KSK Rollover Post-Analysis

Duane Wessels

ICANN 64 DNSSEC Workshop

VERISIGN®

KSK Rollover Schedule of Events

October 27, 2016	KSK-2017 generated in HSMs
July 11, 2017	KSK-2017 first appears in root zone; RFC 5011 begins
September 27, 2017	Rollover postponed
September 18, 2018	Rollover un-postponed
October 11, 2018	Rollover to KSK-2017 occurs
January 11, 2019	KSK-2010 revoked in root zone
March 22, 2019	KSK-2010 removed from root zone

What does the data show for these two events?

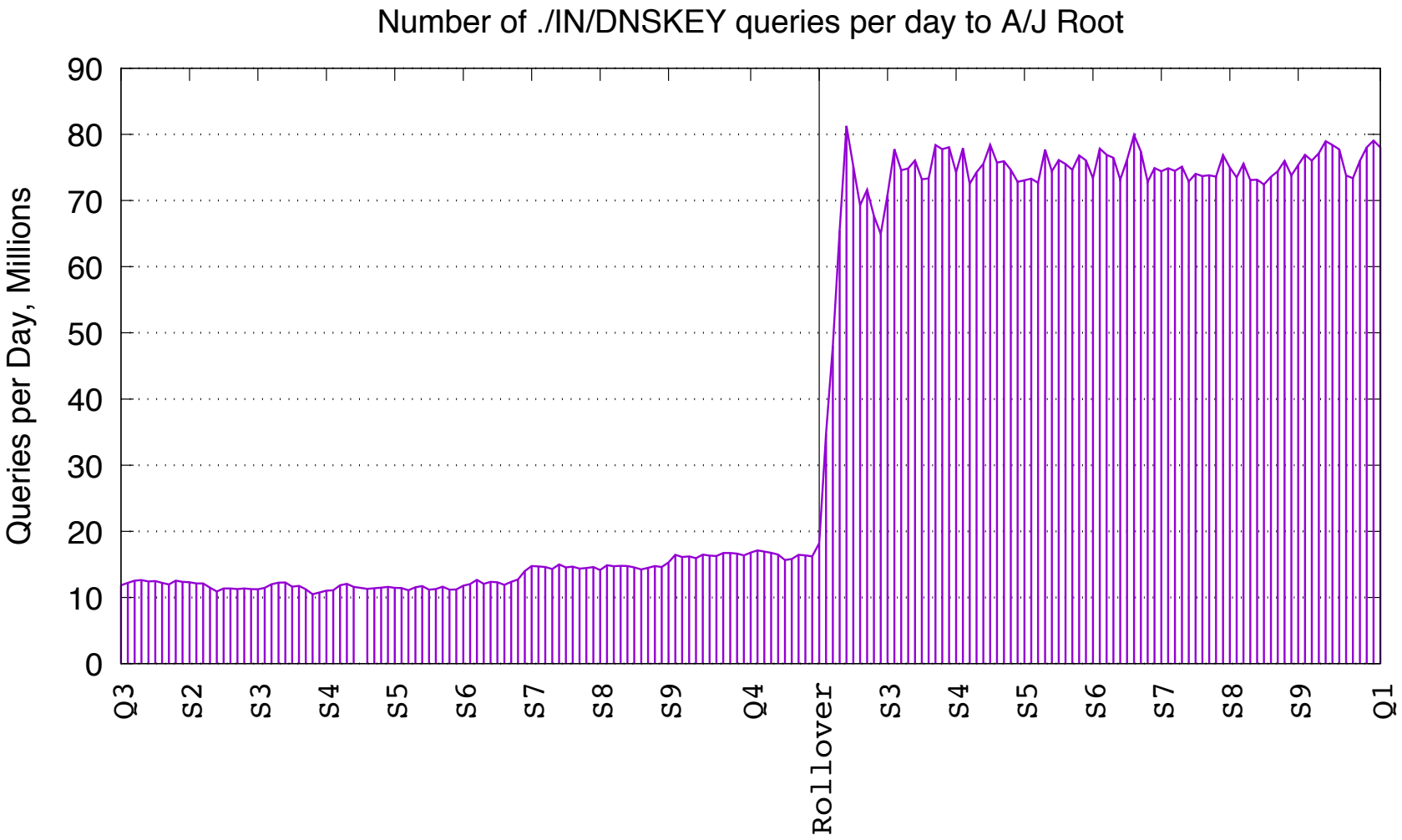
Data Sources

- DNS query traffic to Verisign root servers
- RFC 8145 key tag signals to Verisign root servers

./IN/DNSKEY Query Data

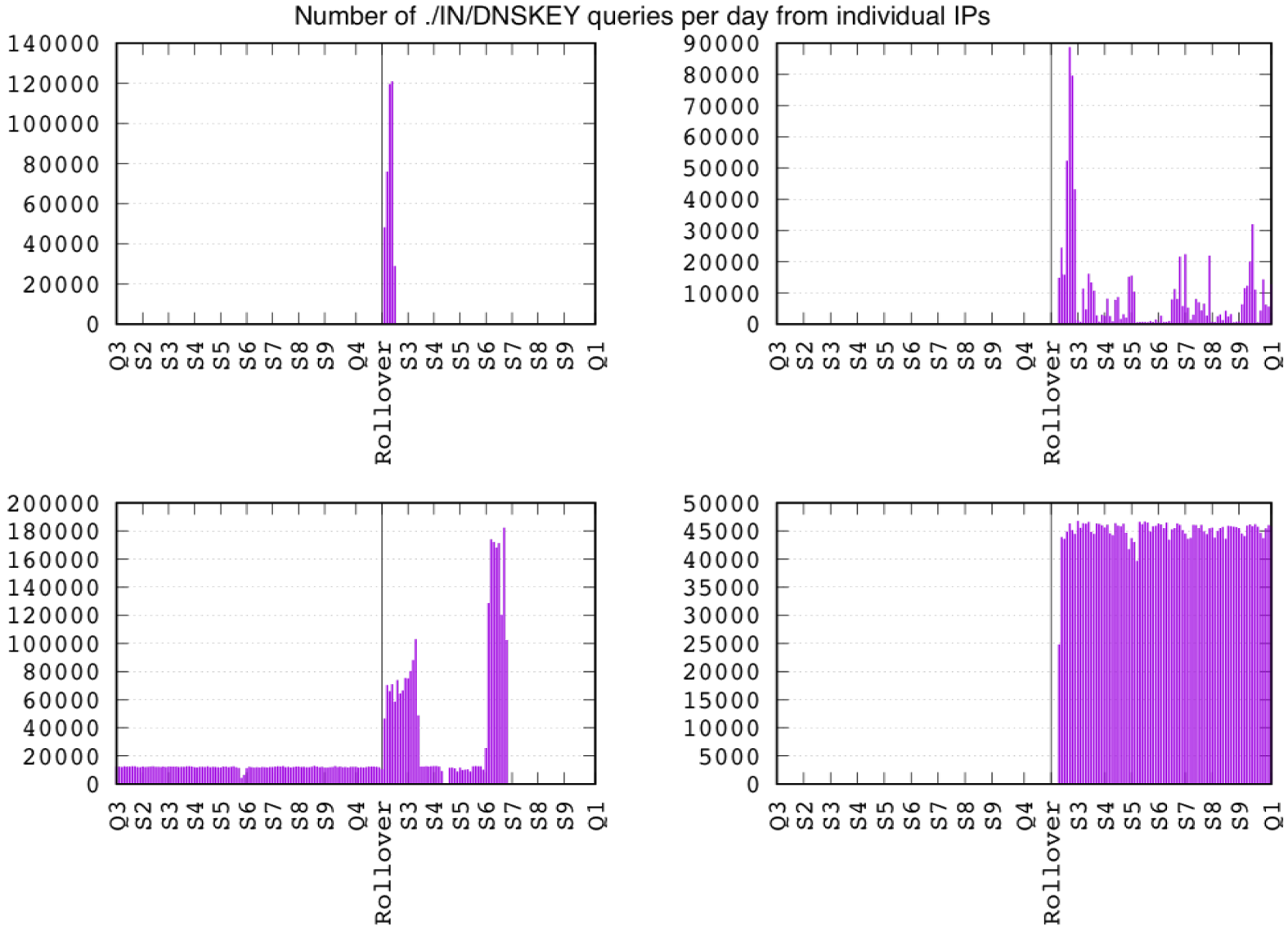
DNS queries for the root zone DNSKEYs

Change in DNSKEY queries at Rollover



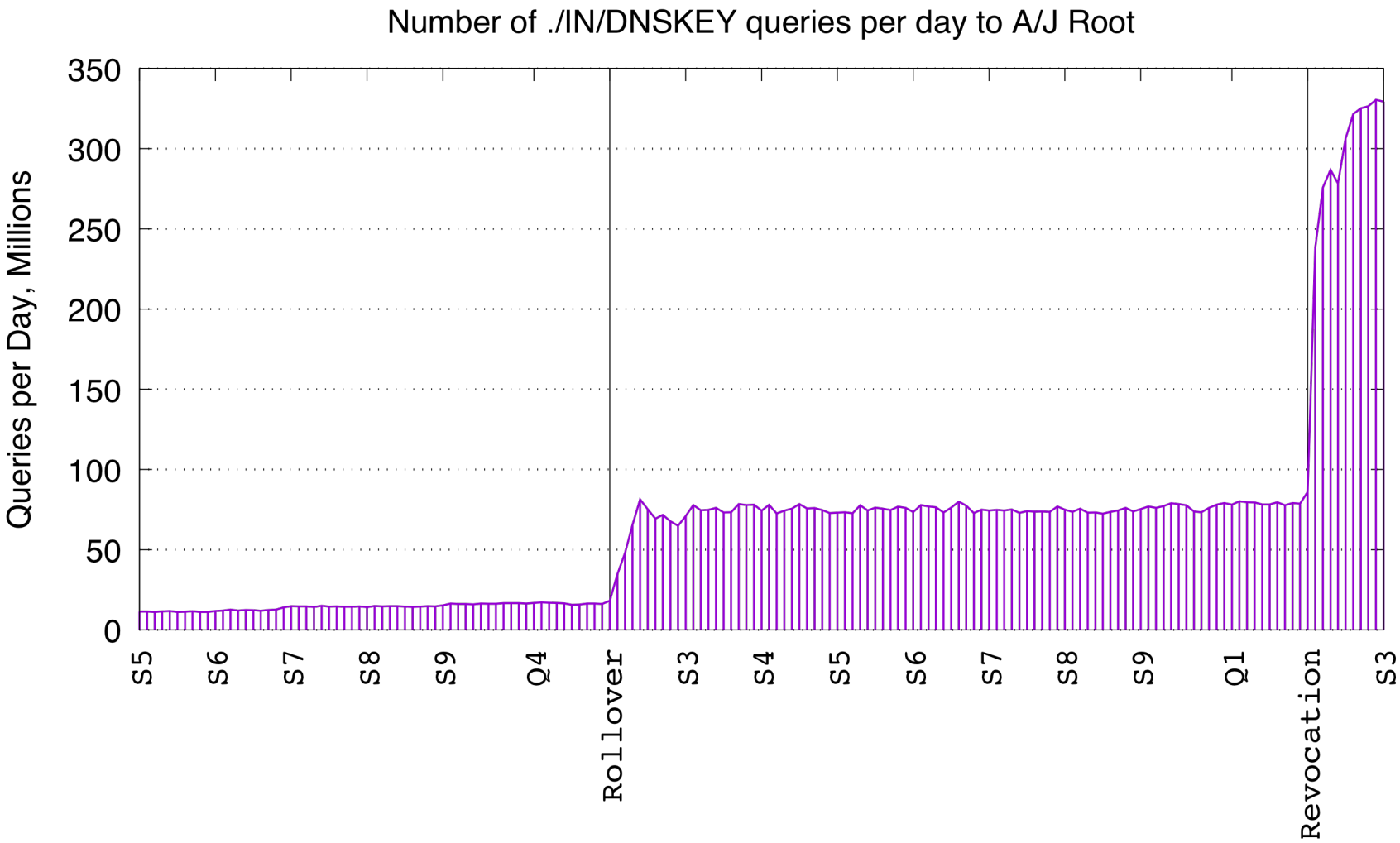
Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

Individual IPs have inconsistent behavior



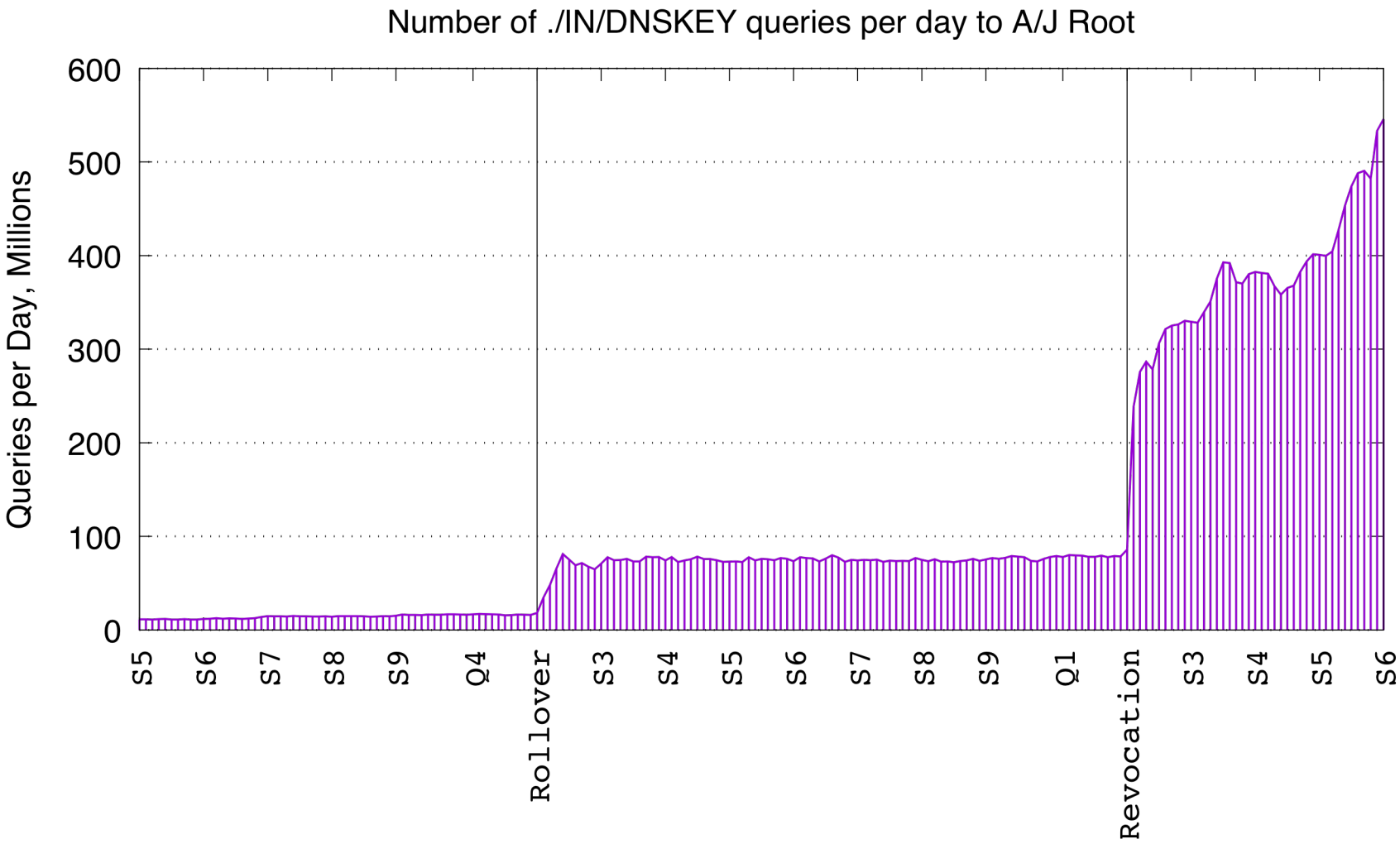
Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

Change in DNSKEY queries at Revocation



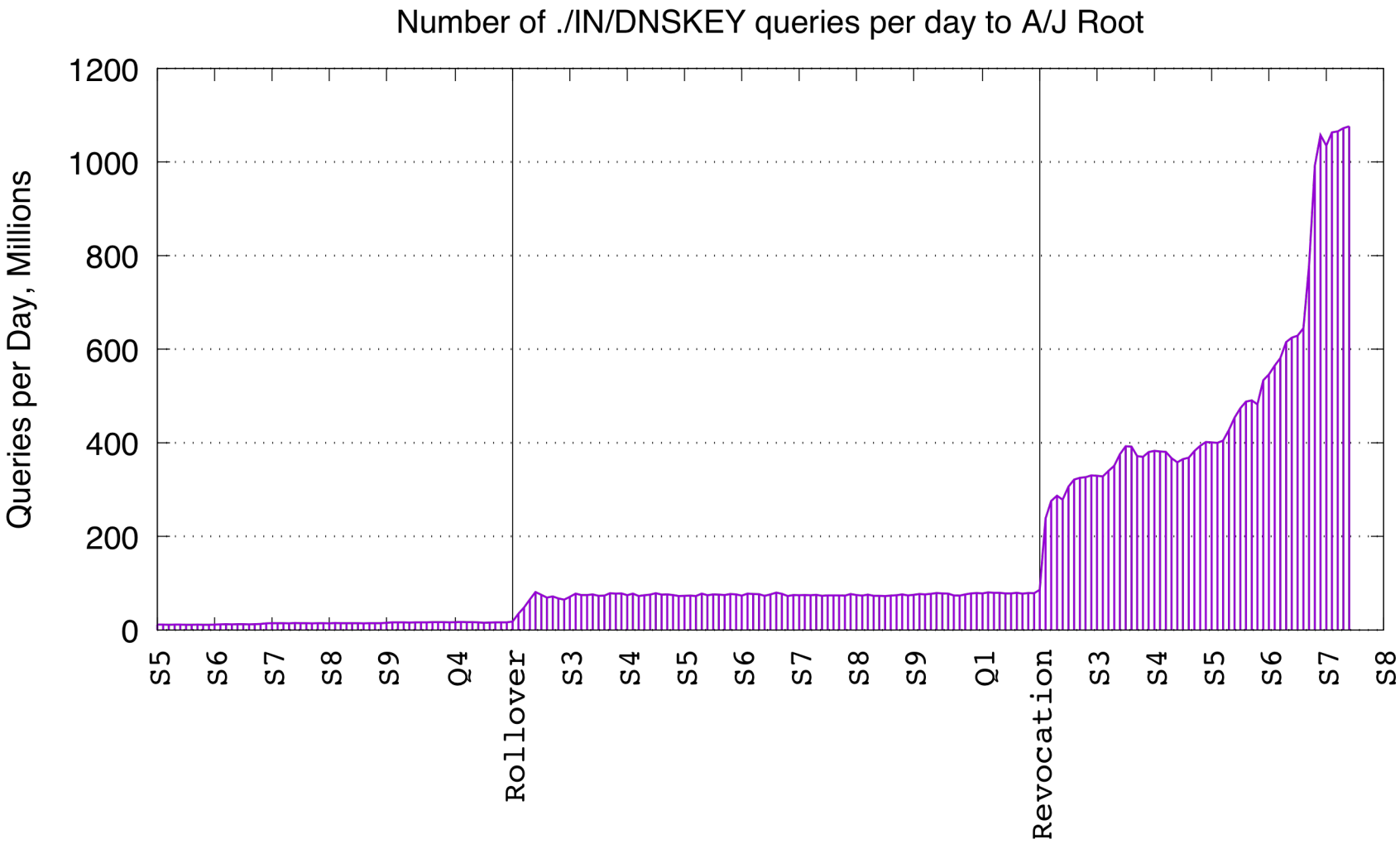
Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

Change in DNSKEY queries at Revocation



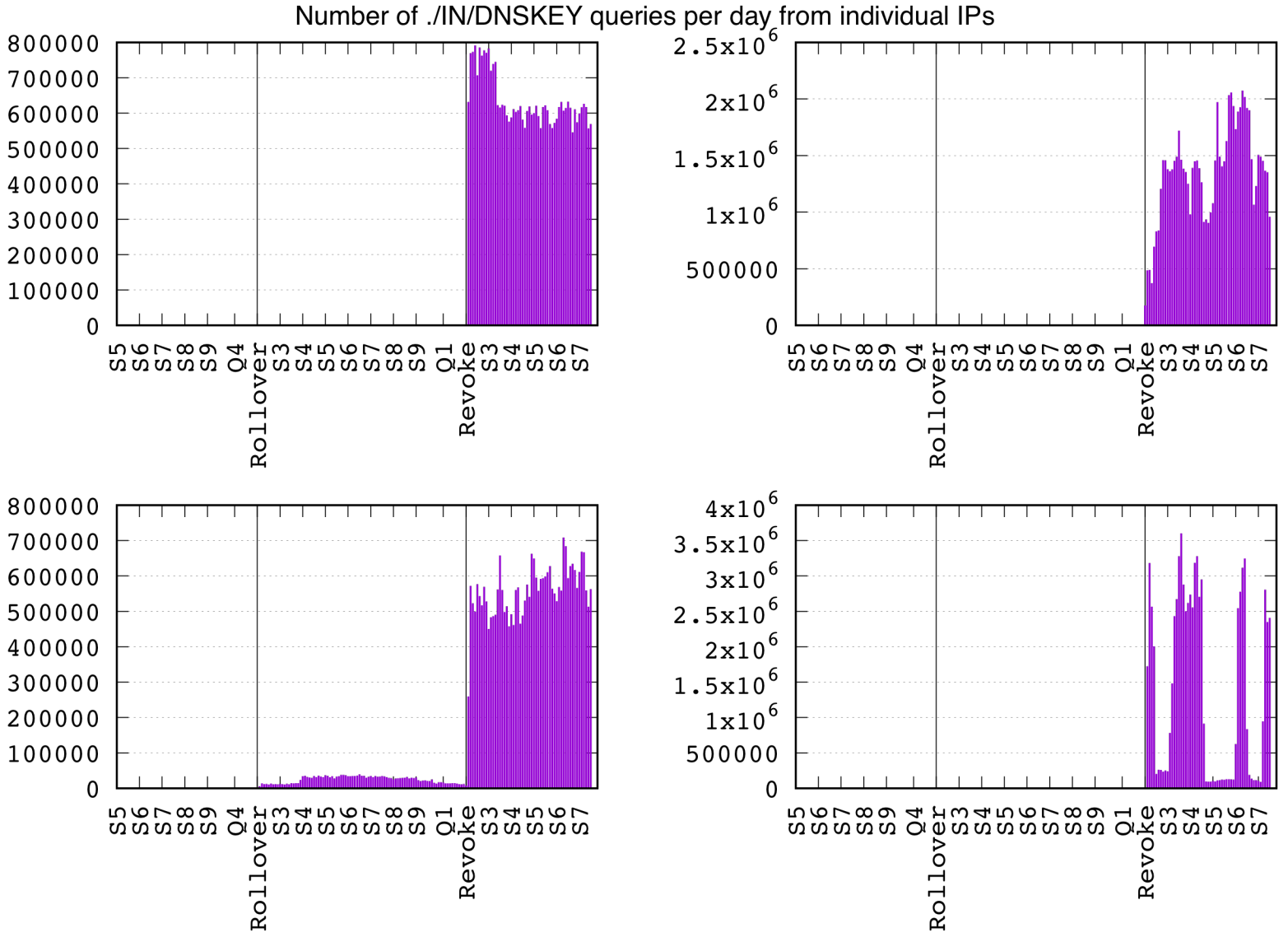
Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

Change in DNSKEY queries at Revocation



Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

Individual IPs have inconsistent behavior



Source: Verisign data; period spanning 2018 Q3 to 2019 Q1

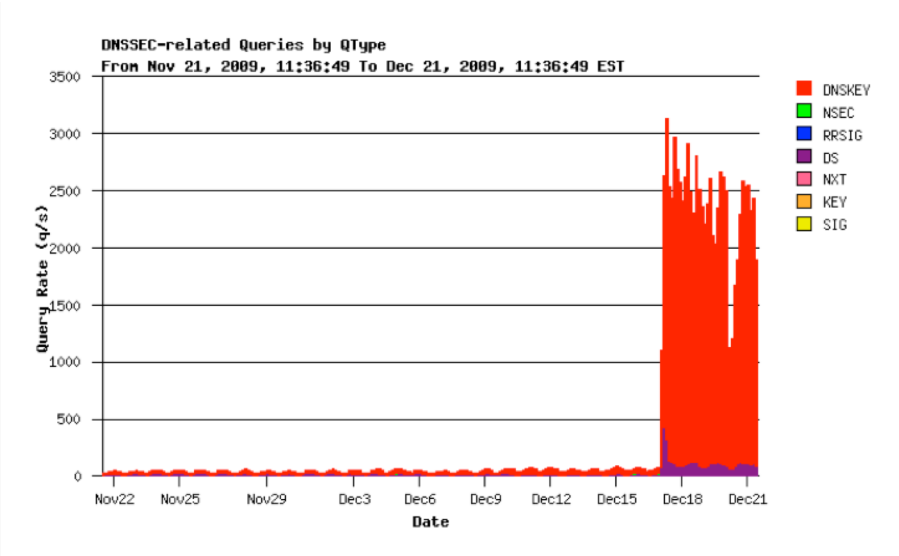
Isn’t this due to large responses carried by IPv6?

- ./IN/DNSKEY response is now 1425 bytes
- IPv6 minimum MTU is 1280 bytes

- This doesn’t look like “timeout-and-retry” behavior
- Seeing 10-100 queries per second from some sources
- Both v4 and v6
- It looks like “rollover-and-die”

Who remembers “Rollover and Die?”

- Key rollovers for in-addr.arpa zones maintained by RIPE
- Late 2009, root zone not yet signed
- Manual configuration of trust anchors in validators
- Old keys removed from zones Dec 16, 2009



- http://www.potaroo.net/ispcol/2010-02/rollover.html

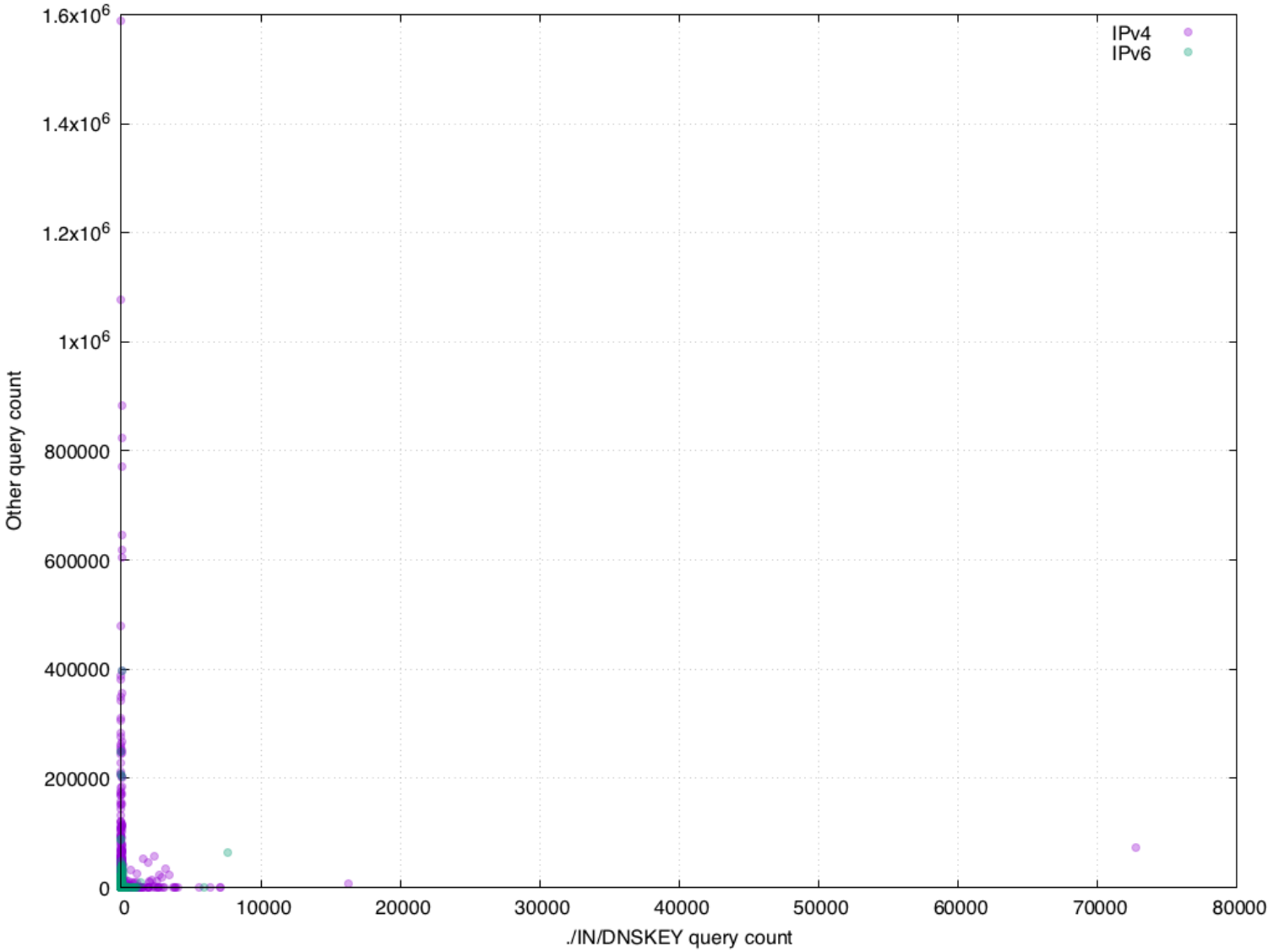
Exploring behavior of individual source IPs through visualization

How many “normal” queries do the high-rate DNSKEY sources make?

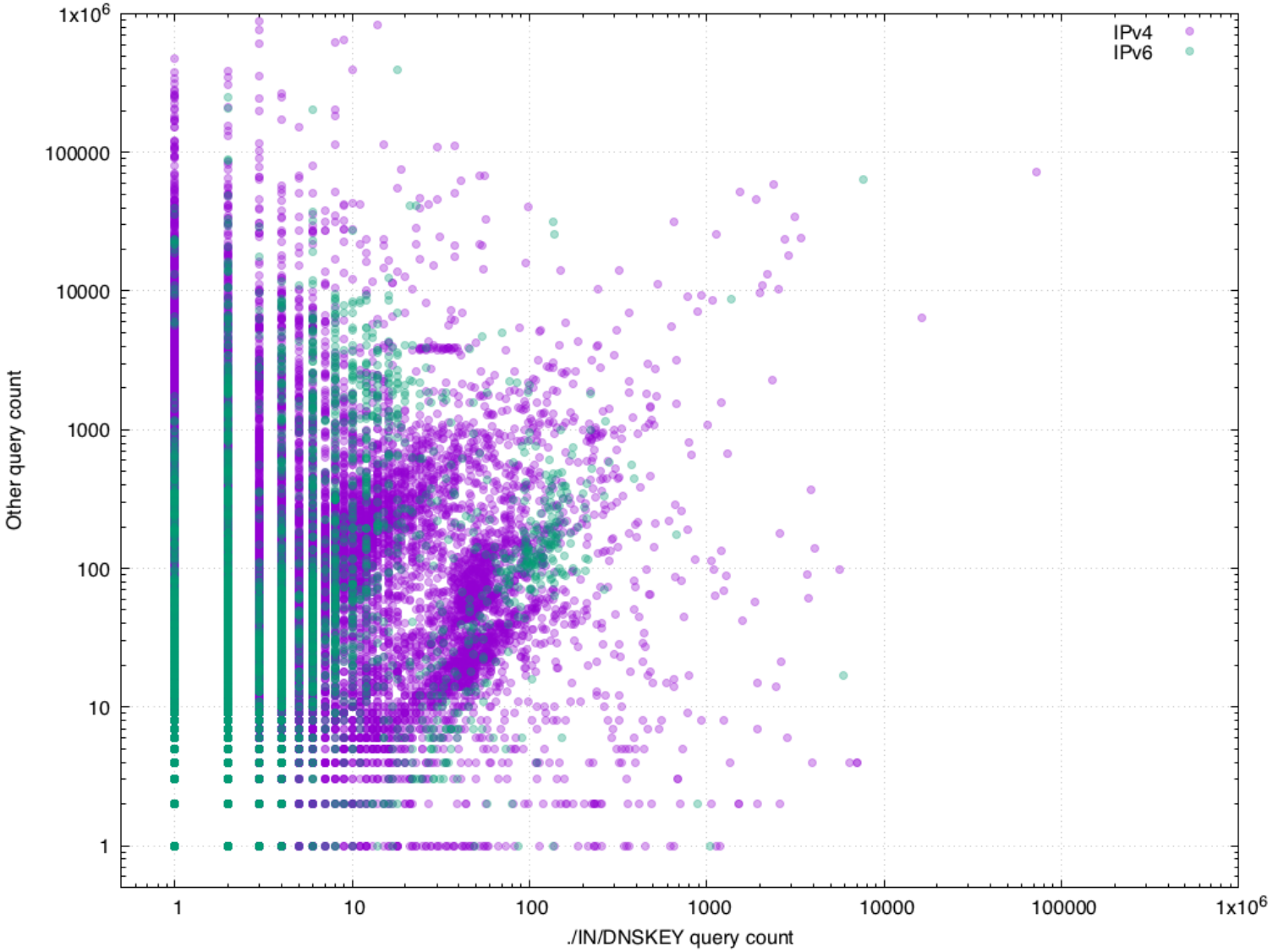
- Zero?
- A lot?

- Idea: scatter plot with count of DNSKEY queries on one axis and count of all others on other axis.

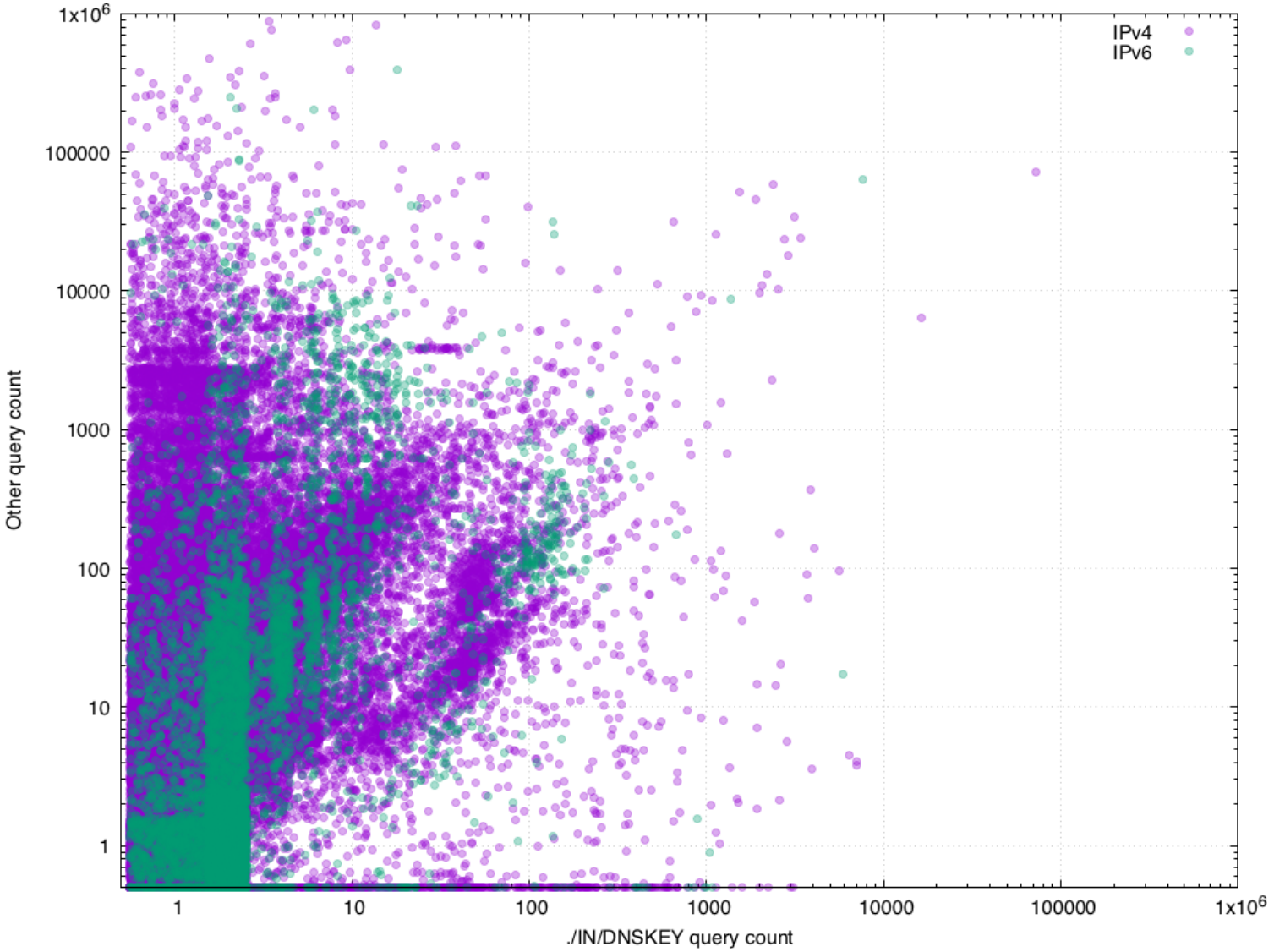
v1: Basic scatterplot



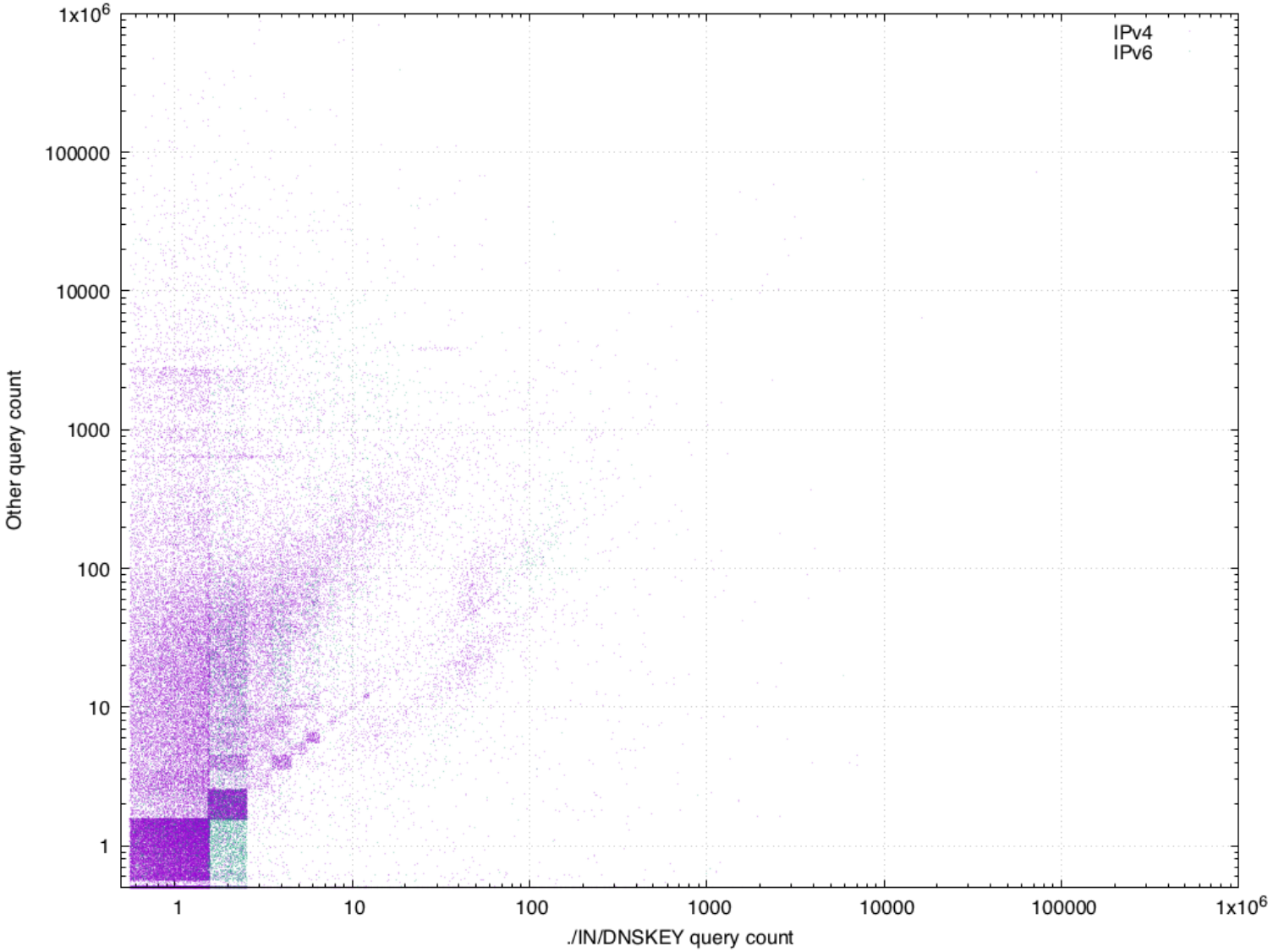
v2: Make axes logarithmic



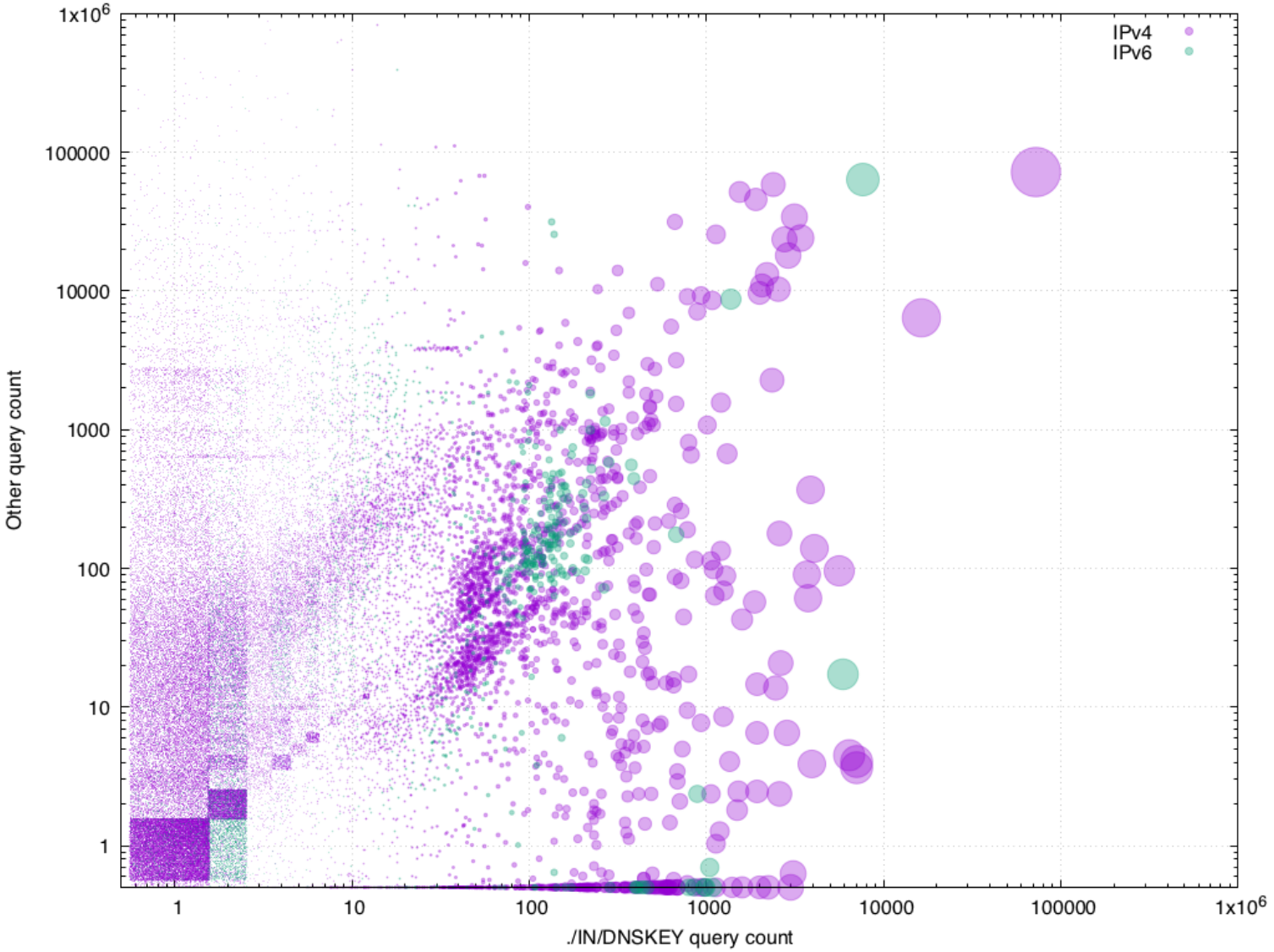
v3: Spread out the points



v4: Make points smaller?



v5: Make points variable size

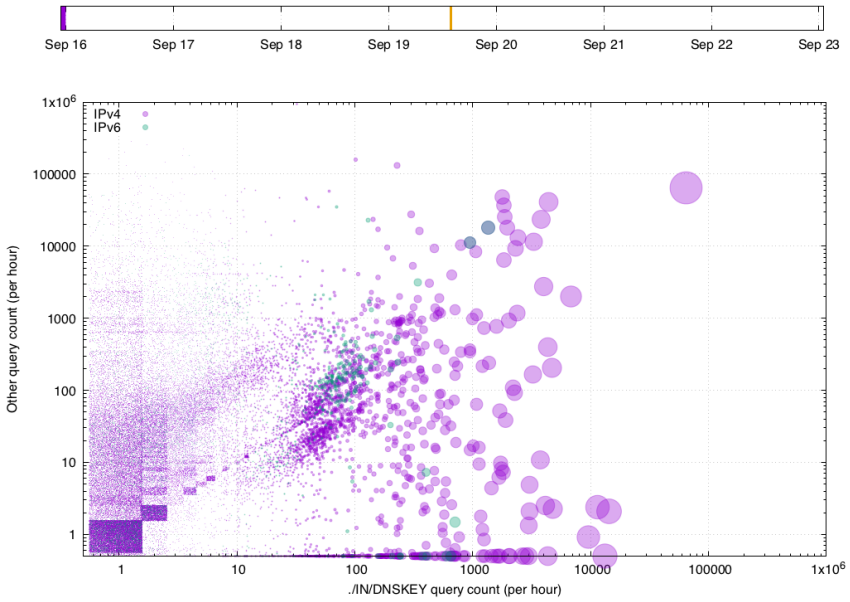


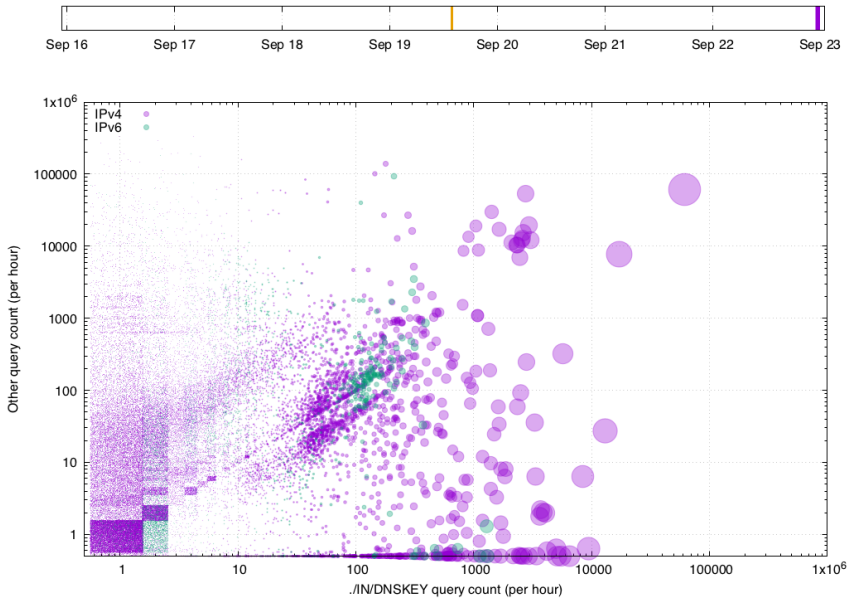
Visualization #1

During ZSK Rollover, September 2018

[placeholder for GIF animation of ZSK rollover event]

ZSK Rollover Before / After



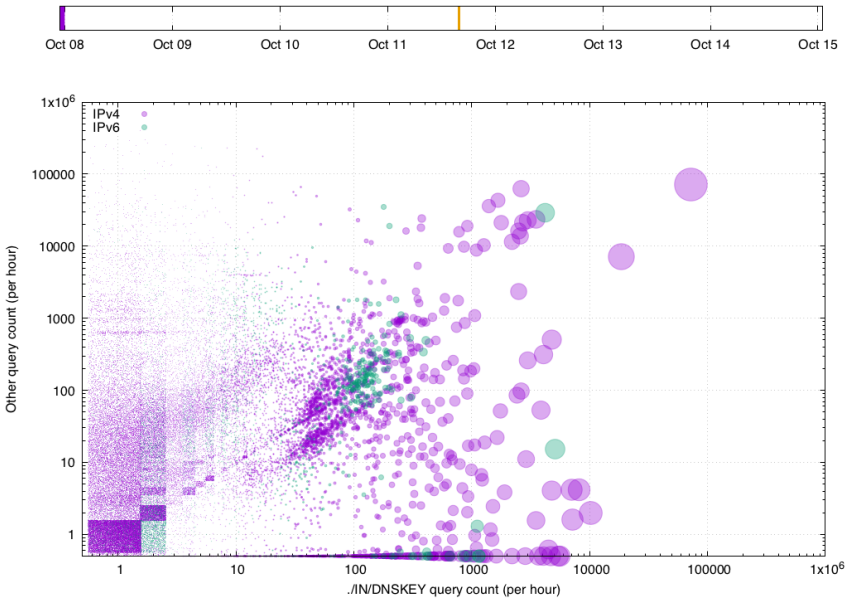


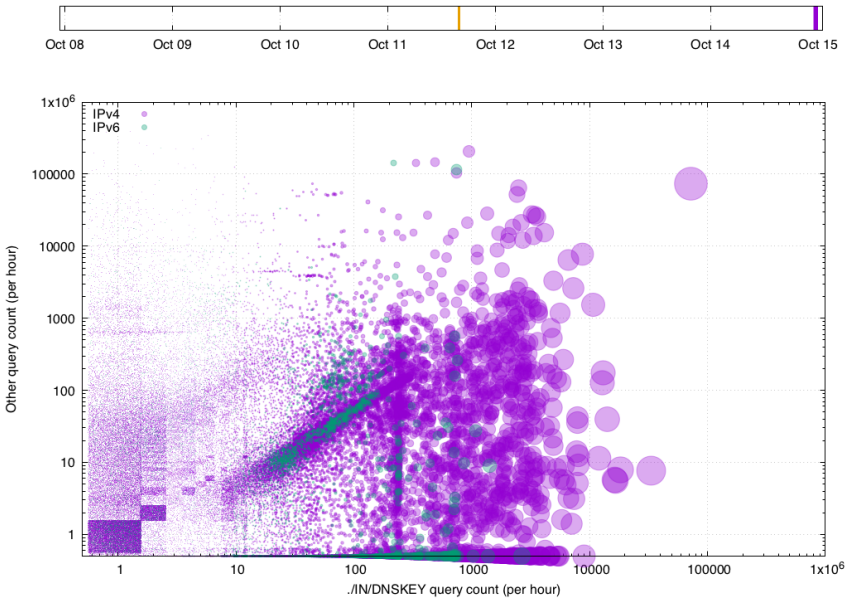
Visualization #2

During KSK Rollover, October 2018

[placeholder for GIF animation of KSK rollover event]

KSK Rollover Before / After



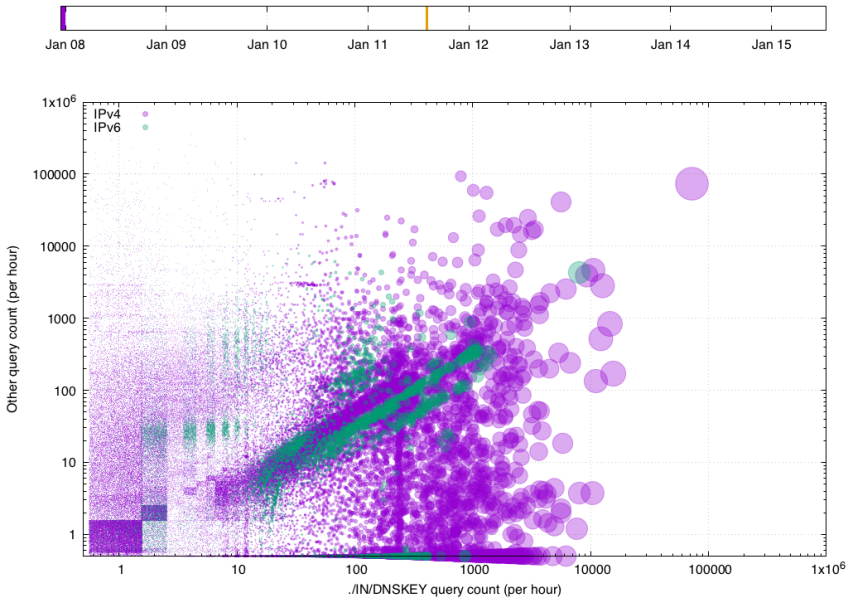


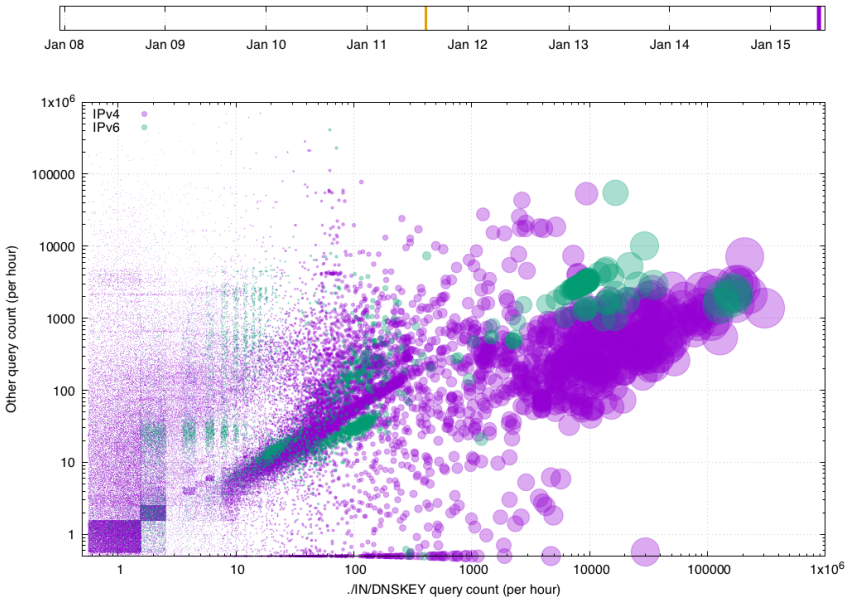
Visualization #3

During KSK Revocation, January 2019

[placeholder for GIF animation of KSK revocation event]

KSK Rollover Before / After



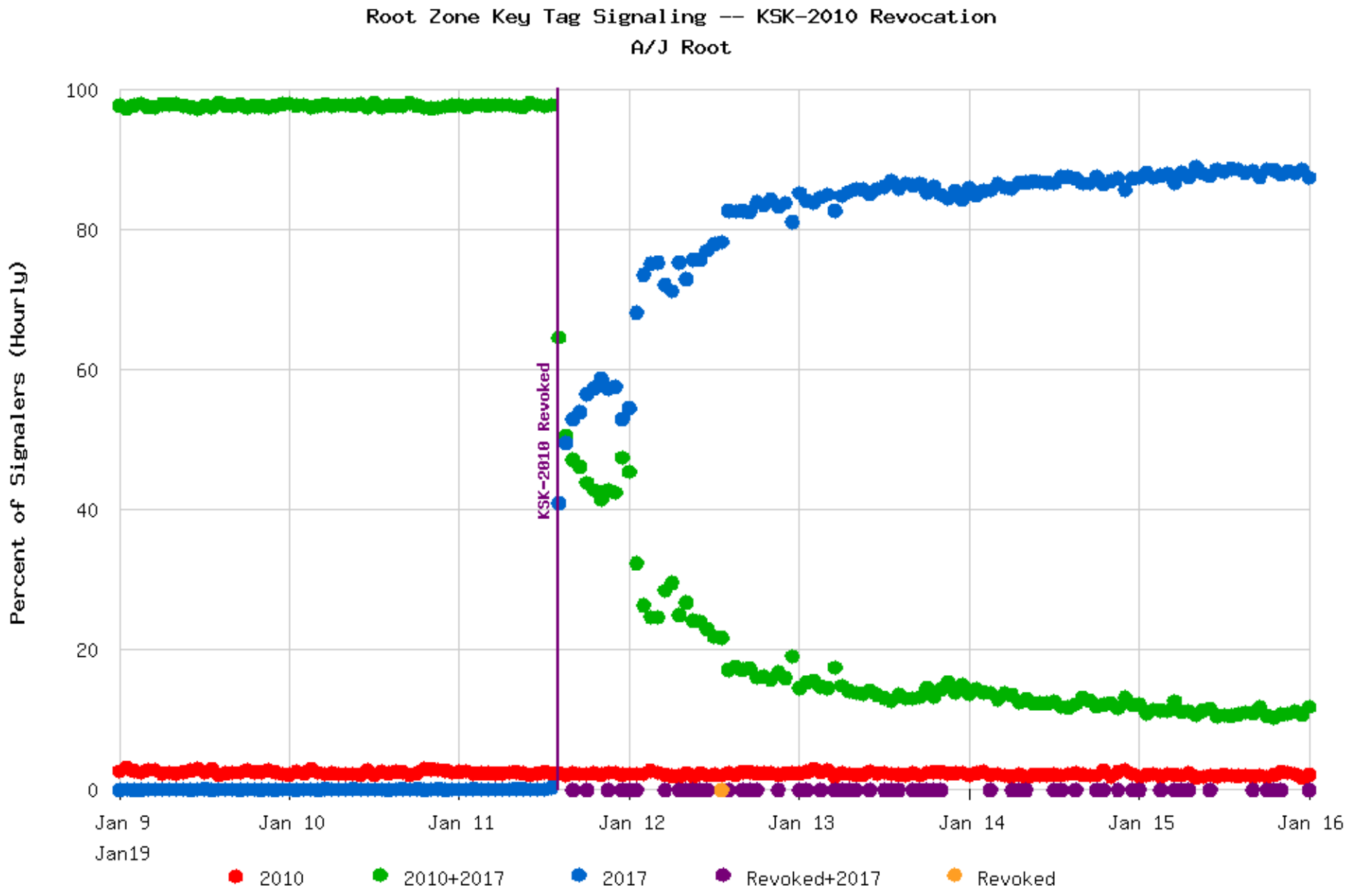


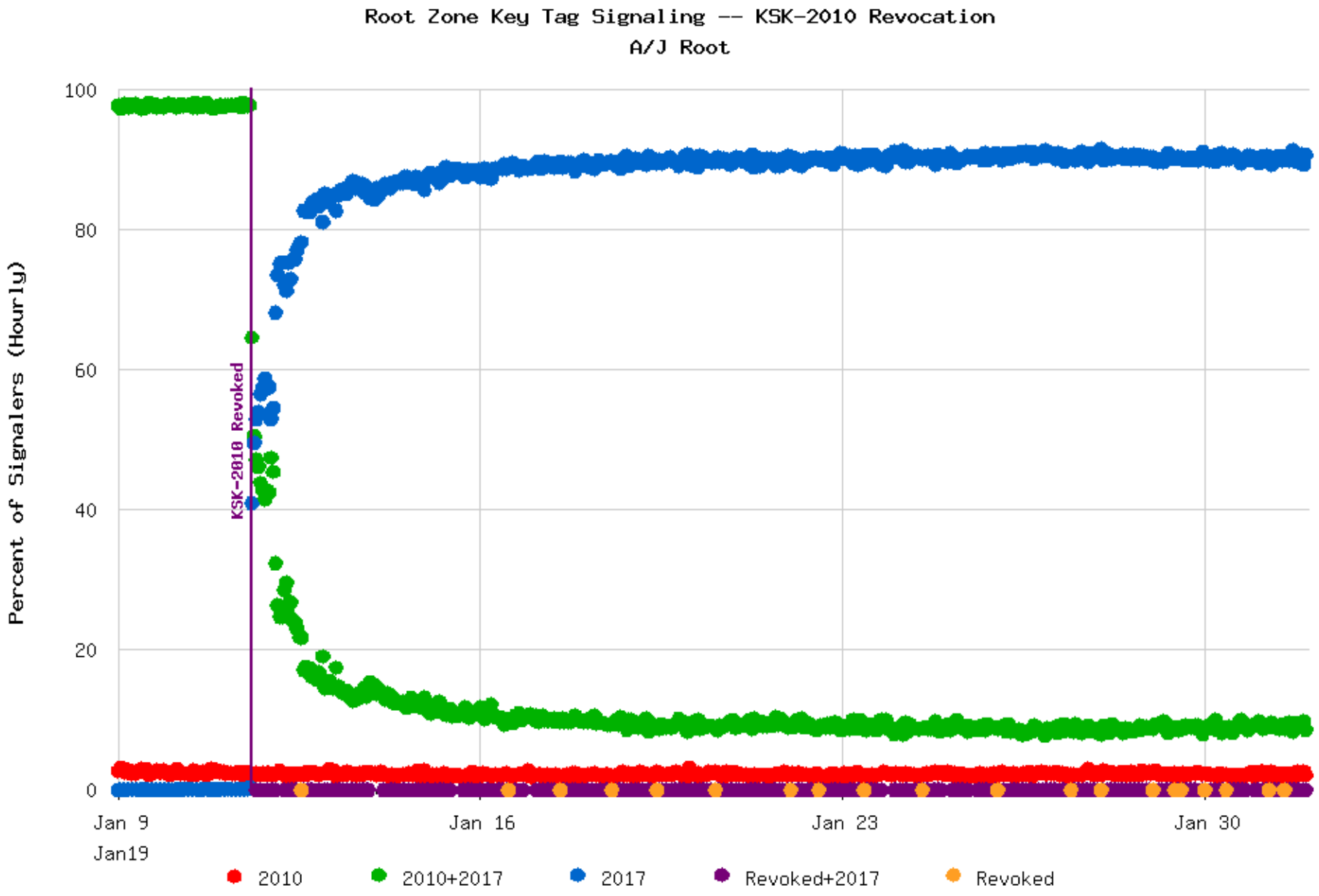
version.bind responses from top talker IPs

Version.bind	Count
9.8.4	71
9.8.1	41
9.10.3	34
9.11.3	30
9.8.2rc1	28
9.9.5	19
9.9.4	8
9.7.3	8
	8
BIND	6

Version.bind	Count
1.0.112	6
9.11.2	5
Dnsmasq	4
9.9.3	4
9.12.3	4
9.11.4	4
None	3
Get lost	3
[SECURED]	3
DNS server	3

RFC 8145 Key Tag Signaling Data

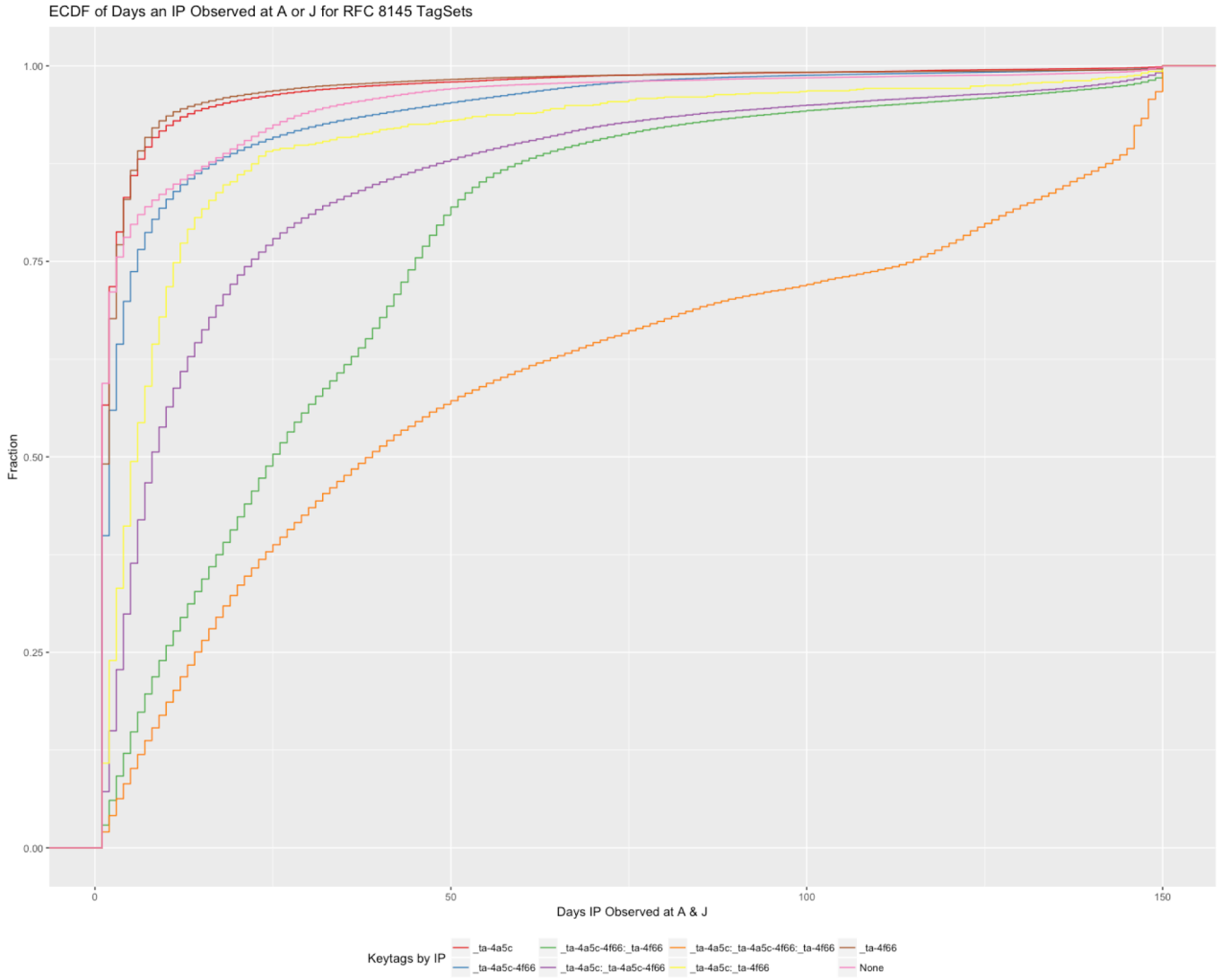

Root Zone Key Tag Signaling -- KSK-2010 Revocation
A/J Root
Percent of Signalers (Hourly)
100
80
60
40
20
0
KSK-2010 Revoked
Jan 9
Jan19
Jan 10
Jan 11
Jan 12
Jan 13
Jan 14
Jan 15
Jan 16
2010
2010+2017
2017
Revoked+2017
Revoked


Root Zone Key Tag Signaling -- KSK-2010 Revocation
A/J Root
Percent of Signalers (Hourly)
100
80
60
40
20
0
KSK-2010 Revoked
Jan 9
Jan19
Jan 16
Jan 23
Jan 30
2010
2010+2017
2017
Revoked+2017
Revoked

Trust Anchor signals at Revocation

- Many signalers removed revoked key very quickly
- But many still holding on to KSK-2010?
  - i.e, did not cross down to zero within 48 hour TTL
- Signalers with only KSK-2010 unchanged by revocation
  - As expected, they're probably manually configured and not doing RFC 5011

Combined ./IN/DNSKEY top talkers with 8145 signalers



VERISIGN®