbox AQ
- Implemented via liboqs
  - Falcon512
  - Dilithium2
  - Sphincs-SHA256-128s
  - XMSSmt-SHA256-h40-4 / XMSSmt-SHA256-h40-8

    … using standard algorithm numbers
- Sanity checks with both unsigned, and algorithms 8, 13, 15
- Used **RIPE ATLAS** for broad experiment (~10,000 probes, ~2M queries)
  - Measurements conducted in May 2024

deSEC

Queries Using an Unaware Resolver

```
dig +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @8.8.8.8
```

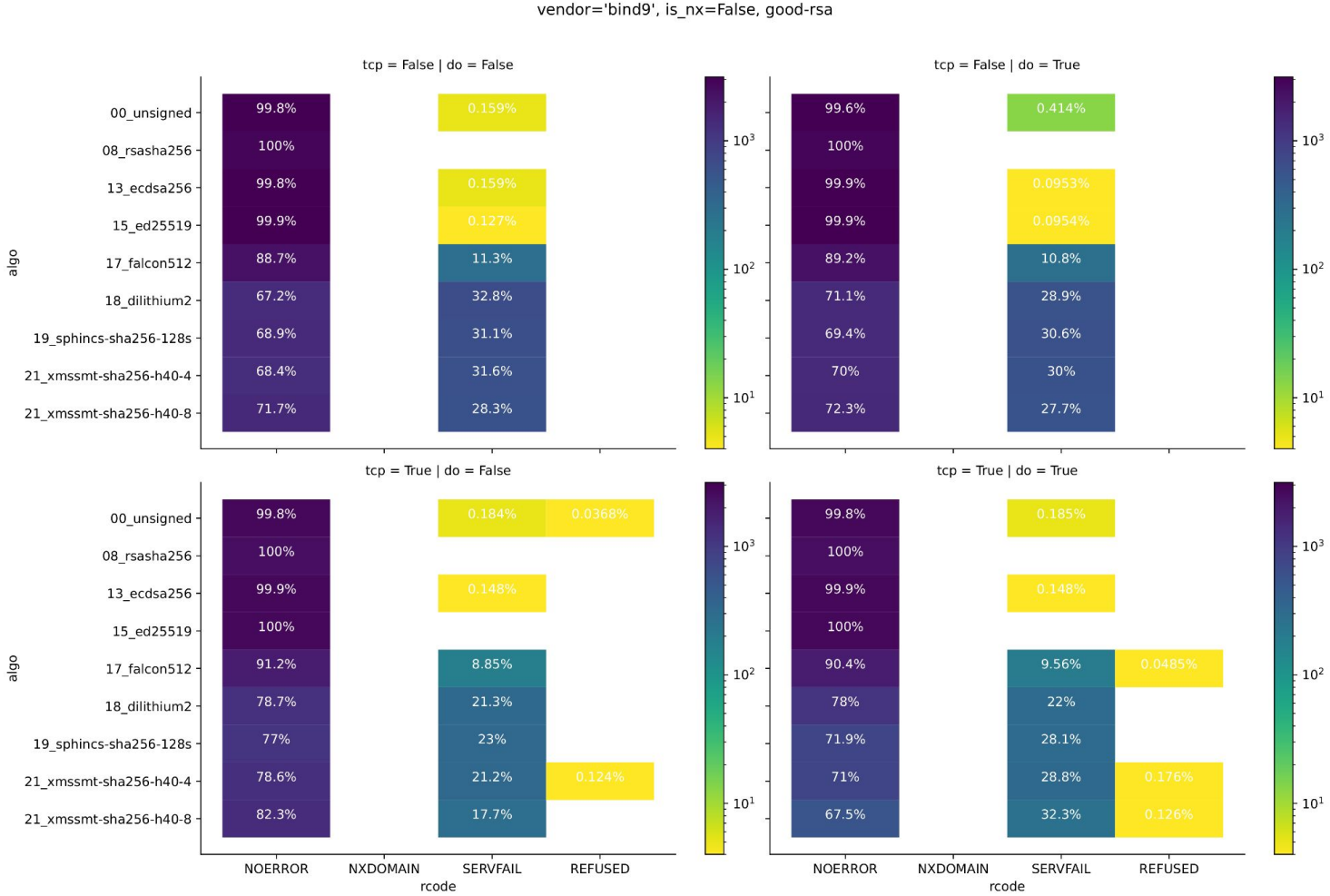
```
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> A +dnssec dilithium2.pdns.pq-dnssec.dedyn.io @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38356
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;dilithium2.pdns.pq-dnssec.dedyn.io. IN A

;; ANSWER SECTION:
dilithium2.pdns.pq-dnssec.dedyn.io. 3600 IN A  95.217.209.184
dilithium2.pdns.pq-dnssec.dedyn.io. 3600 IN RRSIG A 18 5 3600 20240620000000 20240530000000 9247
dilithium2.pdns.pq-dnssec.dedyn.io. 4GiLZuz4ouEsR+bAsCW6hbo/PYKaa3FwPZbFXtWxrX4oZBgYBqc6nb/9
DqE6azh7Pi91r2pmHjb4Lj4l7vFJxMpgEXTRfkqFtZbXnNQl6vKsDW/+ PINJIPSAGTya9Utk2oI37b+K8ItfHwH/C7WOUX6sxFuofvhd1v+eeKs7
C+pRgrtwT9/s/Whsg7IbhFbyDt8n3MKOTeb8oRKtdwTnuabF7s3Ss5vI [...shortened...]qe qa632uPyAAAAAAAAAAAAAAAAAAAAAAAABAiLUA=

;; Query time: 208 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Fri Jun 07 23:09:02 CEST 2024
;; MSG SIZE  rcvd: 2565
```

Results Analysis: Pre-Selection

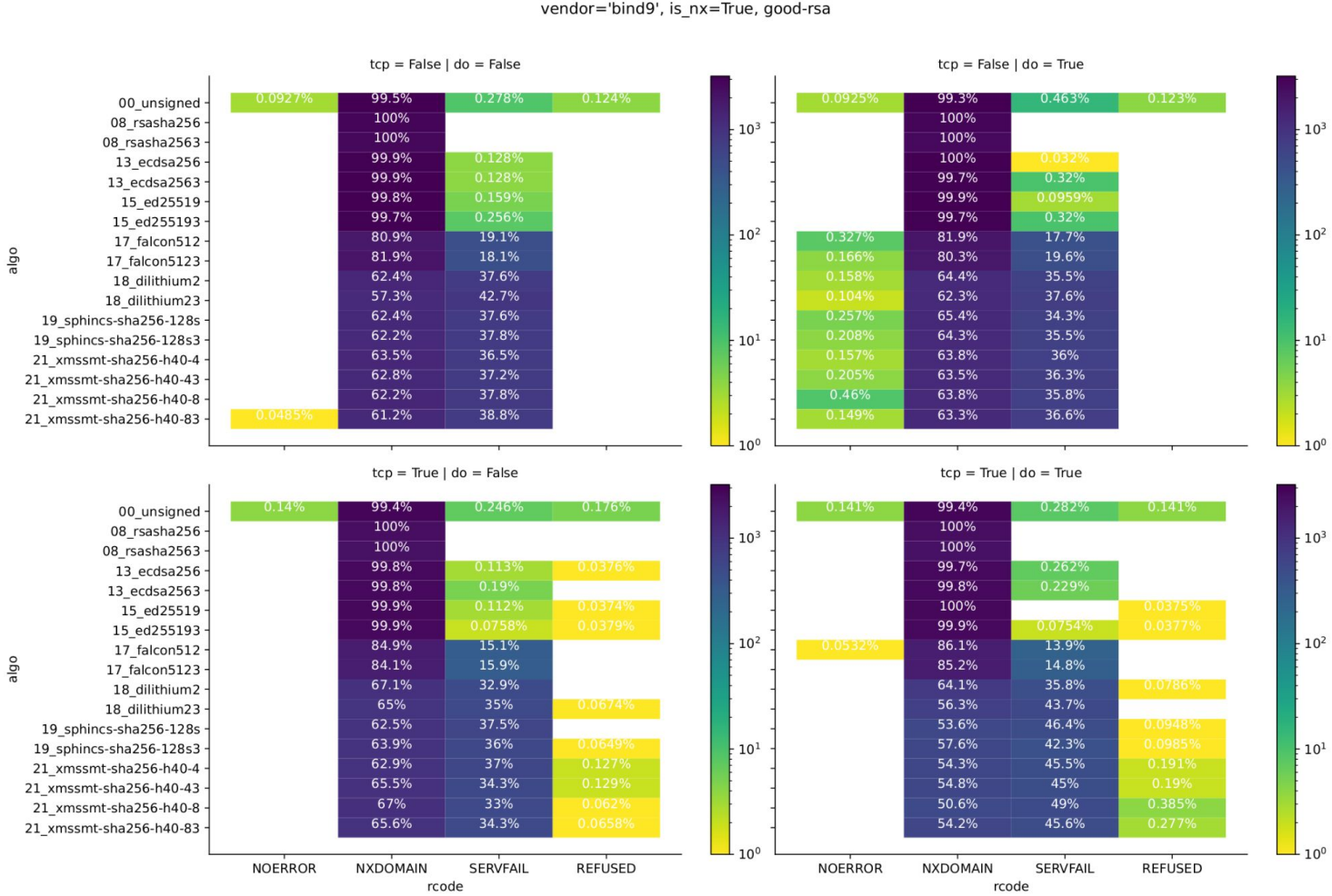
- Public resolver targets (/etc/resolv.conf)
  - For consistency (RIPE ATLAS enforces for TCP)
- Good algorithm 8 response (correct answer or NXDOMAIN, as applicable)
- BIND only
- Received answers only
  - Have not yet discerned frequency of timeouts and other errors

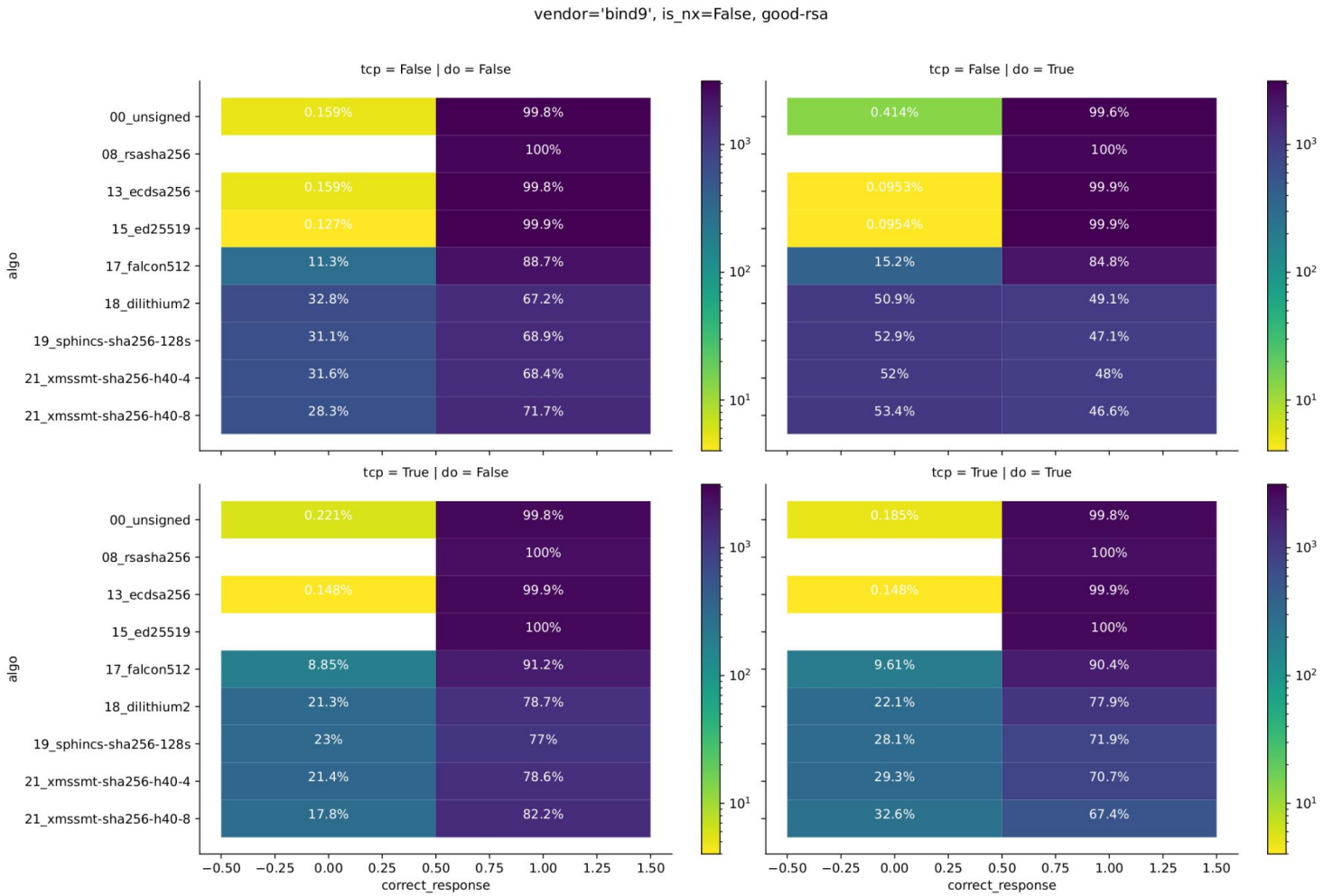
- Still evaluating other cases
  - PowerDNS
  - requiring only good unsigned response
  - …

deSEC

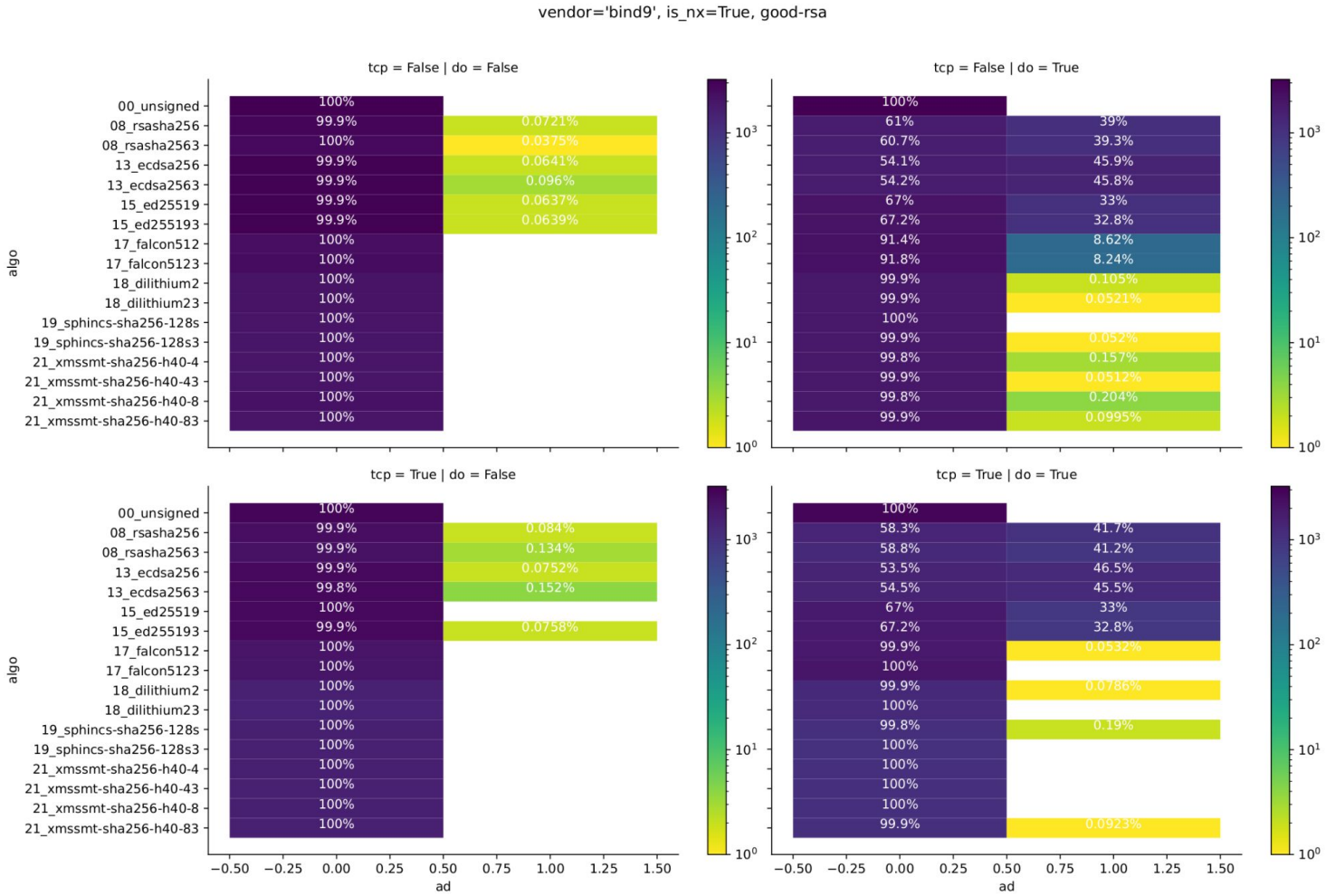

vendor='bind9', is_nx=False, good-rsa
tcp = False | do = False
tcp = False | do = True
tcp = True | do = False
tcp = True | do = True
algo
00_unsigned
08_rsasha256
13_ecdsa256
15_ed25519
17_falcon512
18_dilithium2
19_sphincs-sha256-128s
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-8
99.8%
0.159%
100%
99.8%
0.159%
99.9%
0.127%
88.7%
11.3%
67.2%
32.8%
68.9%
31.1%
68.4%
31.6%
71.7%
28.3%
99.6%
0.414%
100%
99.9%
0.0953%
99.9%
0.0954%
89.2%
10.8%
71.1%
28.9%
69.4%
30.6%
70%
30%
72.3%
27.7%
0.184%
0.0368%
0.148%
91.2%
8.85%
78.7%
21.3%
77%
23%
78.6%
21.2%
0.124%
82.3%
17.7%
0.185%
0.148%
90.4%
9.56%
0.0485%
78%
22%
71.9%
28.1%
71%
28.8%
0.176%
67.5%
32.3%
0.126%
10^3
10^2
10^1
NOERROR
NXDOMAIN
SERVFAIL
REFUSED
rcode

deSEC

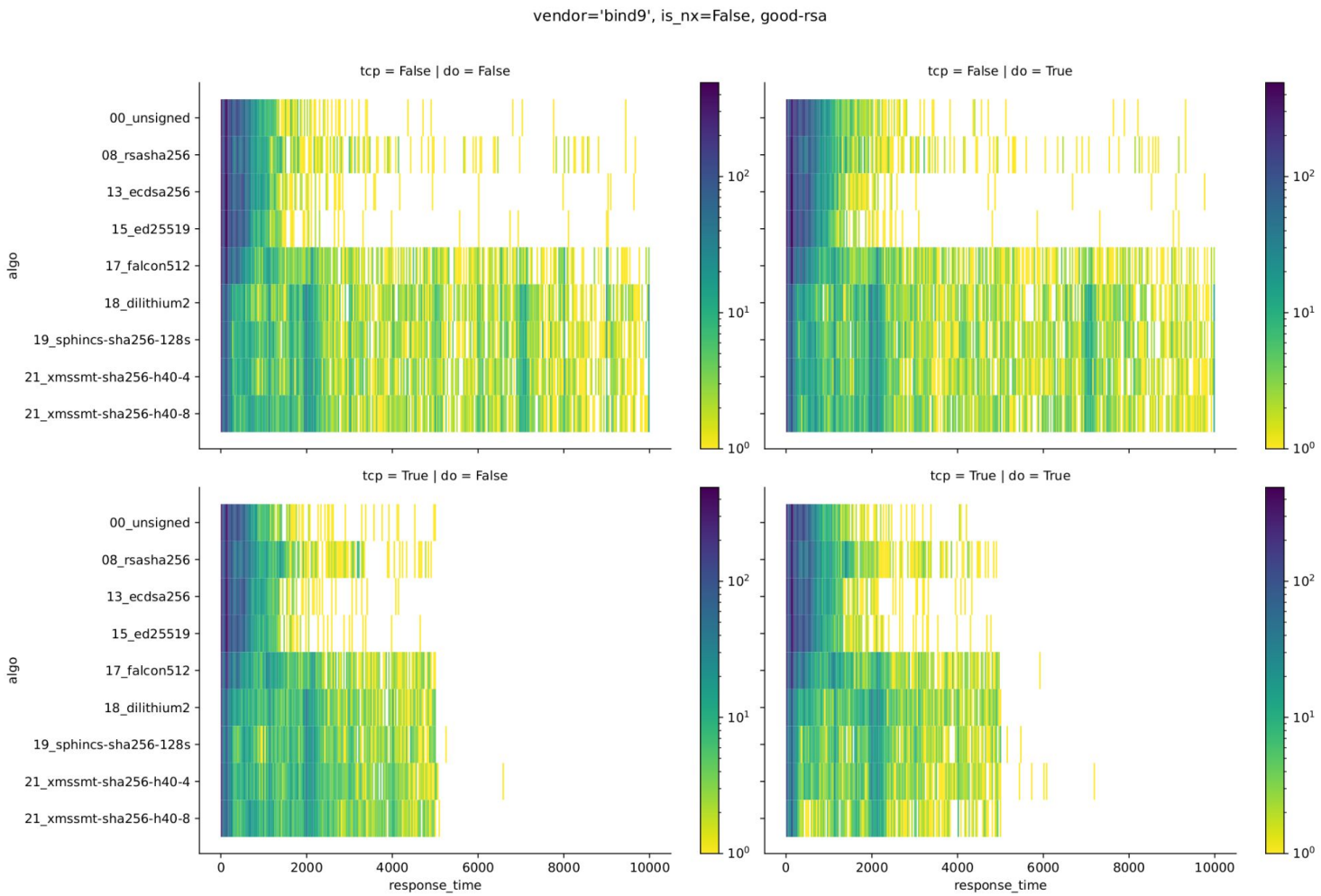

vendor='bind9', is_nx=True, good-rsa
tcp = False | do = False
tcp = False | do = True
tcp = True | do = False
tcp = True | do = True
algo
00_unsigned
08_rsasha256
08_rsasha2563
13_ecdsa256
13_ecdsa2563
15_ed25519
15_ed255193
17_falcon512
17_falcon5123
18_dilithium2
18_dilithium23
19_sphincs-sha256-128s
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


vendor='bind9', 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
0.159%
99.8%
100%
0.159%
99.8%
0.127%
99.9%
11.3%
88.7%
32.8%
67.2%
31.1%
68.9%
31.6%
68.4%
28.3%
71.7%
0.414%
99.6%
100%
0.0953%
99.9%
0.0954%
99.9%
15.2%
84.8%
50.9%
49.1%
52.9%
47.1%
52%
48%
53.4%
46.6%
0.221%
99.8%
100%
0.148%
99.9%
100%
8.85%
91.2%
21.3%
78.7%
23%
77%
21.4%
78.6%
17.8%
82.2%
0.185%
99.8%
100%
0.148%
99.9%
100%
9.61%
90.4%
22.1%
77.9%
28.1%
71.9%
29.3%
70.7%
32.6%
67.4%
10^3
10^2
10^1
−0.50 −0.25 0.00 0.25 0.50 0.75 1.00 1.25 1.50
correct_response

deSEC


vendor='bind9', 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-sha256-128s
19_sphincs-sha256-128s3
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-43
21_xmssmt-sha256-h40-8
21_xmssmt-sha256-h40-83
ad
−0.50 −0.25 0.00 0.25 0.50 0.75 1.00 1.25 1.50
10^3
10^2
10^1
10^0

deSEC


vendor='bind9', 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
0
2000
4000
6000
8000
10000
response_time
10^0
10^1
10^2

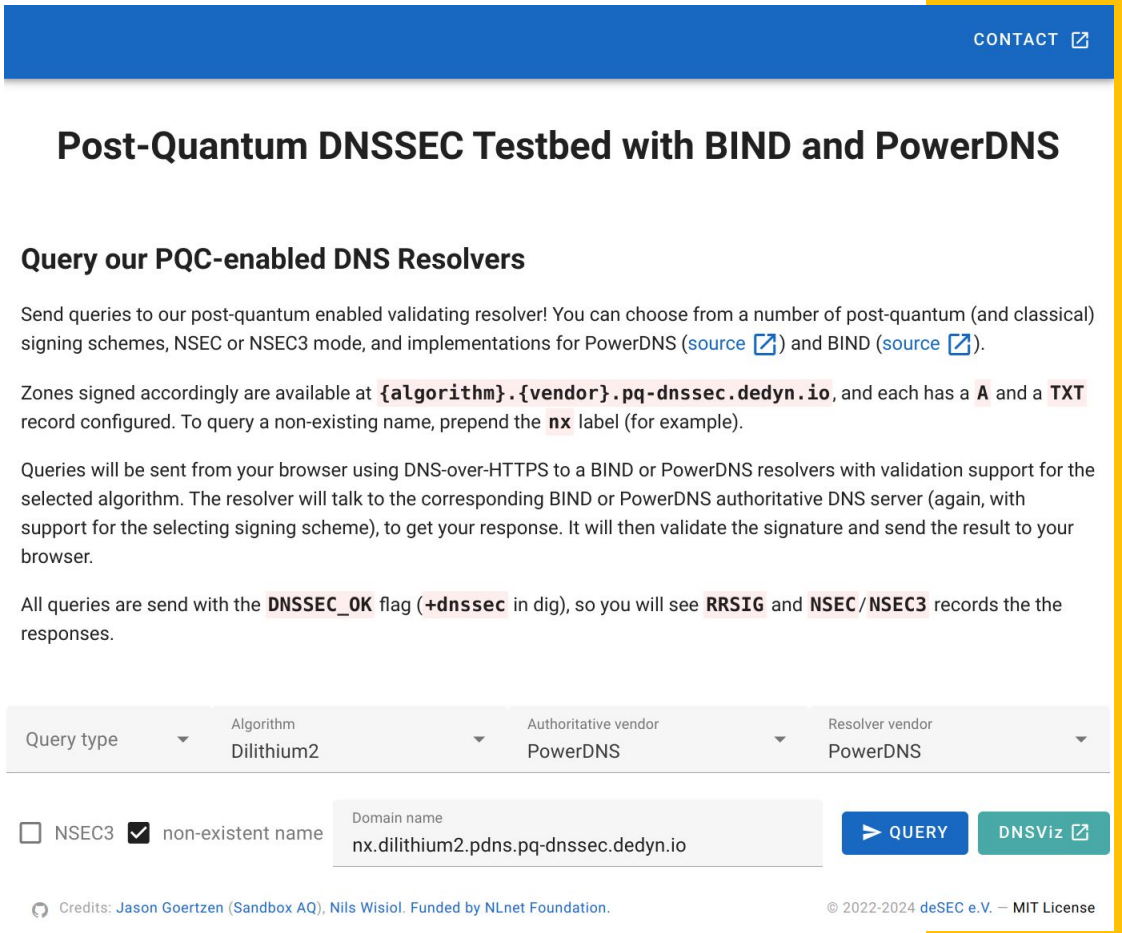
deSEC

Queries Using a PQC-aware Resolver

```
dig +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @pdns.pq-dnssec.dedyn.io -p 5302
```

```
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @pdns.pq-dnssec.dedyn.io -p 5302
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4342
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;dilithium2.pdns.pq-dnssec.dedyn.io. IN A

;; ANSWER SECTION:
dilithium2.pdns.pq-dnssec.dedyn.io. 3599 IN A  95.217.209.184
dilithium2.pdns.pq-dnssec.dedyn.io. 3599 IN RRSIG A 18 5 3600 20240620000000 20240530000000 9247
dilithium2.pdns.pq-dnssec.dedyn.io. 4GiLZuz4ouEsR+bAsCW6hbo/PYKaa3FwPZbFXtWxrX4oZBgYBqc6nb/9
DqE6azh7Pi91r2pmHjb4Lj4l7vFJxMpgEXTRfkqFtZbXnNQl6vKsDW/+ PINJIPSAGTya9Utk2oI37b+K8ItfHwH/C7WOUX6sxFuofvhd1v+eeKs7
C+pRgrtwT9/s/Whsg7IbhFbyDt8n3MKOTeb8oRKtdwTnuabF7s3Ss5vI [...shortened...]qe qa632uPyAAAAAAAAAAAAAAAAAAAAAAAABAiLUA=

;; Query time: 308 msec
;; SERVER: 95.217.209.184#5302(pdns.pq-dnssec.dedyn.io) (TCP)
;; WHEN: Fri Jun 07 23:58:35 CEST 2024
;; MSG SIZE  rcvd: 2565
```

deSEC



Try it yourself!

https://pq-dnssec.dedyn.io/

Final Thoughts

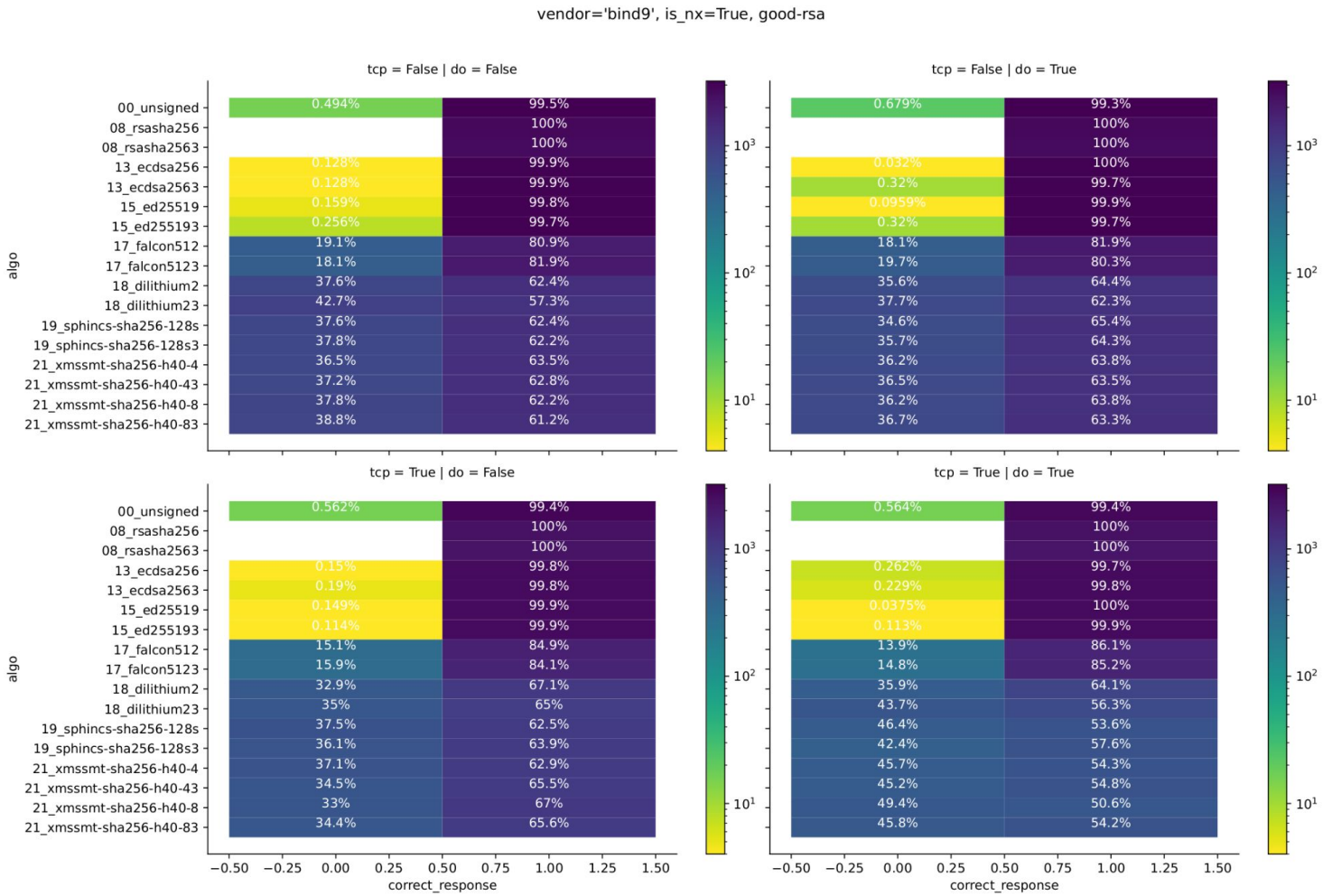
- **Transmission issues are real**
  - Gets worse with response size
- Fixing may require **revamping signature representation** in DNS
  - Merkle trees? ARRF?
  - Does not necessarily involve a wire format / spec change
  - Or will more robust DoT/DoH/DoQ gain enough traction?
- What would it take to **make the root quantum-safe**?
  - Further complications from double-signing – is this really needed?
- To transition, **any scalable solution will require DS provisioning automation**
- Future work needed!
  → Research agenda

Thank you!

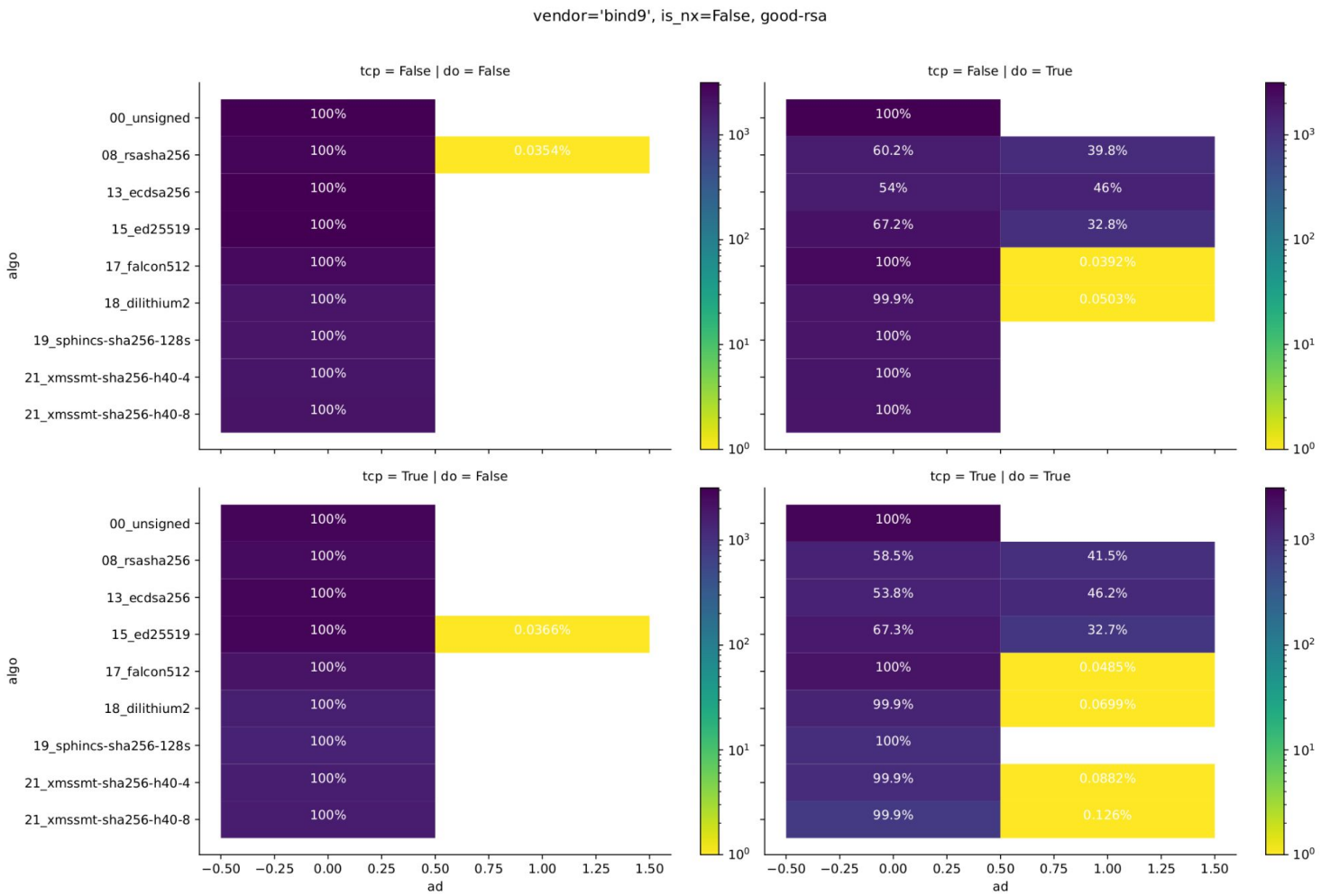
… also to:

Questions?

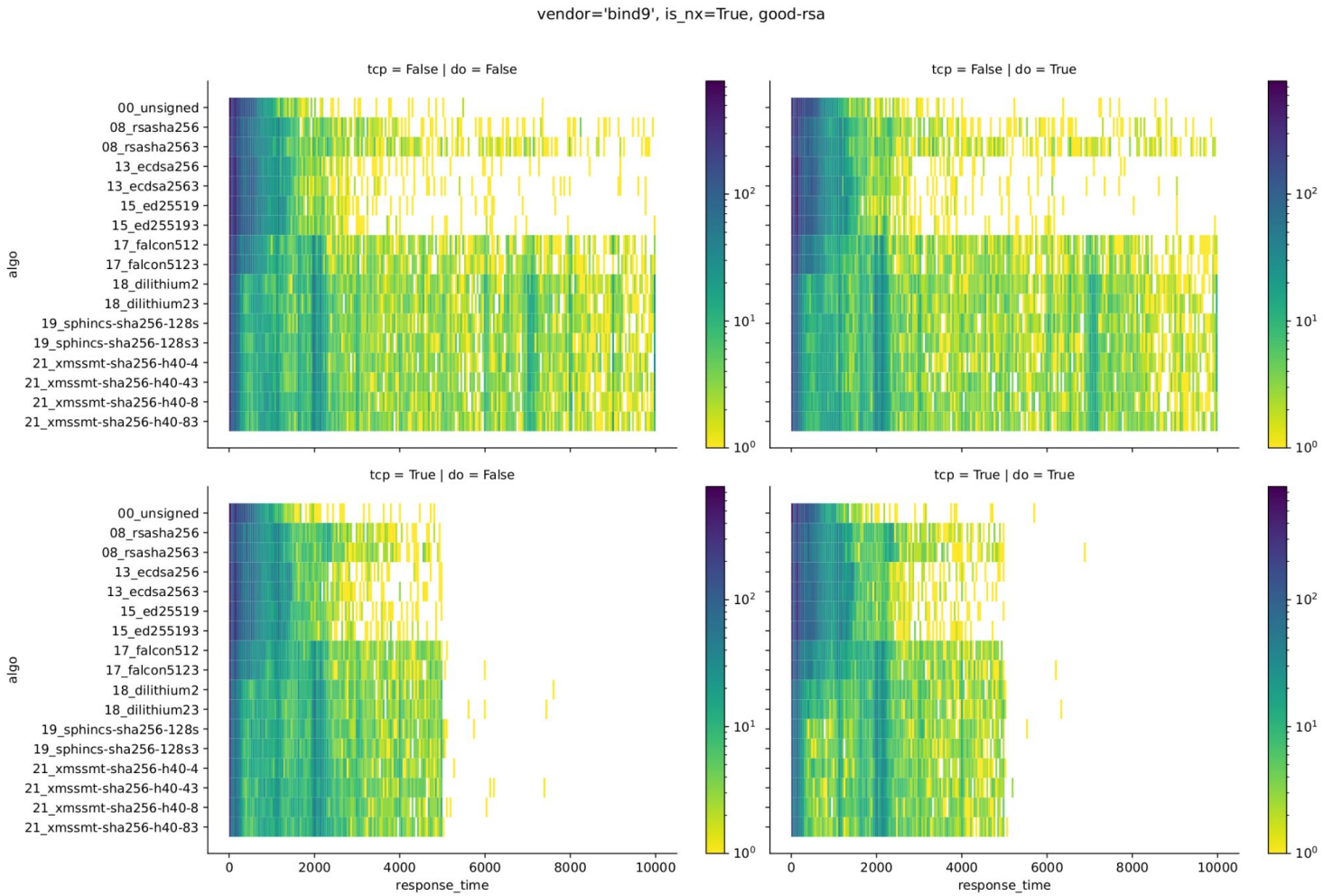
deSEC


vendor='bind9', 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-sha256-128s
19_sphincs-sha256-128s3
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-43
21_xmssmt-sha256-h40-8
21_xmssmt-sha256-h40-83
0.494% 99.5%
100% 100% 100% 100%
0.128% 99.9%
0.128% 99.9%
0.159% 99.8%
0.256% 99.7%
19.1% 80.9%
18.1% 81.9%
37.6% 62.4%
42.7% 57.3%
37.6% 62.4%
37.8% 62.2%
36.5% 63.5%
37.2% 62.8%
37.8% 62.2%
38.8% 61.2%
0.679% 99.3%
100% 100% 100%
0.032% 100%
0.32% 99.7%
0.0959% 99.9%
0.32% 99.7%
18.1% 81.9%
19.7% 80.3%
35.6% 64.4%
37.7% 62.3%
34.6% 65.4%
35.7% 64.3%
36.2% 63.8%
36.5% 63.5%
36.2% 63.8%
36.7% 63.3%
0.562% 99.4%
100% 100% 100%
0.15% 99.8%
0.19% 99.8%
0.149% 99.9%
0.114% 99.9%
15.1% 84.9%
15.9% 84.1%
32.9% 67.1%
35% 65%
37.5% 62.5%
36.1% 63.9%
37.1% 62.9%
34.5% 65.5%
33% 67%
34.4% 65.6%
0.564% 99.4%
100% 100% 100%
0.262% 99.7%
0.229% 99.8%
0.0375% 100%
0.113% 99.9%
13.9% 86.1%
14.8% 85.2%
35.9% 64.1%
43.7% 56.3%
46.4% 53.6%
42.4% 57.6%
45.7% 54.3%
45.2% 54.8%
49.4% 50.6%
45.8% 54.2%
10^3
10^2
10^1
−0.50 −0.25 0.00 0.25 0.50 0.75 1.00 1.25 1.50
correct_response

deSEC


vendor='bind9', 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
100%
0.0354%
60.2%
39.8%
54%
46%
67.2%
32.8%
0.0392%
99.9%
0.0503%
0.0366%
58.5%
41.5%
53.8%
46.2%
67.3%
32.7%
0.0485%
0.0699%
0.0882%
0.126%
ad
−0.50 −0.25 0.00 0.25 0.50 0.75 1.00 1.25 1.50
10^0 10^1 10^2 10^3

deSEC


vendor='bind9', 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-sha256-128s
19_sphincs-sha256-128s3
21_xmssmt-sha256-h40-4
21_xmssmt-sha256-h40-43
21_xmssmt-sha256-h40-8
21_xmssmt-sha256-h40-83
10^2
10^1
10^0
0
2000
4000
6000
8000
10000
response_time