# Measuring PQ DNSSEC performance

DNS OARC 47

*Bas Westerbaan, Joe Abley, Sebastiaan Neuteboom, Vicky Shrestha, Wouter de Vries*
Cloudflare

# Post-Quantum Cryptography

- The core standards are settled
  - FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)
  - FIPS 206 (FN-DSA) still under construction
- PQC is mainstream
  - ML-KEM hybrids are enabled by default across major browsers, CDNs, OS TLS libraries
  - A significant amount of encrypted web traffic is quantum-resistant in transit
- The clock is now official
  - NIST's transition guidance in IR 8547 deprecates classical 112-bit-strength crypto around 2030 and proposes full disallowance by 2035
  - Several governments have 2030/2031 deadlines for critical or high-impact systems
- Work has shifted to the long tail
  - embedded devices, industrial systems, long-lived code
  - "harvest now, decrypt later"

# DNSSEC

- Lots of talks at lots of meetings
  - IETF working groups, interims and side meetings; multiple DNS-OARCs, RIPE dns-wgs
- Root zone signed with alg 8 (RSA/SHA-256)
- Most TLDs signed with alg 8
  - a growing number signed with 13 (ECDSA Curve P-256/SHA-256)
  - three still signed with 3 (RSA/SHA-1)
  - 86 TLDs are not signed at all, so at least they are not threatened by quantum computers
- Number of PQ algorithms available in mainstream DNSSEC signers: zero
- Proportion of DNS responses signed with PQ algorithms: zero
- Number of PQ algorithms actually specified for use in DNSSEC: zero
- Number of registries that will accept a PQ algorithm in a DS RRSet: zero

# Details in case anybody is interested (2026-10-20)

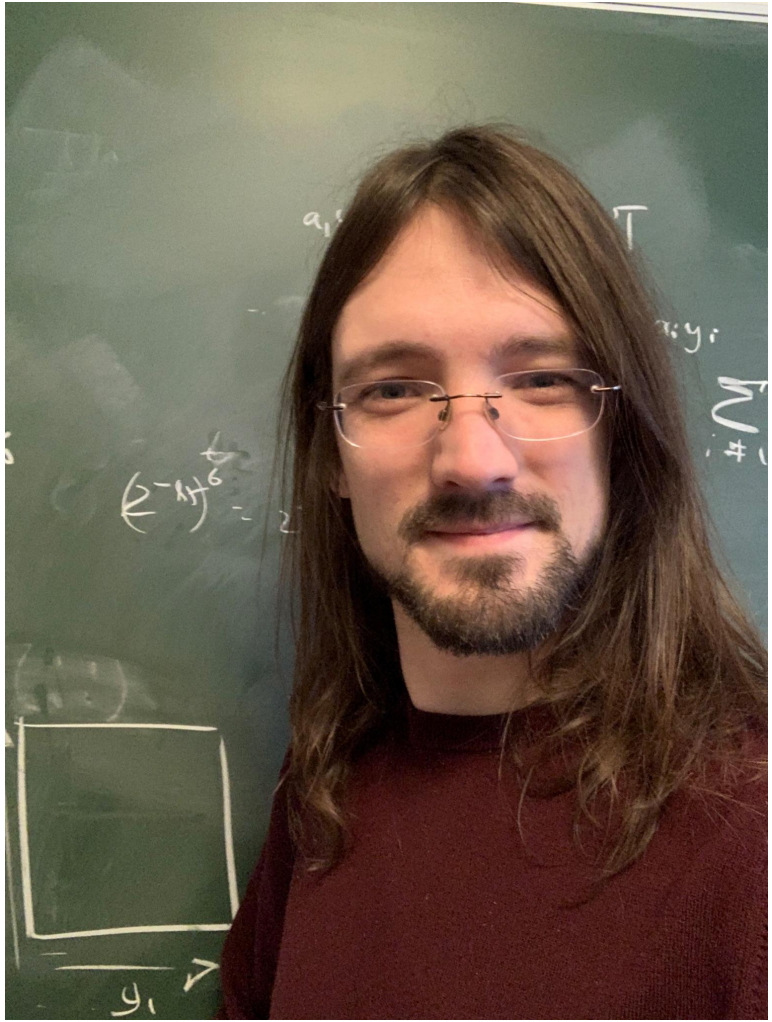
```
Source: https://www.internic.net/domain/root.zone
Algorithm names: IANA registry
Total TLDs in root zone: 1437
  Signed (DS present):     1351  94.0%
  Unsigned (no DS):          86   6.0%
 Alg   TLDs   % all  Algorithm
----  -----  ------  ----------------------------------------
   8   1046   72.8%  RSASHA256 - RSA/SHA-256
  13    273   19.0%  ECDSAP256SHA256 - ECDSA Curve P-256 with SHA-256
  10     28    1.9%  RSASHA512 - RSA/SHA-512
   5      3    0.2%  RSASHA1 - RSA/SHA-1  [includes NSEC3 alias 7]
  15      3    0.2%  ED25519 - Ed25519
  14      1    0.1%  ECDSAP384SHA384 - ECDSA Curve P-384 with SHA-384
   -     86    6.0%  Unsigned (insecure delegation)
3 TLD(s) publish DS records for more than one algorithm (counted under each; likely mid-rollover):
  .biz: 8, 13
  .club: 8, 13
  .vip: 8, 13
TLDs using alg 10 (RSASHA512):
  .alstom, .barcelona, .bauhaus, .bcn, .cat, .erni, .eurovision, .eus, .gal, .gmx, .gw, .ifm, .lacaixa, .madrid, .man, .mango, .nrw, .quebec, .radio, .sap, .scot,
.seat, .sport, .swiss, .vu, .xn--80asehdb, .xn--80aswg, .xn--mgbab2bd
TLDs using alg 5 (RSASHA1):
  .gd, .la, .xn--q7ce6a
TLDs using alg 15 (ED25519):
  .fj, .ml, .pg
TLDs using alg 14 (ECDSAP384SHA384):
  .md
Unsigned TLDs:
  .ae, .ao, .aq, .ba, .bb, .bo, .bs, .cd, .cf, .cg, .ck, .cu, .cv, .cw, .do, .eg, .fk, .gb, .gf, .gh, .gm, .gp, .gq, .gt, .gu, .hm, .im, .iq, .jm, .jo, .kh, .km, .kn,
.kp, .mh, .mk, .mo, .mp, .mq, .mt, .mv, .mw, .mz, .ne, .ni, .np, .nr, .om, .pa, .pf, .pn, .ps, .qa, .sd, .sl, .sm, .so, .st, .sv, .sy, .sz, .td, .tg, .tj, .tk, .to,
.va, .vg, .vi, .xn--d1alf, .xn--fzc2c9e2c, .xn--j1amh, .xn--lgbbat1ad8j, .xn--mgb9awbf, .xn--mgba3a4f16a, .xn--mgbaam7a8h, .xn--mgbc0a9azcg, .xn--mgbpl2fh,
.xn--mgbtx2b, .xn--mix891f, .xn--node, .xn--ogbpf8fl, .xn--wgbl6a, .xn--ygbi2ammx, .ye, .zw
```

# This seems not so great

- We are hostages in a siege of response size paranoia
  - PQ signatures are large
  - Large responses cannot be reliably carried over UDP
  - Fallback to TCP is unreliable
    - because blocked by middleboxes
    - because not implemented in clients
  - Fallback to TCP will break authoritative servers
    - because stream setup/teardown overhead
    - because state explosion
- This seems even more dreadful
- This is why people joke about replacing the DNS protocol altogether
  - but they have a haunted look in their eye while they are choking back their tears

# Bas Westerbaan is Displeased

- This is Bas
  - Hello Bas! 👋
- Bas has run out of PQ things to fix in other protocols now
- Bas has noticed DNSSEC
  - Oh dear, Bas is on to us



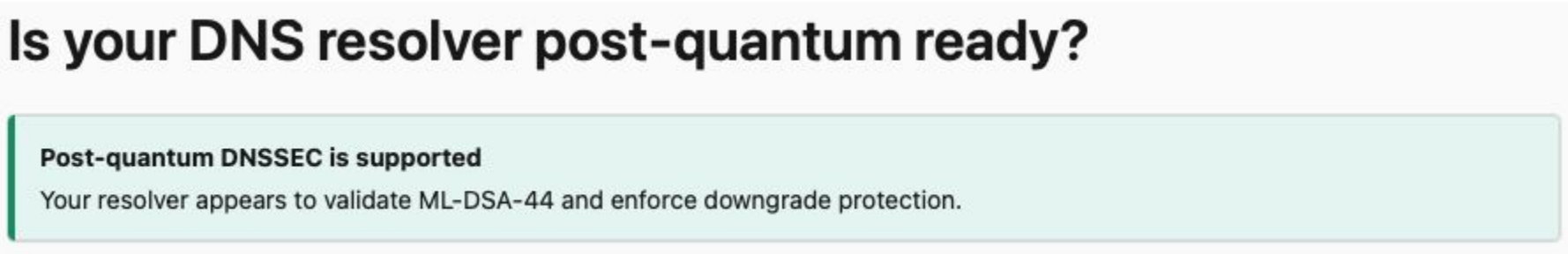
# First we need an algorithm

- Let's put a finger in the air and choose a PQ algorithm to try
  - Something that is standardised
  - Something that is easy to implement safely (e.g. using integer arithmetic)
  - Something that is fast, for signers and for validators
  - Something with signatures that are not too alarmingly monstrous
- Let's say ML-DSA, which plausibly checks all of those boxes
  - In fact, ML-DSA-44, since that has the smallest parameter set
  - Other algorithms might turn out to be better
  - Fixating on choice of algorithm is the opposite of trying things, so let's not fixate
  - Let's try this
- draft-westerbaan-dnssec-mldsa
  - code-point 18 assigned following expert review

# Validation

# Implement ML-DSA-44 in 1.1.1.1

- 1.1.1.1 now supports post-quantum DNSSEC, all 2,420 bytes of it (10 September 2026)
  - Fully live for all clients
  - This seemed like a reasonable thing to do first
    - there are no alg 18 signatures to speak of in the wild, so nothing should break
- Implemented a way to tell what your local resolver is doing
  - https://dnstest.dev/post-quantum/ (details on that page)



# Downgrade protection

- Normally DNSSEC validators accept any valid chain of signatures
  - There is no concept of downgrade protection
  - If a signature is present that you can validate, hooray! you are done, full steam ahead
  - If multiple signatures are present and one of them fails to validate, keep trying, one of them might work
- The whole point of PQ algorithms is they offer protection against attacks against non-PQ algorithms
  - If a response is signed by both PQ and legacy algorithms and the PQ signature fails to validate while the legacy signature is fine, this is actually not OK
    - this is what an attack by a quantum computer looks like
- draft-jabley-dnsop-local-signing-algorithm-policy

# Measurements

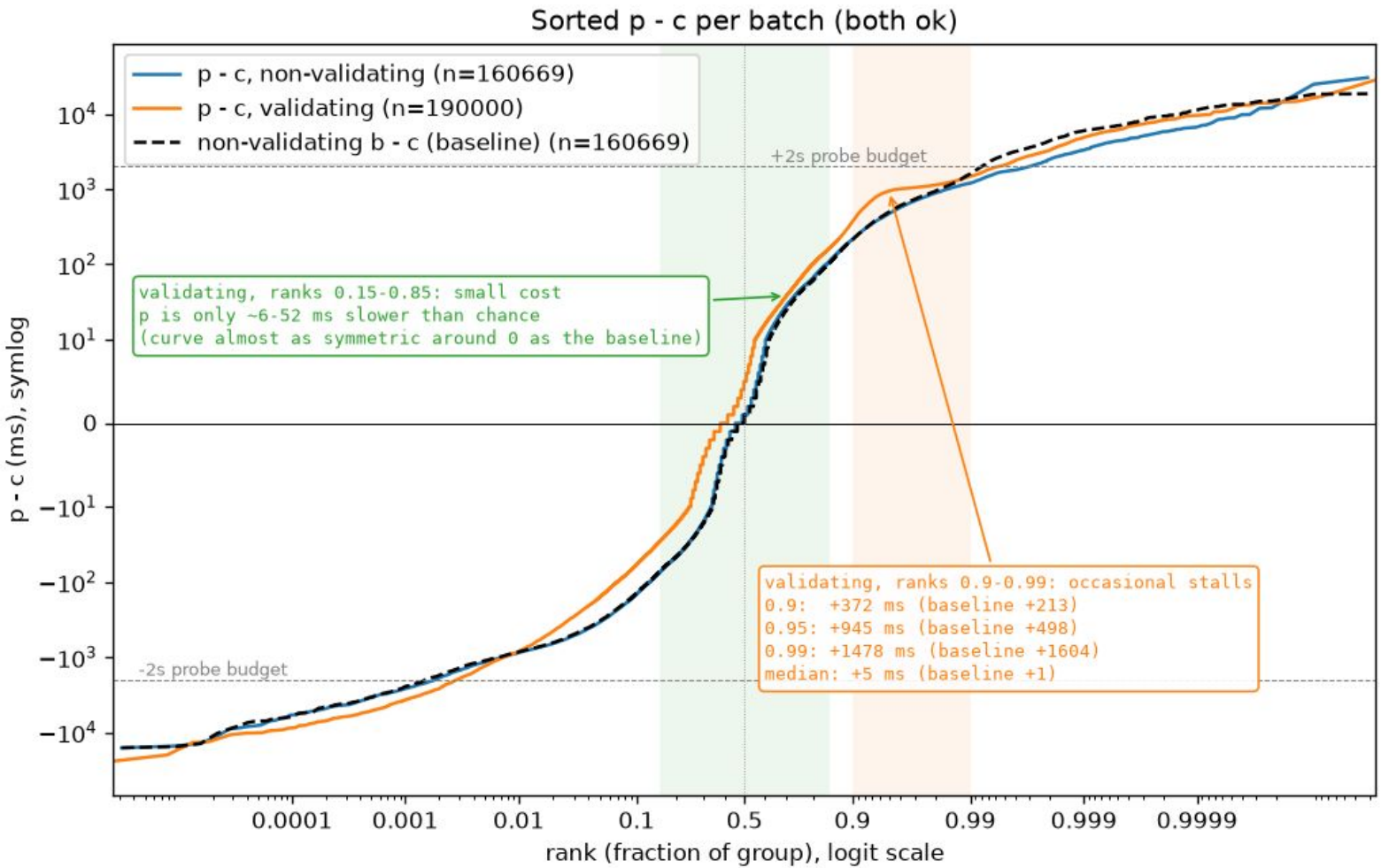

Verifying...
CLOUDFLARE
Privacy • Terms

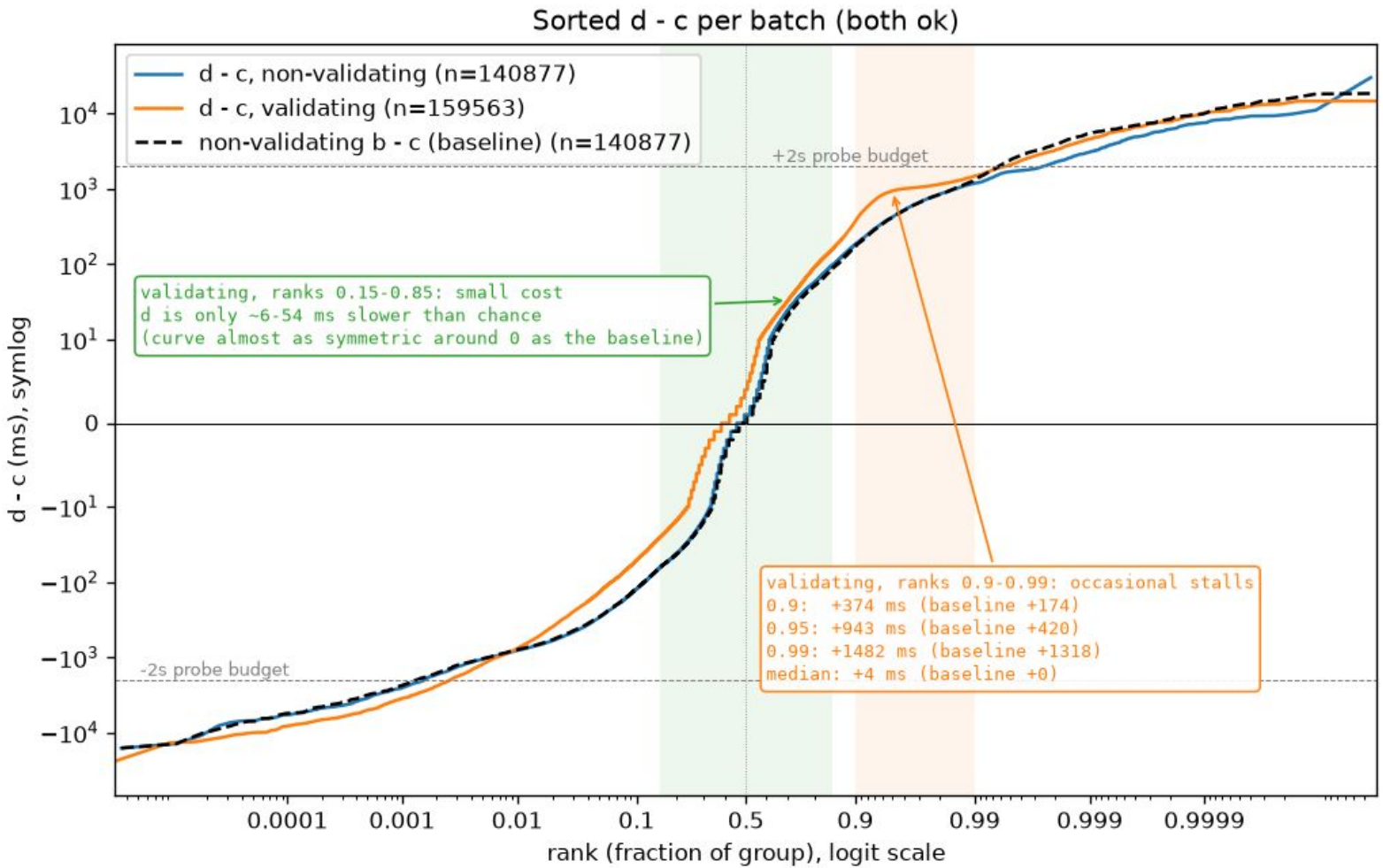
# Experiment embedded in challenge

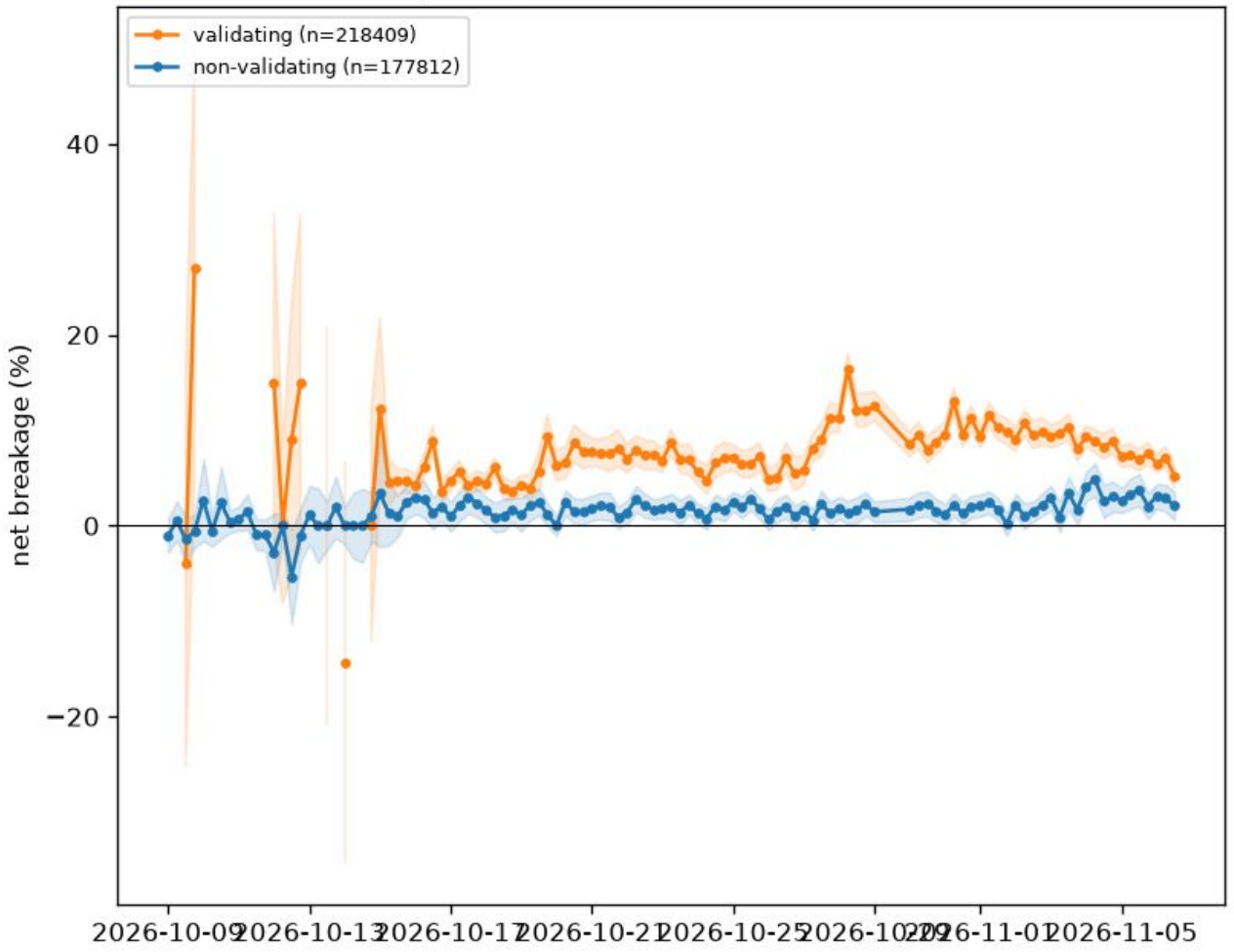
- Four identical objects fetched using HTTPS by name in parallel
- Names served by Cloudflare DNS
  - one name signed with alg 13 (c = control)
  - one name signed with alg 13 with a broken signature (b = broken)
  - one name signed with alg 18 (p = pq)
  - one name dual-signed with alg 13 and 18 (d = dual)
- Fetches can succeed, fail with an error or time out
- The experiment is capped, incomplete fetches at 2 seconds show as timeouts
- Timeouts can be a result of the user solving the challenge quickly
- Lots of background noise (browsers, home networks)
- No cache busting in the initial dataset

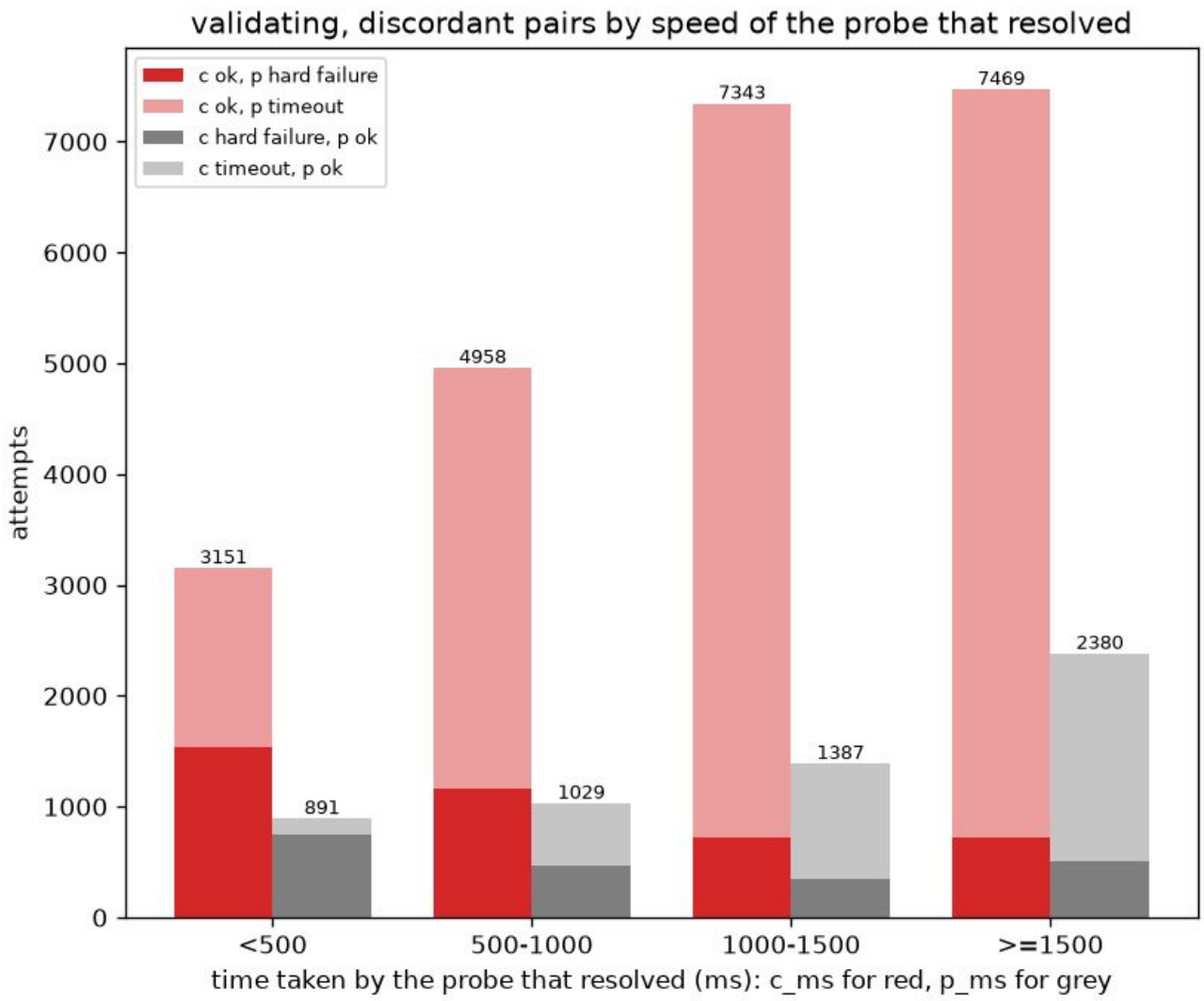
# These are initial results

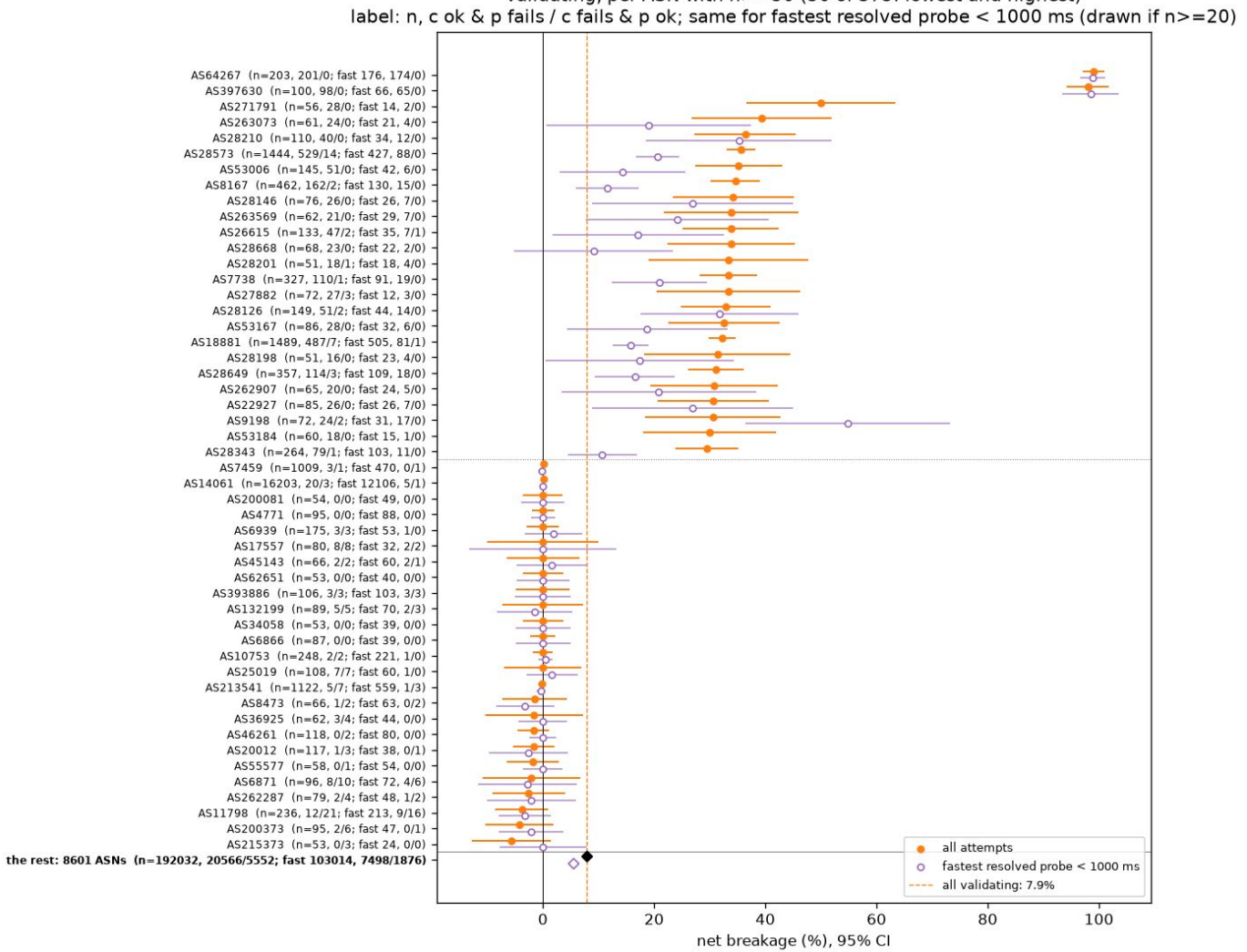
- These experiments have only been running for a short time
- This is an early glimpse into what we see so far
- There are actual AS numbers mentioned ahead
  - This is encouragement for people to help us understand our data
  - This is not a wall of shame
- These visualisations are also early attempts to understand the data
  - Put on your peril-sensitive sunglasses

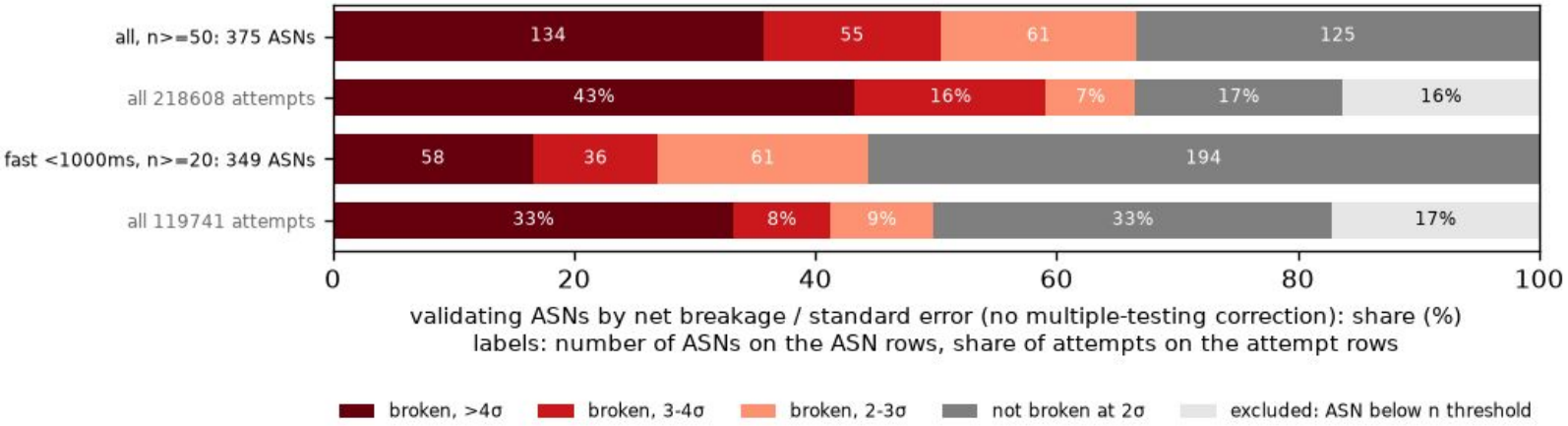

Sorted p - c per batch (both ok)
p - c, non-validating (n=160669)
p - c, validating (n=190000)
non-validating b - c (baseline) (n=160669)
+2s probe budget
-2s probe budget
validating, ranks 0.15-0.85: small cost
p is only ~6-52 ms slower than chance
(curve almost as symmetric around 0 as the baseline)
validating, ranks 0.9-0.99: occasional stalls
0.9: +372 ms (baseline +213)
0.95: +945 ms (baseline +498)
0.99: +1478 ms (baseline +1604)
median: +5 ms (baseline +1)
p - c (ms), symlog
rank (fraction of group), logit scale
0.0001
0.001
0.01
0.1
0.5
0.9
0.99
0.999
0.9999


Sorted d - c per batch (both ok)
d - c, non-validating (n=140877)
d - c, validating (n=159563)
non-validating b - c (baseline) (n=140877)
+2s probe budget
-2s probe budget
validating, ranks 0.15-0.85: small cost
d is only ~6-54 ms slower than chance
(curve almost as symmetric around 0 as the baseline)
validating, ranks 0.9-0.99: occasional stalls
0.9: +374 ms (baseline +174)
0.95: +943 ms (baseline +420)
0.99: +1482 ms (baseline +1318)
median: +4 ms (baseline +0)
d - c (ms), symlog
rank (fraction of group), logit scale
0.0001
0.001
0.01
0.1
0.5
0.9
0.99
0.999
0.9999


p vs c net breakage: (c ok & p fails - c fails & p ok) / attempts with one resolved
per 6h, 95% CI, bins with n>=20
validating (n=218409)
non-validating (n=177812)
net breakage (%)
40
20
0
−20
2026-10-09
2026-10-13
2026-10-17
2026-10-21
2026-10-25
2026-10-29
2026-11-01
2026-11-05


validating, discordant pairs by speed of the probe that resolved
c ok, p hard failure
c ok, p timeout
c hard failure, p ok
c timeout, p ok
attempts
0
1000
2000
3000
4000
5000
6000
7000
3151
891
4958
1029
7343
1387
7469
2380
<500
500-1000
1000-1500
>=1500
time taken by the probe that resolved (ms): c_ms for red, p_ms for grey


validating, per ASN with n>=50 (50 of 375: lowest and highest)
label: n, c ok & p fails / c fails & p ok; same for fastest resolved probe < 1000 ms (drawn if n>=20)
AS64267 (n=203, 201/0; fast 176, 174/0)
AS397630 (n=100, 98/0; fast 66, 65/0)
AS271791 (n=56, 28/0; fast 14, 2/0)
AS263073 (n=61, 24/0; fast 21, 4/0)
AS28210 (n=110, 40/0; fast 34, 12/0)
AS28573 (n=1444, 529/14; fast 427, 88/0)
AS53006 (n=145, 51/0; fast 42, 6/0)
AS8167 (n=462, 162/2; fast 130, 15/0)
AS28146 (n=76, 26/0; fast 26, 7/0)
AS263569 (n=62, 21/0; fast 29, 7/0)
AS26615 (n=133, 47/2; fast 35, 7/1)
AS28668 (n=68, 23/0; fast 22, 2/0)
AS28201 (n=51, 18/1; fast 18, 4/0)
AS7738 (n=327, 110/1; fast 91, 19/0)
AS27882 (n=72, 27/3; fast 12, 3/0)
AS28126 (n=149, 51/2; fast 44, 14/0)
AS53167 (n=86, 28/0; fast 32, 6/0)
AS18881 (n=1489, 487/7; fast 505, 81/1)
AS28198 (n=51, 16/0; fast 23, 4/0)
AS28649 (n=357, 114/3; fast 109, 18/0)
AS262907 (n=65, 20/0; fast 24, 5/0)
AS22927 (n=85, 26/0; fast 26, 7/0)
AS9198 (n=72, 24/2; fast 31, 17/0)
AS53184 (n=60, 18/0; fast 15, 1/0)
AS28343 (n=264, 79/1; fast 103, 11/0)
AS7459 (n=1009, 3/1; fast 470, 0/1)
AS14061 (n=16203, 20/3; fast 12106, 5/1)
AS200081 (n=54, 0/0; fast 49, 0/0)
AS4771 (n=95, 0/0; fast 88, 0/0)
AS6939 (n=175, 3/3; fast 53, 1/0)
AS17557 (n=80, 8/8; fast 32, 2/2)
AS45143 (n=66, 2/2; fast 60, 2/1)
AS62651 (n=53, 0/0; fast 40, 0/0)
AS393886 (n=106, 3/3; fast 103, 3/3)
AS132199 (n=89, 5/5; fast 70, 2/3)
AS34058 (n=53, 0/0; fast 39, 0/0)
AS6866 (n=87, 0/0; fast 39, 0/0)
AS10753 (n=248, 2/2; fast 221, 1/0)
AS25019 (n=108, 7/7; fast 60, 1/0)
AS213541 (n=1122, 5/7; fast 559, 1/3)
AS8473 (n=66, 1/2; fast 63, 0/2)
AS36925 (n=62, 3/4; fast 44, 0/0)
AS46261 (n=118, 0/2; fast 80, 0/0)
AS20012 (n=117, 1/3; fast 38, 0/1)
AS55577 (n=58, 0/1; fast 54, 0/0)
AS6871 (n=96, 8/10; fast 72, 4/6)
AS262287 (n=79, 2/4; fast 48, 1/2)
AS11798 (n=236, 12/21; fast 213, 9/16)
AS200373 (n=95, 2/6; fast 47, 0/1)
AS215373 (n=53, 0/3; fast 24, 0/0)
the rest: 8601 ASNs (n=192032, 20566/5552; fast 103014, 7498/1876)
all attempts
fastest resolved probe < 1000 ms
all validating: 7.9%
0
20
40
60
80
100
net breakage (%), 95% CI


all, n>=50: 375 ASNs
all 218608 attempts
fast <1000ms, n>=20: 349 ASNs
all 119741 attempts
134
55
61
125
43%
16%
7%
17%
16%
58
36
61
194
33%
8%
9%
33%
17%
0
20
40
60
80
100
validating ASNs by net breakage / standard error (no multiple-testing correction): share (%)
labels: number of ASNs on the ASN rows, share of attempts on the attempt rows
broken, >4σ
broken, 3-4σ
broken, 2-3σ
not broken at 2σ
excluded: ASN below n threshold

# Signing

# Support for signing with ML-DSA-44

- We are currently experimenting with online signing with ML-DSA-44
- It is too early to say when or how this will be available to customers
- It is possible we will find some customers have (e.g.) compliance reasons to use ML-DSA-44 and there may be demand to opt-in
- Deploying dual-sign 13/18 by default (for signed zones) on an opt-out basis would require high confidence that things will not break

# Domain Registry Allowlists

- An ML-DSA-44 KSK requires a DS RR in the parent zone with alg 18
  - For domains delegated from most TLD zones, this means EPP
    - <secDNS:dsData>[...]**<secDNS:alg>18</secDNS:alg>**[...]</secDNS:dsData>
- Although EPP is extensible (as it says on the tin) many/most/all registries constrain the allowable values of <secDNS:alg>
  - 3, 5, 6, 7, 8, 10, 12, 13, 14, 15, 16 is a common allowlist
  - There is a lot of variation
  - 18 is allowed by the latest CoCCA build, but nobody else
- This is a bit of a mess. We have an IANA registry for this. We could do better.
- This is also not PQ-specific. This is a problem for all new algorithms.
- draft-jabley-regext-allowable-dnssec-parameters

Are we there yet?

# We are not there yet

- Implement online signing with ML-DSA-44
- Standards actions (smash that wg like button)
  - draft-westerbaan-dnssec-mldsa
  - draft-jabley-dnsop-local-signing-algorithm-policy
  - draft-jabley-regext-allowable-dnssec-parameters
- Registry policy work
  - Identify ICANN communities who might be interested in this
  - Targeted outreach to individual back-end registry operators, ccTLD registry operators
- More experiments
  - More data
  - Radar all the things
- Targeted outreach to ASes where we see particularly interesting things

Thank you!