Field Experiments on Post-Quantum DNSSEC

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

IEPG, Vancouver – July 21, 2024

Context & Motivation

- In 2022, performed (local-only) DNSSEC study with **Falcon** in PowerDNS
  - Results: https://blog.powerdns.com/2022/04/07/falcon-512-in-powerdns
- Now: Broader experiments with **multiple PQC algorithms**
  - fast validation, short signatures, short-ish keys
- Goal: **Public deployment** on the Internet, to investigate …
  - **behavior of non-PQC-aware resolvers** typically used by clients
  - **behavior of PQC-aware resolvers**
- Parameters:
  - KSK/ZSK (BIND) vs. CSK (PowerDNS)
  - Name existence and NSEC vs. [NSEC3 conventional (BIND) vs. minimal (PowerDNS)]
  - UDP vs. TCP
  - DO bit

deSEC

SANDBOXAQ

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)

deSEC

SANDBOXAQ

Steps Taken

- Implemented via **liboqs** (with regular unassigned algorithm numbers)
  - Falcon512
  - Dilithium2
  - Sphincs-SHA256-128s
  - XMSSmt-SHA256-h40-4 / XMSSmt-SHA256-h40-8 (and other parameter sets)
- Measurements using **RIPE ATLAS** (~10,000 probes, ~2M queries in May 2024)
- Output variables: **Rcode, Correctness, AD bit, response time**
- Pre-selection: Exclude …
  - probe-resolver combinations with incorrect response for RSA-SHA256 (due to noise)
  - resolvers in private IP ranges (due to RIPE ATLAS limitation for TCP)
  - timeouts and network errors

deSEC

SANDBOXAQ

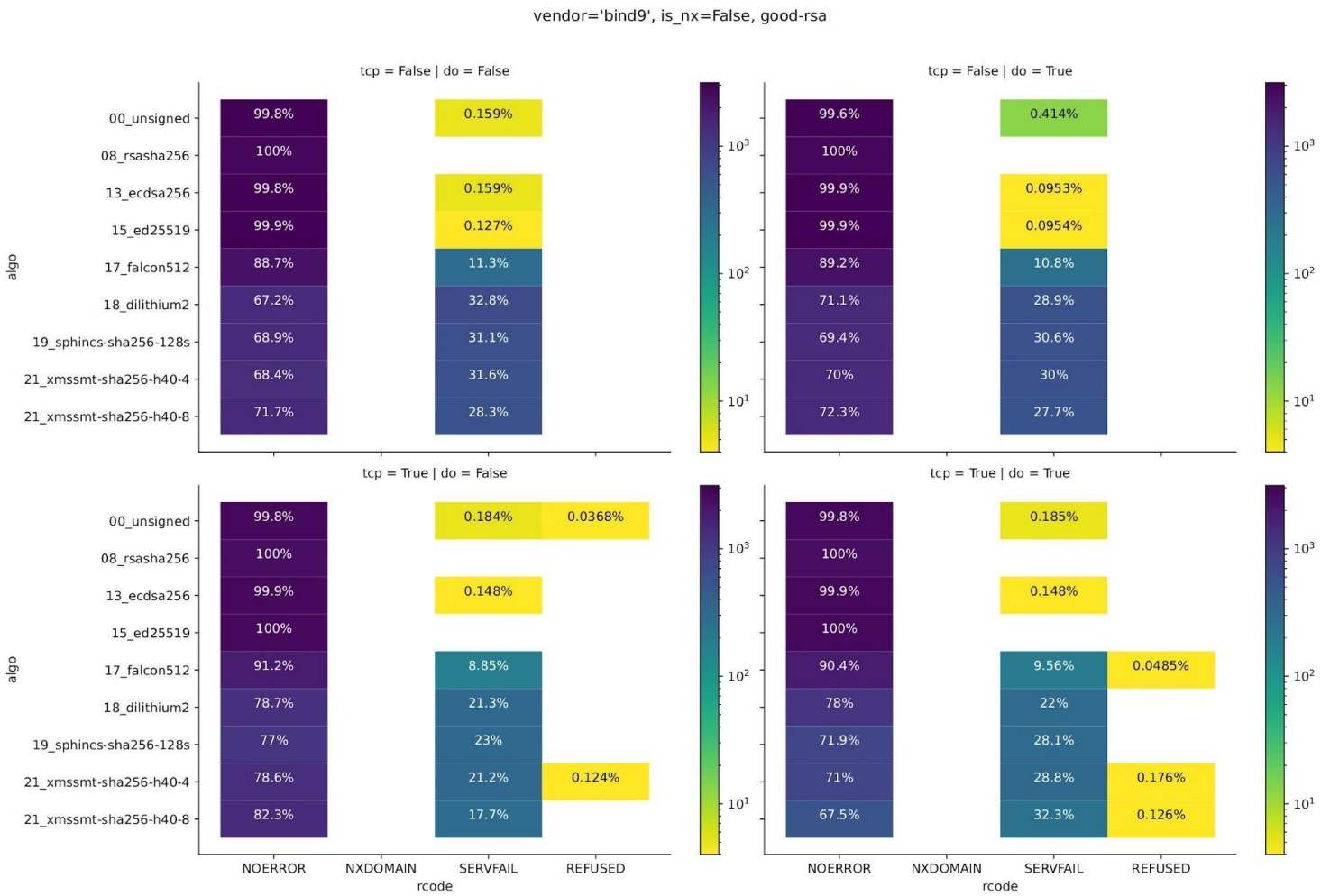
Queries Using an Unaware Resolver

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

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

; <<>> DiG 9.18.24-0ubuntu0.22.04.1-Ubuntu <<>> +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29078
;; 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. 3599 IN RRSIG A 18 5 3600 20240801000000 20240711000000 3978 dilithium2.pdns.pq-dnssec.ded
yn.io. 19/28JXGCgGbNtEAtUOzv1/SzP+kr6vBlglWrJ/ZfYgdC1DXZHdh+xol rnZ9uhvmADCqZzJXOyOU1Tyw2sHN32Vmcv4KLR8lI7TBwfTJq6T3nGfV oQnv9
DNvPJTyb4VonYH3fLTMYeQ3/0Wy9gbv0ngy55QqRjw+ikhS0yIp ezpZYH3ArY/xxmTgM7OBW0yBg3gXgo1G2mrX97ufqrwkO/n0Vu/xXfSI npGKq+dVu7LQQR7nM
lmM3FkbaRAFyo0FjmbzXDPtyrwJekJP8dfQ5zvc pOCRfrpjRg+ZBUofhdk1PURO539JwD[...shortened...]AA AAAAAAAAAAAAAAAAAAAAAAAAAAABAcJzc=

;; Query time: 208 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Fri Jul 19 23:57:40 PDT 2024
;; MSG SIZE  rcvd: 2565
```

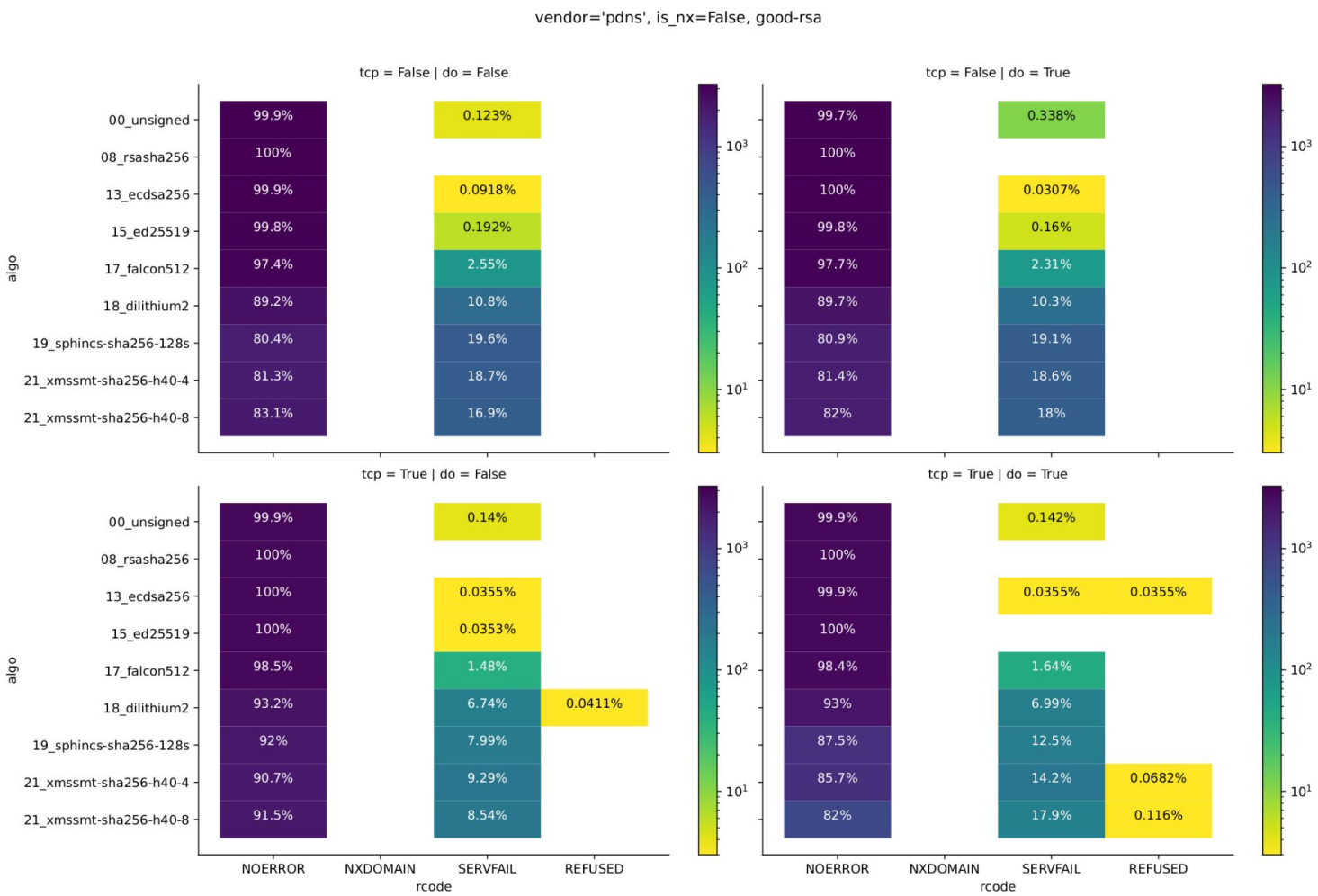
deSEC

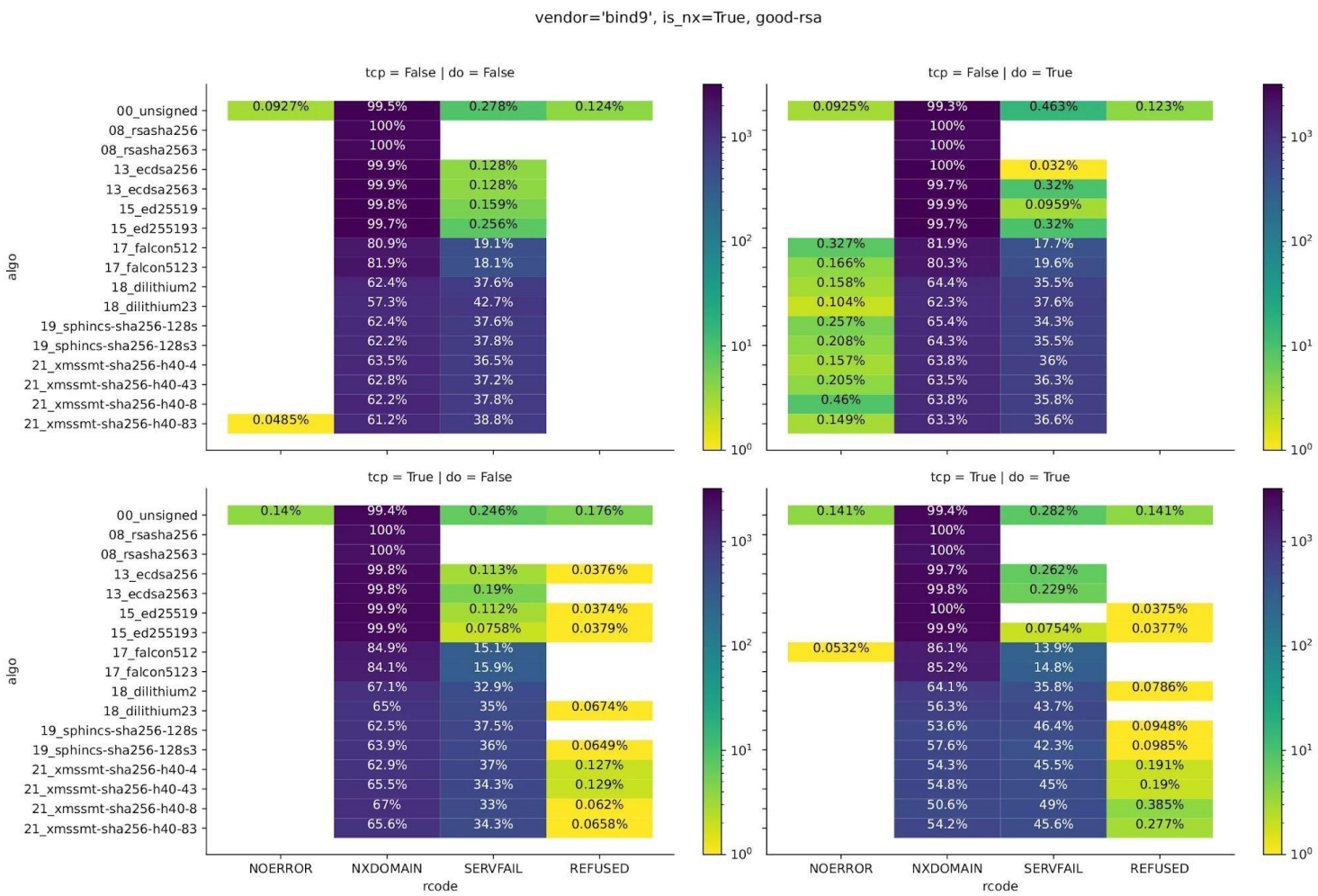
SANDBOXAQ



deSEC

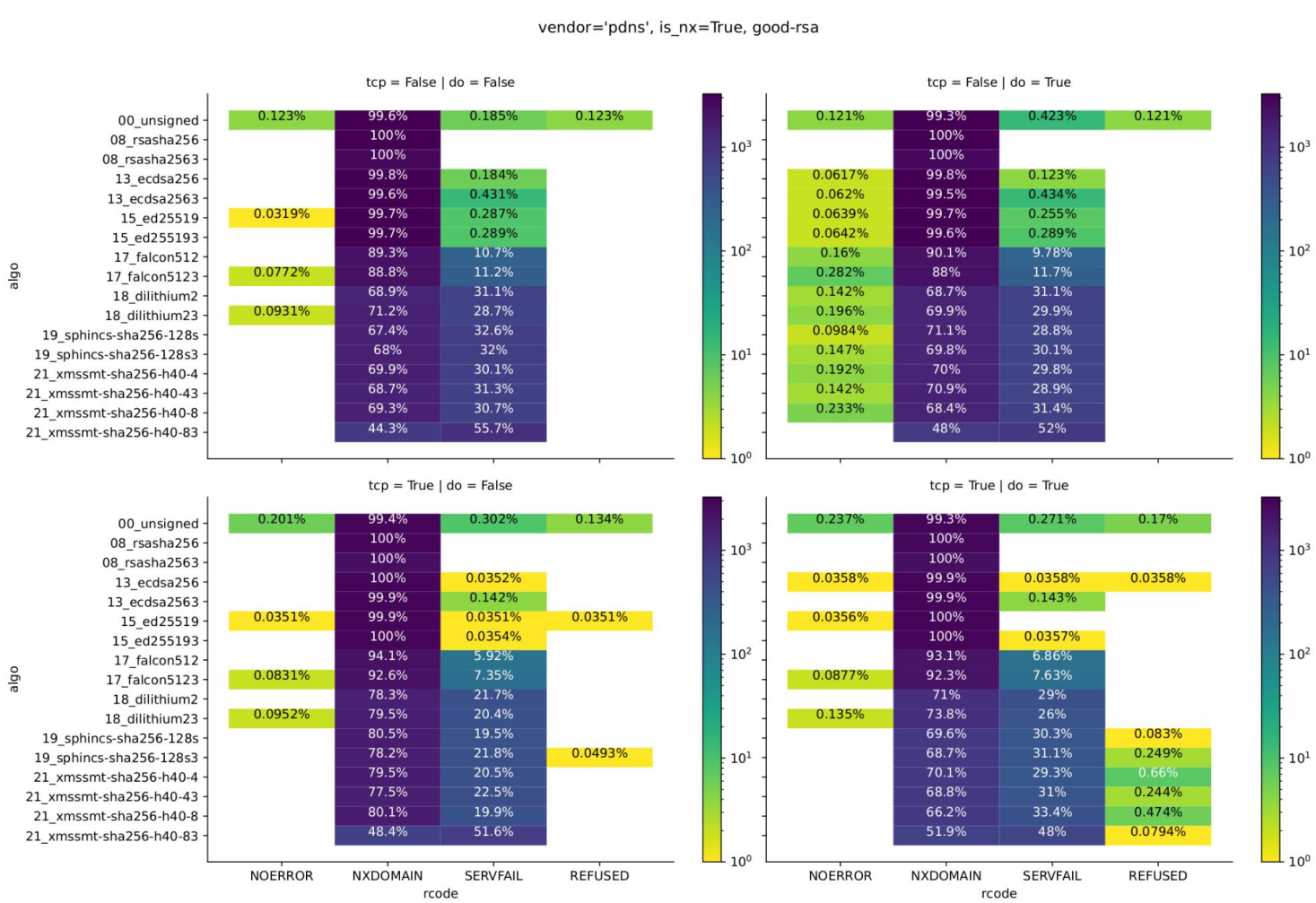
SANDBOXAQ





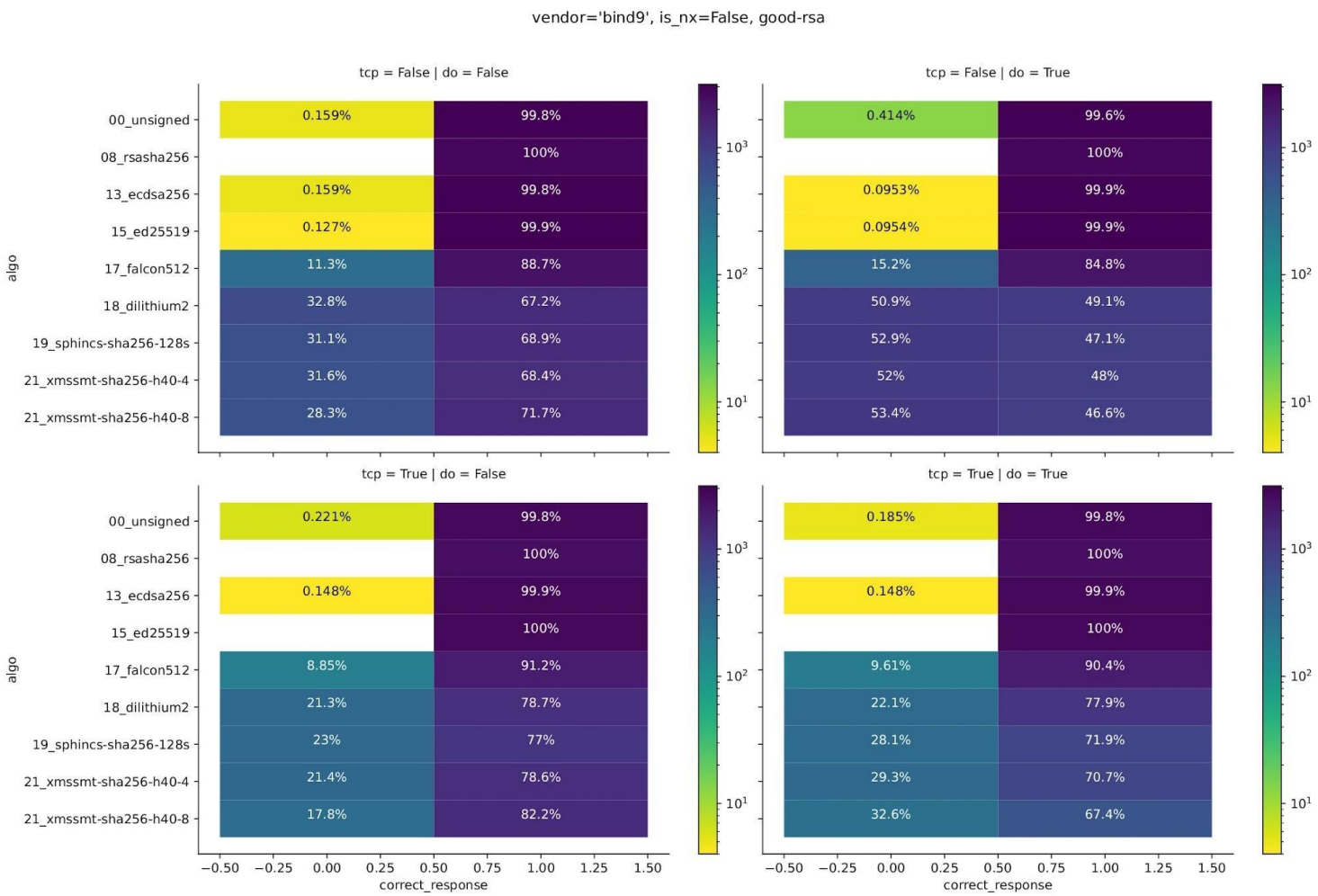
deSEC

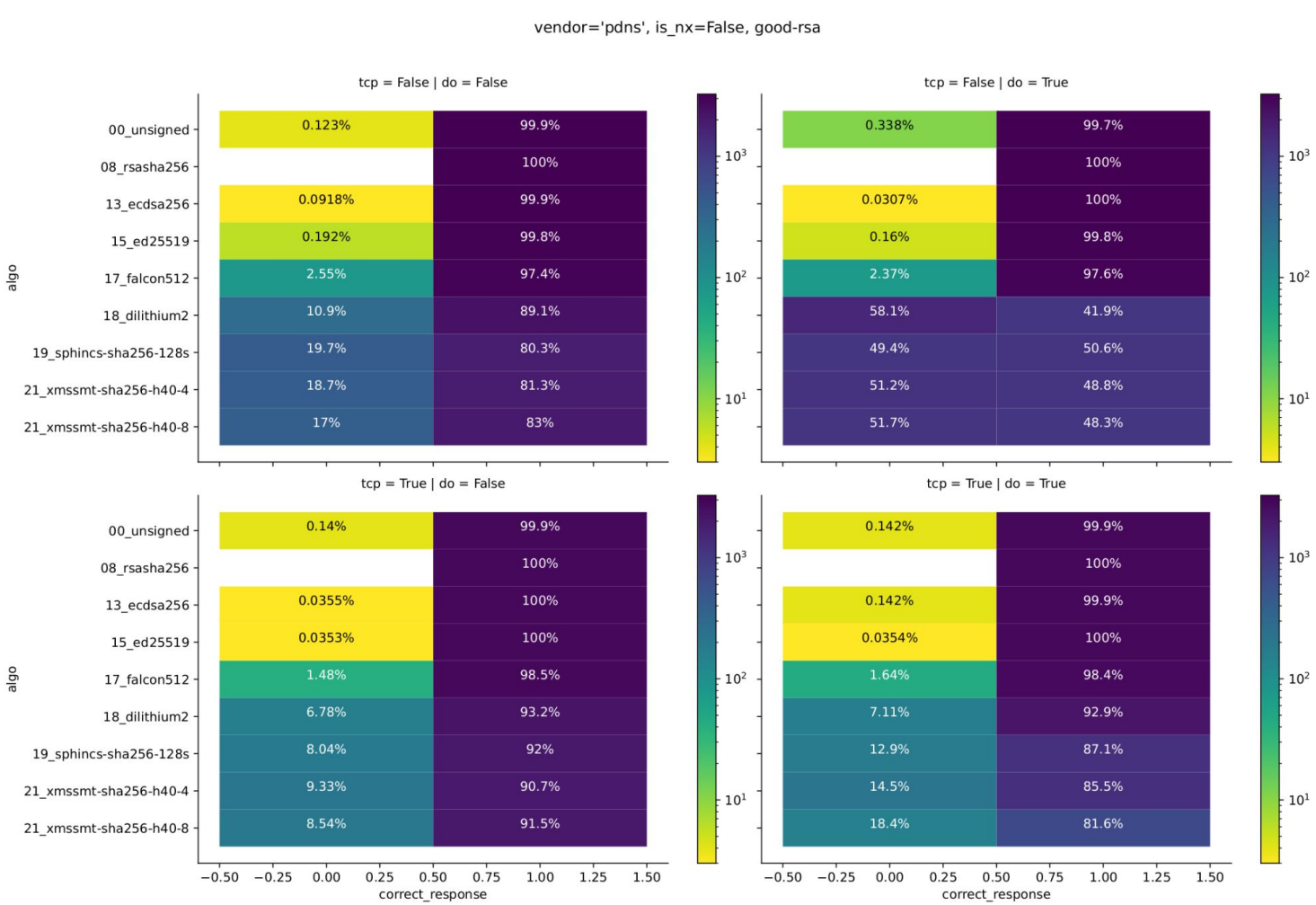
SANDBOXAQ


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-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
10^3
10^2
10^1
10^0

deSEC

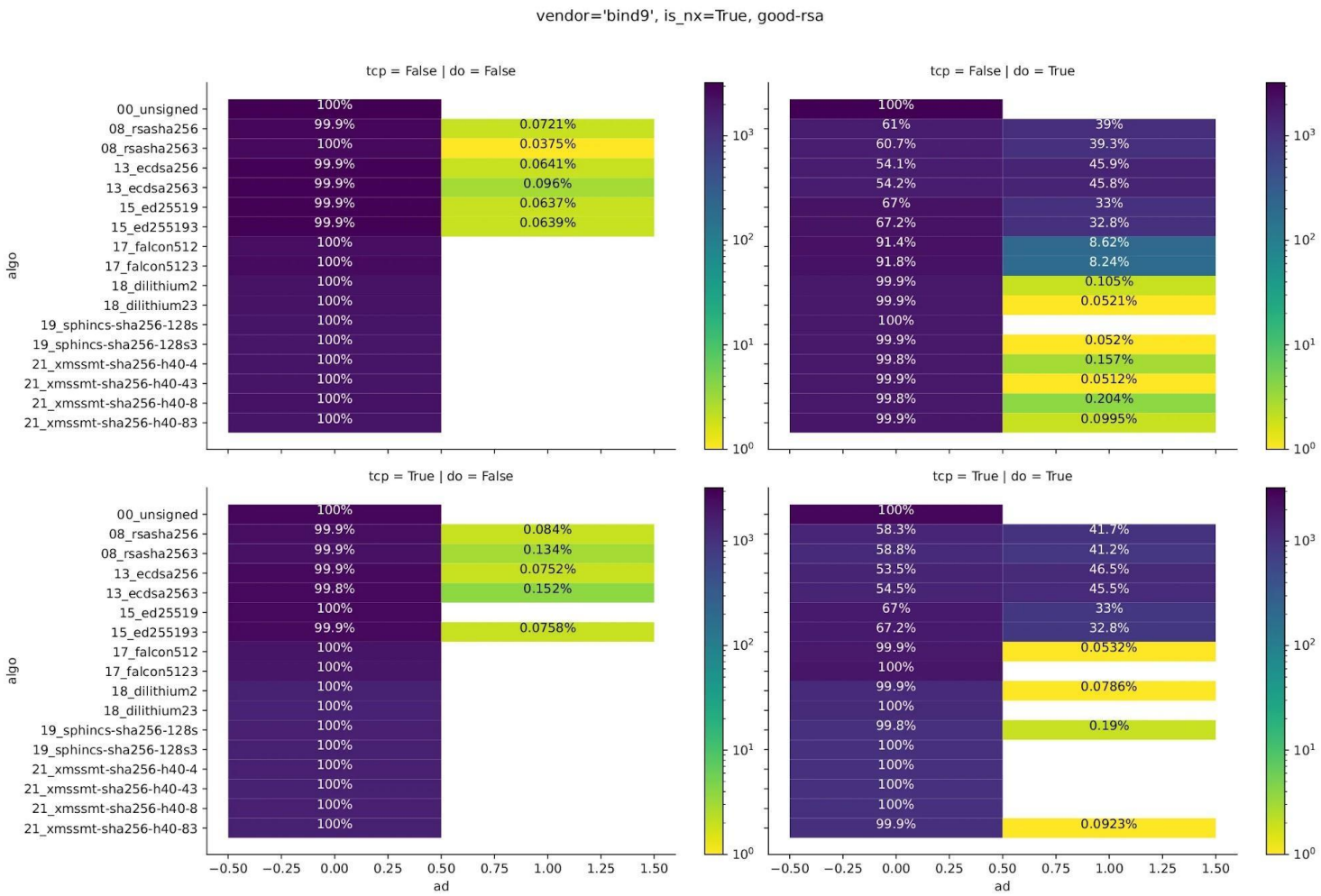
SANDBOXAQ




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
0.123% 99.9%
100%
0.0918% 99.9%
0.192% 99.8%
2.55% 97.4%
10.9% 89.1%
19.7% 80.3%
18.7% 81.3%
17% 83%
0.338% 99.7%
100%
0.0307% 100%
0.16% 99.8%
2.37% 97.6%
58.1% 41.9%
49.4% 50.6%
51.2% 48.8%
51.7% 48.3%
0.14% 99.9%
100%
0.0355% 100%
0.0353% 100%
1.48% 98.5%
6.78% 93.2%
8.04% 92%
9.33% 90.7%
8.54% 91.5%
0.142% 99.9%
100%
0.142% 99.9%
0.0354% 100%
1.64% 98.4%
7.11% 92.9%
12.9% 87.1%
14.5% 85.5%
18.4% 81.6%
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

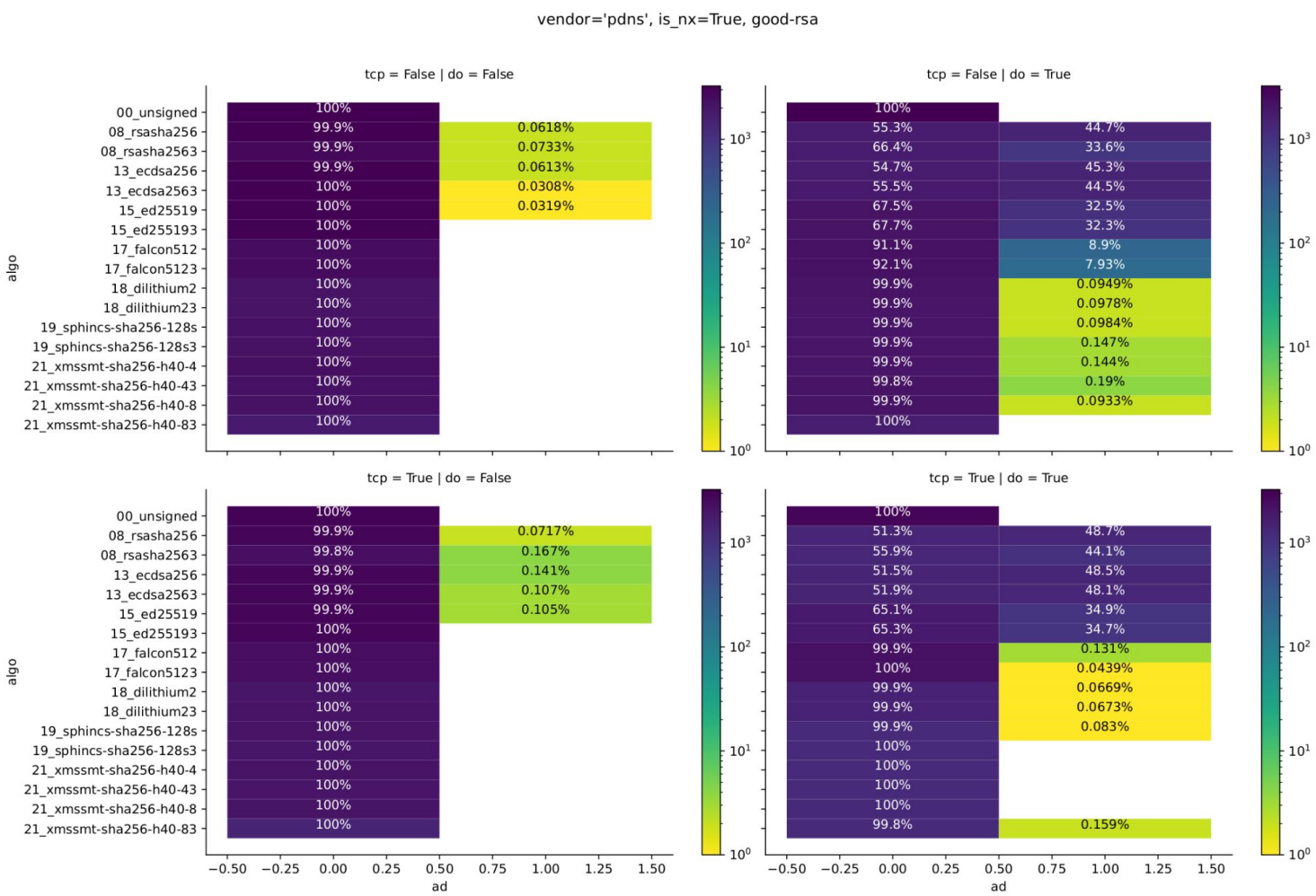
deSEC

SANDBOXAQ



deSEC

SANDBOXAQ



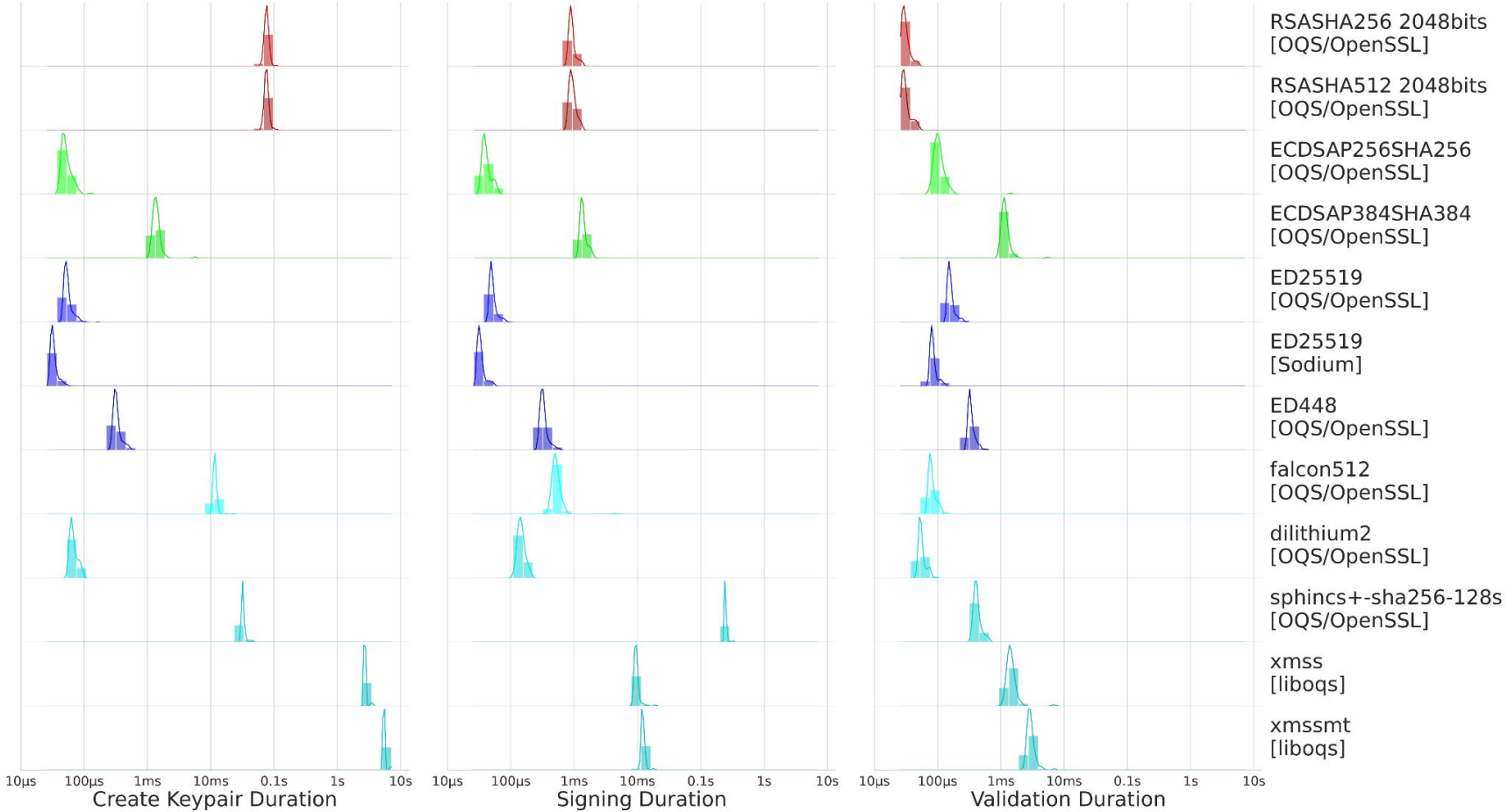
deSEC

SANDBOXAQ

Takeaways

- **Transmission issues are real**
  - PQC response delivery rates go down significantly as response sizes increase → Falcon leads
  - Gets worse depending on circumstances, like with DO bit or with NSEC3
- **UDP & DO=0:**
  ~70% KSK/ZSK responses correct
  ~80% CSK responses correct
  - Goes up by ~10% via TCP
- **UDP & DO=1:**
  ~50% responses correct
  - Goes up by ~20–40% via TCP
- 8.5% of probe-resolver pairs claim successfully validating Falcon

Crypto Algorithm Run Time (PowerDNS)



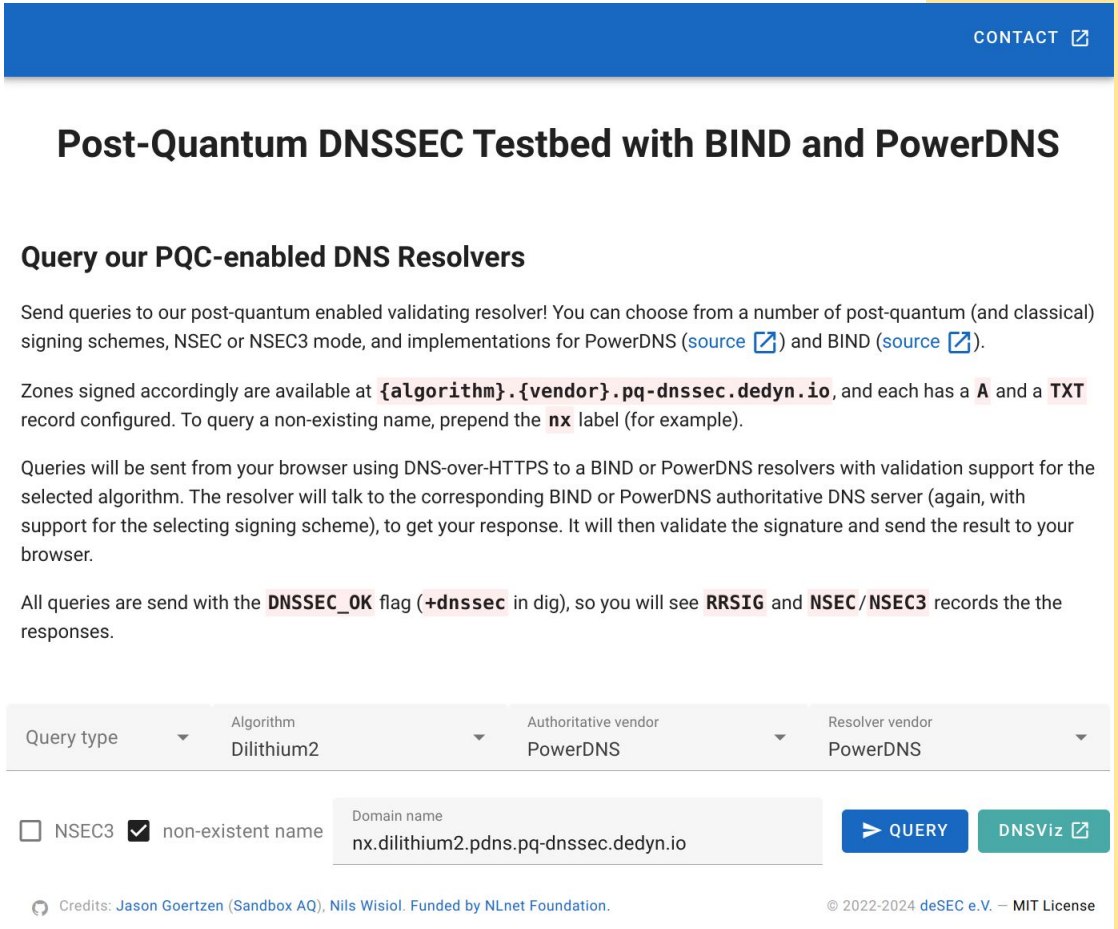
Queries Using a PQC-aware Resolver

deSEC

SANDBOXAQ

```
dig +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @bind9.pq-dnssec.dedyn.io -p 5304
```

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

; <<>> DiG 9.18.24-0ubuntu0.22.04.1-Ubuntu <<>> +dnssec A dilithium2.pdns.pq-dnssec.dedyn.io @bind9.pq-dnssec.dedyn.io -p 5304
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22245
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 8455829f86d7fb7601000000669b5d9517dfc67dff539cac (good)
;; 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 20240801000000 20240711000000 3978 dilithium2.pdns.pq-dnssec.dedyn.io. 19/28JXGCgGbNtEAtUOzv1/SzP+kr6vBlglWrJ/ZfYgdC1DXZHdh+xol rnZ9uhvmADCqZzJXOyOU1Tyw2sHN32Vmcv4KLR8lI7TBwfTJq6T3nGfV oQnv9DNvPJTyb4VonYH3fLTMYeQ3/0Wy9gbv0ngy55QqRjw+ikhS0yIp ezpZYH3ArY/xxmTgM7OBW0yBg3gXgo1G2mrX97ufqrwkO/n0Vu/xXfSI npGKq+dVu7LQQR7nMlmM3FkbaRAFyo0FjmbzXDPtyrwJekJP8dfQ5zvc pOCRfrpjRg+ZBUofhdk1PURO539JwD[...shortened...]AA AAAAAAAAAAAAAAAAAAAAAAAAAAAABAcJzc=

;; Query time: 56 msec
;; SERVER: 35.232.14.170#5304(bind9.pq-dnssec.dedyn.io) (TCP)
;; WHEN: Fri Jul 19 23:47:49 PDT 2024
;; MSG SIZE  rcvd: 2593
```



deSEC

SANDBOXAQ

Try it yourself!

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

deSEC

SANDBOXAQ

Thank you!

… also to:

Questions?

deSEC

SANDBOXAQ

Backup: Outlook

- 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