DNSSEC parameters for TLDs

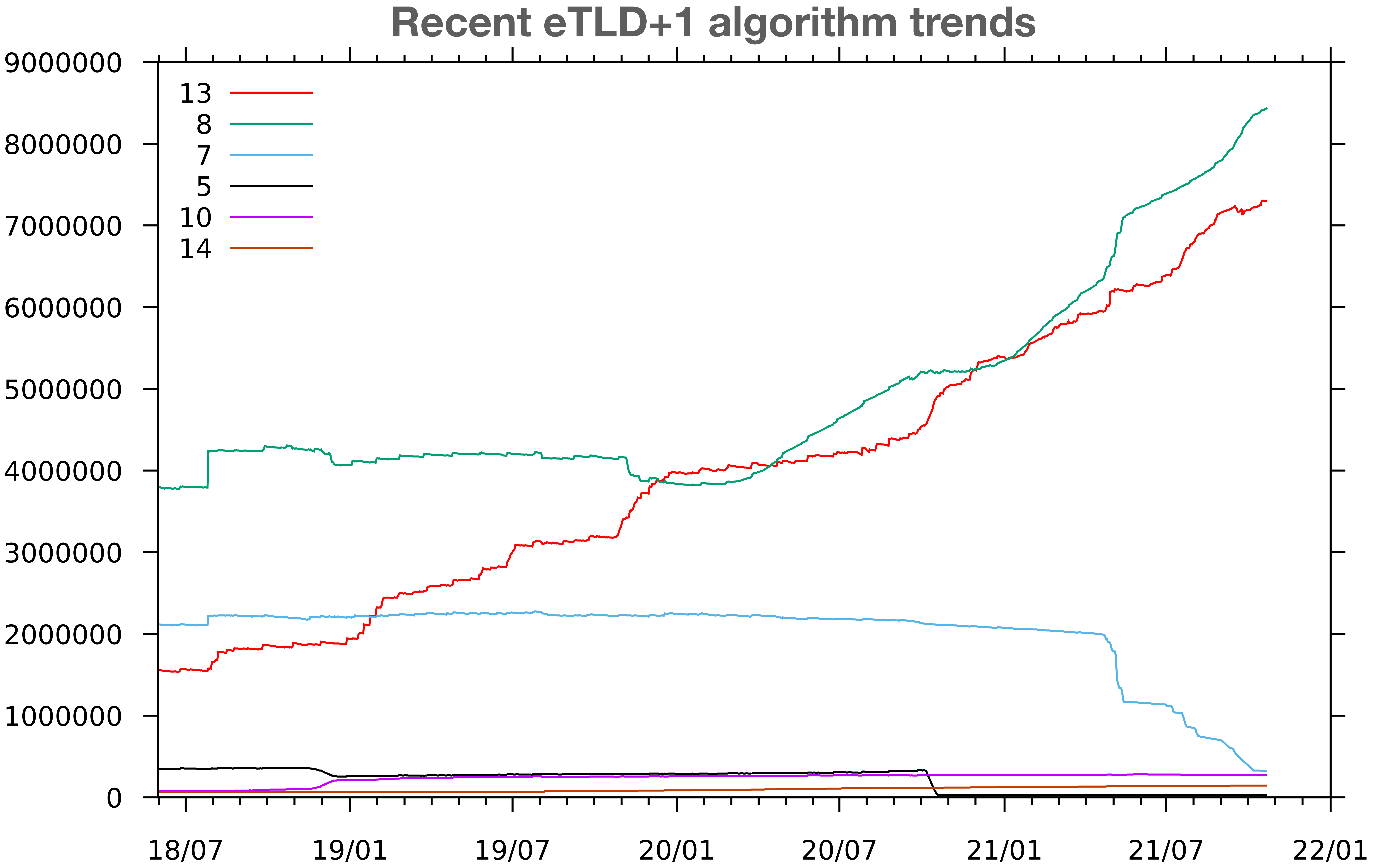
Operations and optics

Viktor Dukhovni & Wes Hardaker

DNSSEC algorithm requirements

https://datatracker.ietf.org/doc/html/rfc8624#section-3.1

- Deprecated Algorithms (https://www.dns.cam.ac.uk/news/2020-01-09-sha-mbles.html#content)
  - **RSASHA1**(5)
  - **RSASHA1-NSEC3-SHA1**(7)
- Mandatory to implement (MTI) algorithms for both signing and validation:
  - **RSASHA256**(8): Only MTI RSA algorithm
  - **ECDSAP256SHA256**(13): Only MTI EC algorithm
- Much progress has been made in eTLD+1 (effective TLD + 1 label) zones...



Recent eTLD+1 algorithm trends
13
8
7
5
10
14
9000000
8000000
7000000
6000000
5000000
4000000
3000000
2000000
1000000
0
18/07
19/01
19/07
20/01
20/07
21/01
21/07
22/01

TLD DNSKEY algorithms

- Algorithms 5 and 7 are deprecated
- 10 OK, but not widely used
- 13 is under-used by TLDs

DNSKEY algorithm	#TLDs
RSASHA1(5)	29
RSASHA1-NSEC3-SHA1(7)	38
RSASHA256(8)	1229
RSASHA512(10)	33
ECDSAP256SHA256(13)	45

TLD RSA key sizes: Room for improvement

- 1024-bits often criticised as weak by:
  - Broadly the WebPKI community,
  - Dan Bernstein & Tanja Lange (Curve 25519, EdDSA, ...)
    - Describe potentially efficient attacks on multiple RSA keys in parallel
- RSA-250 (829 bit) challenge factored in Feb 2020 (2700 core-years, Intel Xeon Gold 6130) or ~2^{67} clock cycles: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;dc42ccd1.2002
- The NIST formula for symmetric equivalent strength of RSA keys can be used to estimate ***upper bounds*** and **relative costs** of factoring large keys
  - (This cost estimate for RSA-250 is ~2^{72})

TLD KSK options

- Goldilocks RSA choice: 2048

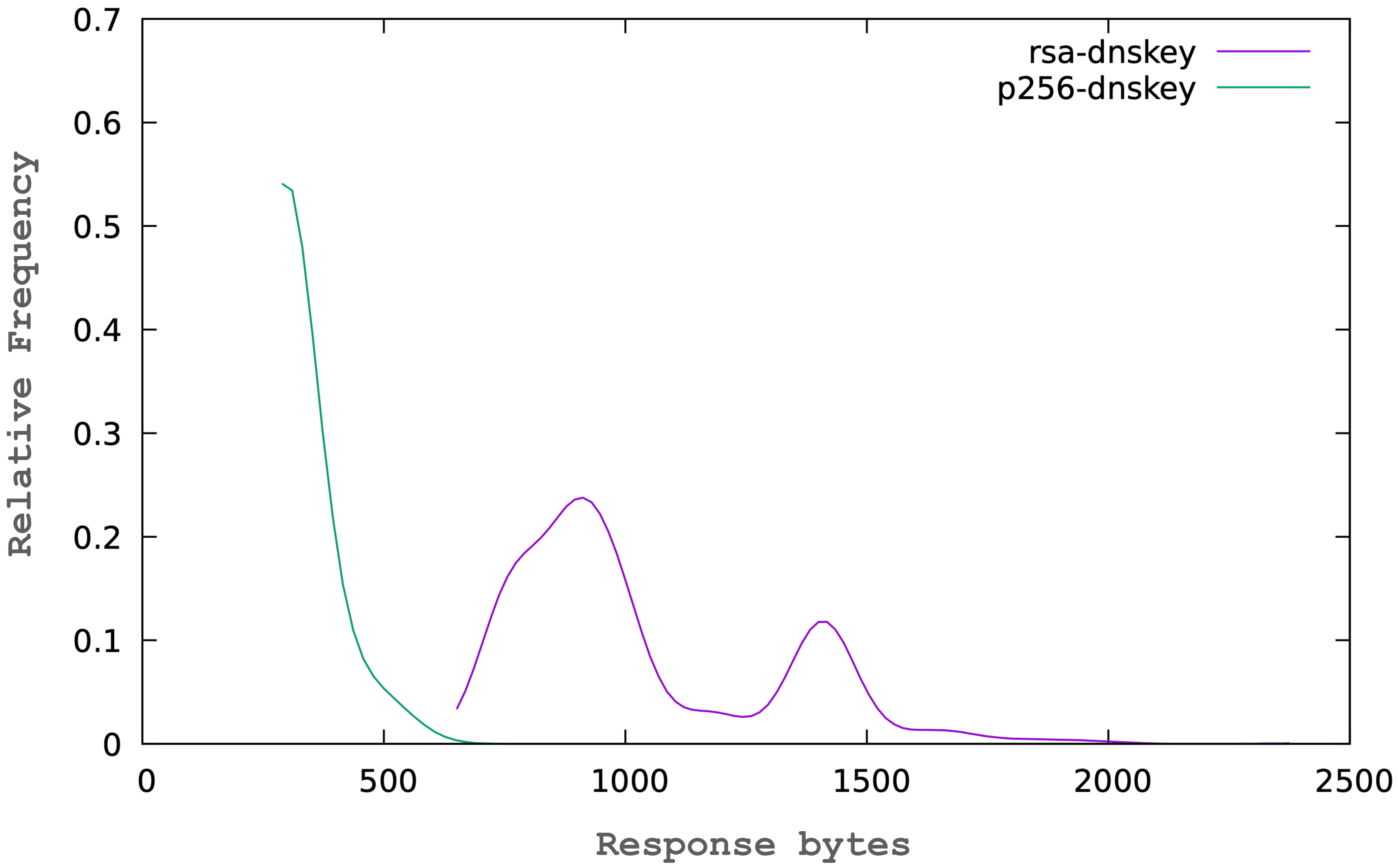
KSK size	#TLDs	Factoring cost $\log_2$	Factoring cost Million core-years (scaled RSA250)
RSA-1024	2	80	0.54
RSA-1280	–	89	240
RSA-1536	–	97	54000
RSA-2048	1300	110	Quantum Computer (QC)?
RSA-4096	23	150	QC?
ECDSA-P256	45	128	QC?

TLD ZSK options

- Goldilocks RSA choice: 1280 (with NSEC3), perhaps 1536 with NSEC?

ZSK size	#TLDs	Factoring cost bits	Factoring cost M-core years	Sigs/sec Skylake core	Verify/sec	NSEC3 size (median)	NSEC size (median)
RSA-1024	804	80	0.54	9400	147000	1043	714
RSA-1280	618	89	240	2600	83000	1207	–
RSA-1536	–	97	54000	2000	78500	–	–
RSA-2048	162	110	QC?	1400	48000	1554	1090
ECDSA-P256	45	128	QC?	38000	12500	769	494

TLD DNSKEY response size



If stuck for now with RSA

- **Upgrade** 1024-bit ZSKs to 1280 bits (or 1536 if using NSEC).
- **Switch** to algorithm 8 (RSASHA256), or 10, away from 5 or 7 (.am, .gr, .la, .pw)
- **Ensure** 2048-bit KSK, ***avoid*** 4096-bit KSKs.
- **Rotate** 1280-bit or less RSA ZSKs regularly, e.g. every ~90 days
  - 135 TLDs have at least one 1024-bit ZSK not changed since 2021-01-18
    - 16 of these are ccTLDs:
      - .uk, .ee, .vn, .cn, .gr, .vc, .hr, .ws, .az, .ky, .lk, .mc, .ax, .bw, .kg, .bt
  - 638 TLDs have all their 1024-bit ZSKs new since 2021-06-29 or later

Better still...

- Switch to **ECDSAP256SHA256** (algorithm 13)
  - Mandatory to implement and widely supported (no less than RSA!)
  - Smaller DNSKEY and NSEC/NSEC3 packets, faster signing
  - Keys as strong or better as WebPKI root CAs
- Consider **NSEC** instead of **NSEC3**
  - Especially for smaller largely static gTLD zones
- If sticking with NSEC3, keep iteration count low (ideally 0 and no opt-out)

  https://datatracker.ietf.org/doc/html/draft-hardaker-dnsop-nsec3-guidance-03