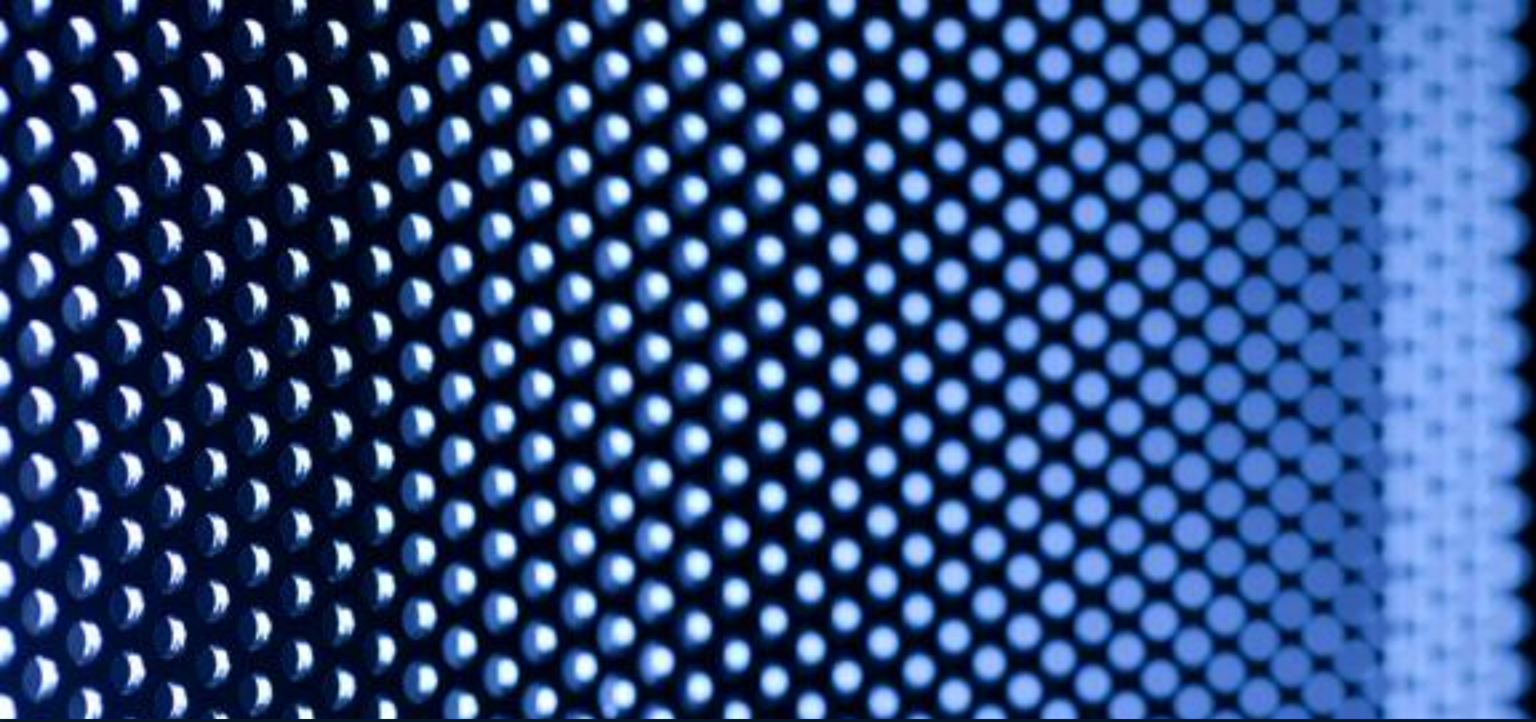


A Multi-Perspective Analysis of the Root KSK rollover

Duane Wessels

30th DNS-OARC Workshop, Bangkok

May 13, 2019

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 three events?

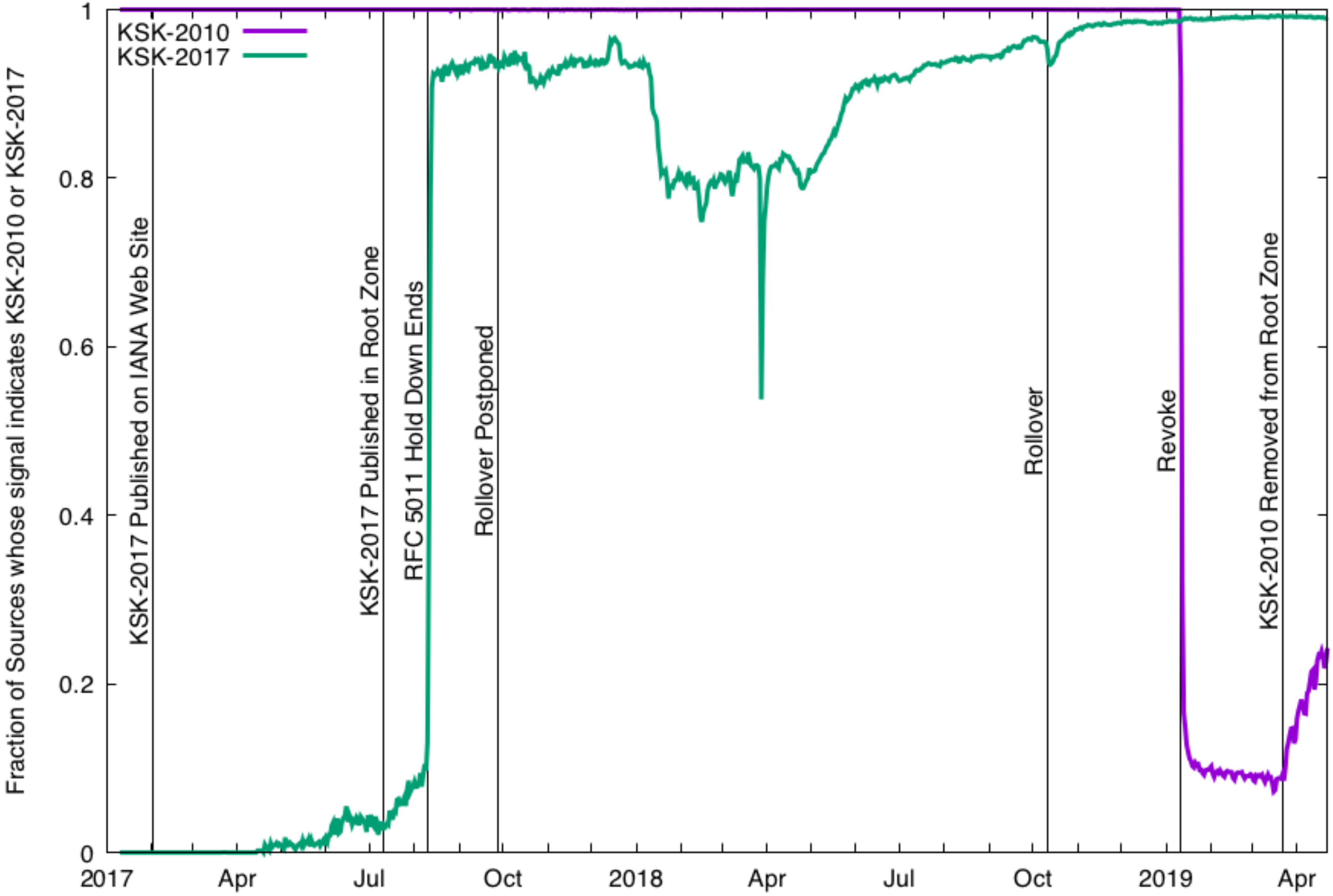
RFC 8145 Data

About RFC 8145

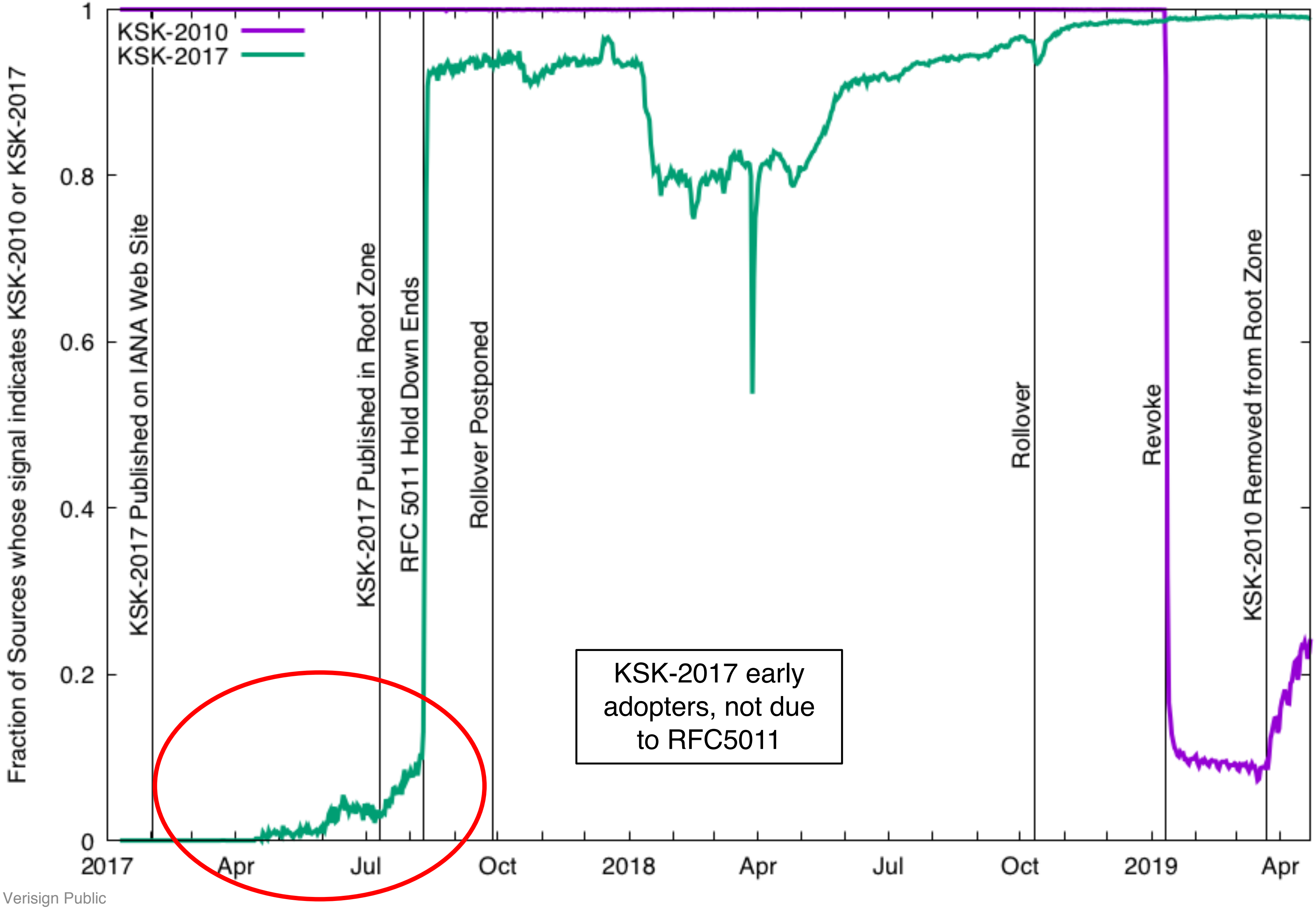
- First Internet-Draft: December 2015
- First implementation: July 2016
- First known signals: January 2017
- RFC: April 2017

- What does 2+ years of 8145 data show us?
  - The percentage of signal sources that report having KSK-2010
  - The percentage of signal sources that report having KSK-2017

RFC 8145 Long Term Data

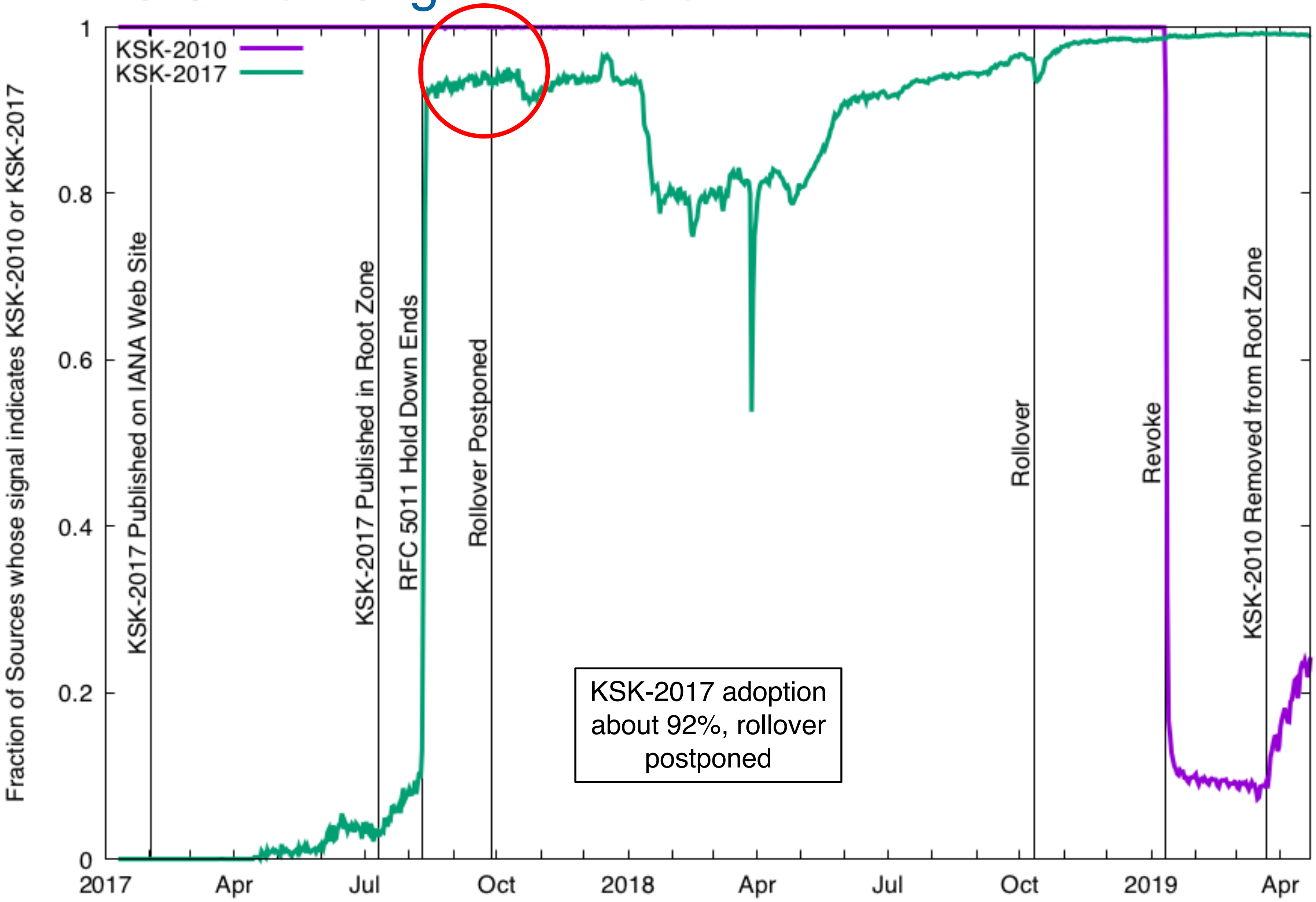


RFC 8145 Long Term Data



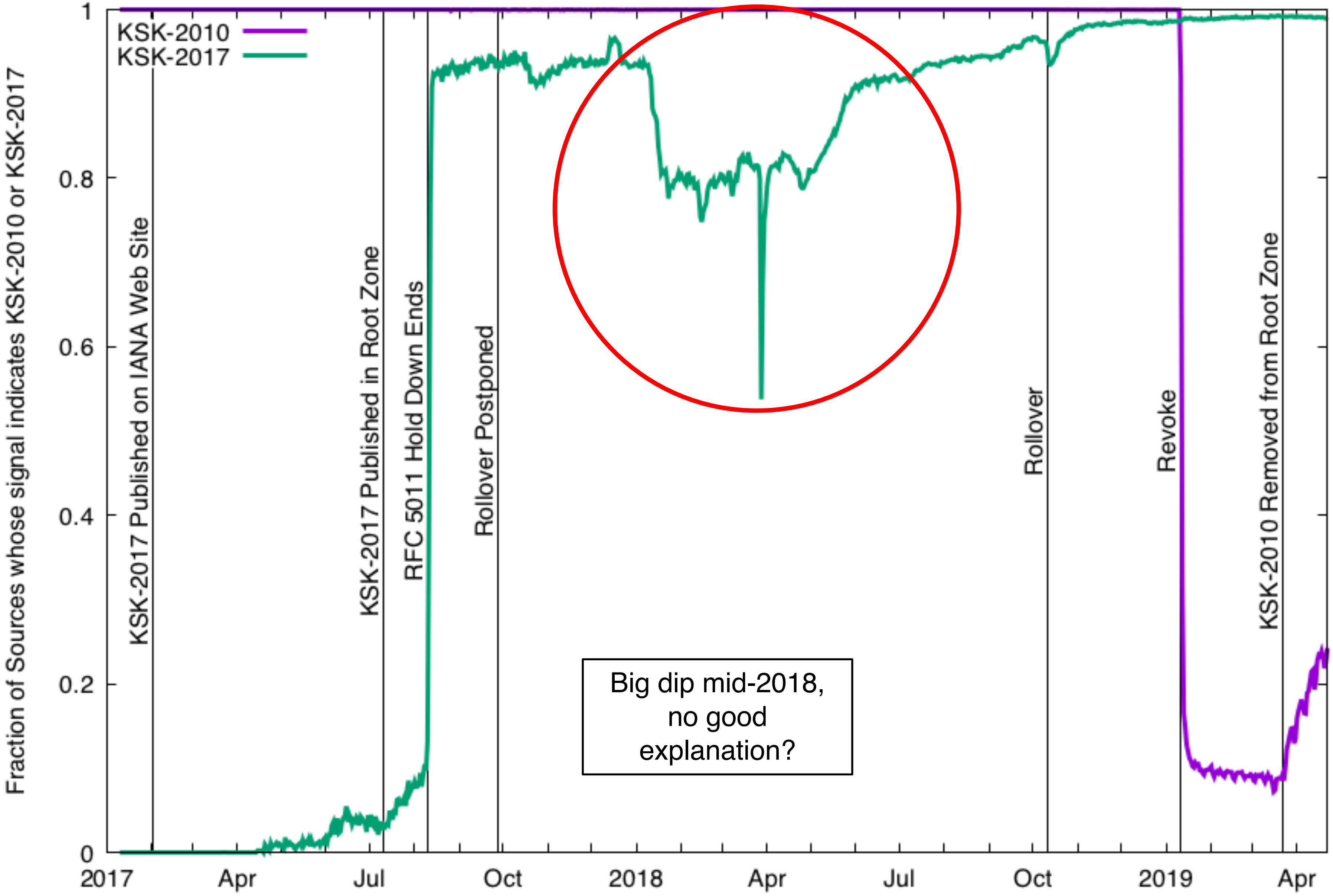
KSK-2017 early adopters, not due to RFC5011

RFC 8145 Long Term Data



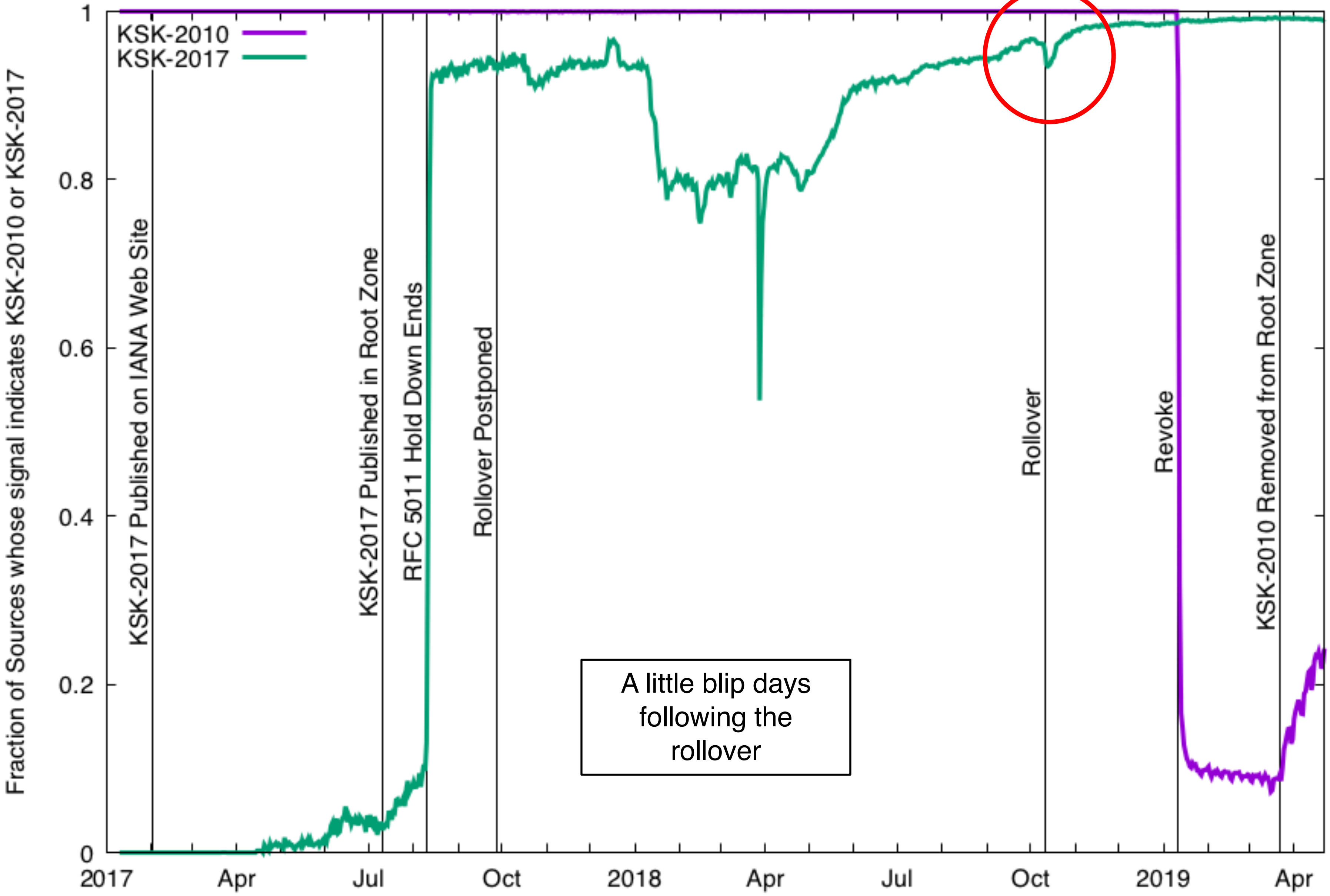
KSK-2017 adoption about 92%, rollover postponed

RFC 8145 Long Term Data



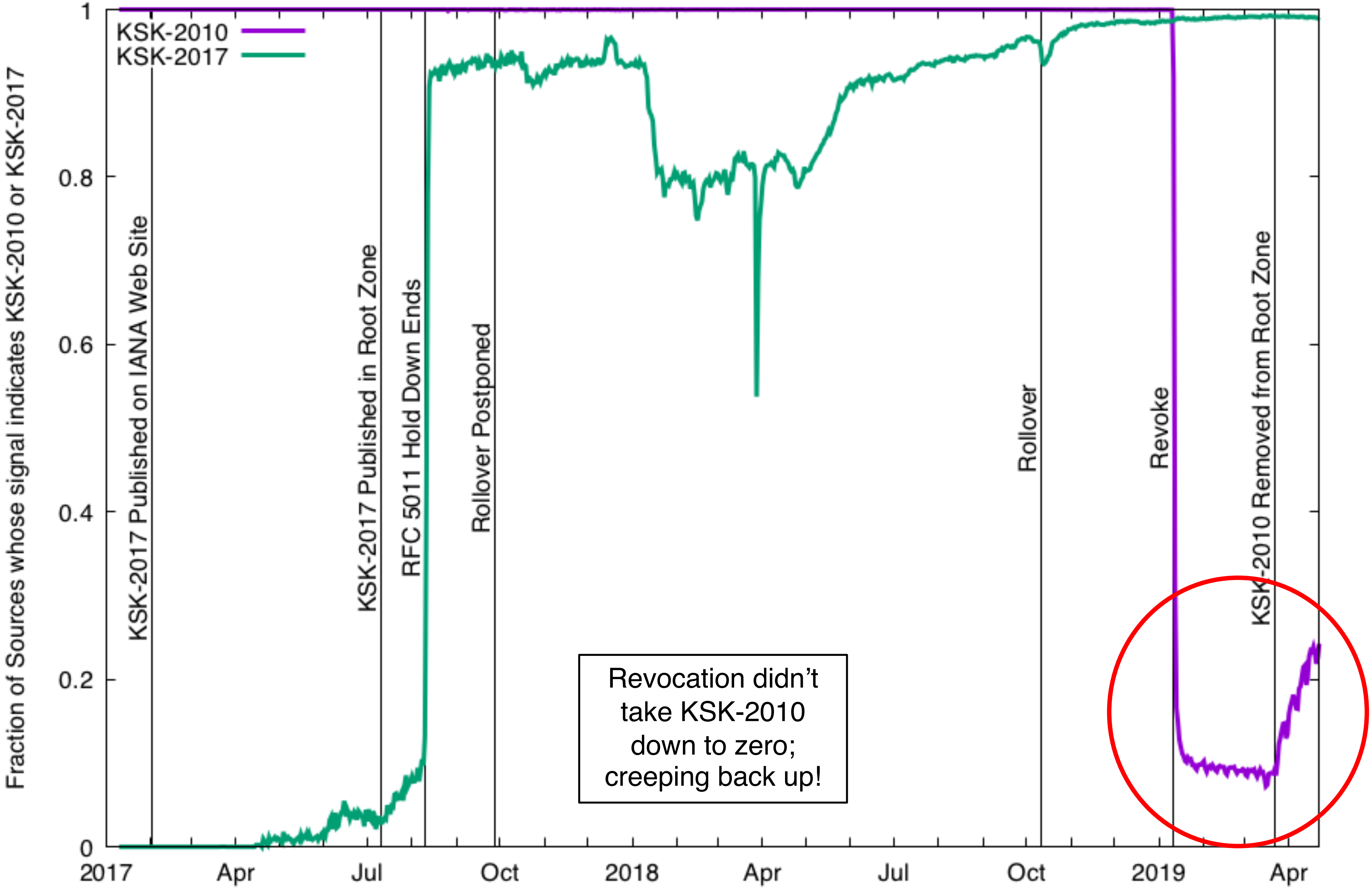
Big dip mid-2018, no good explanation?

RFC 8145 Long Term Data



A little blip days following the rollover

RFC 8145 Long Term Data



Revocation didn't take KSK-2010 down to zero; creeping back up!

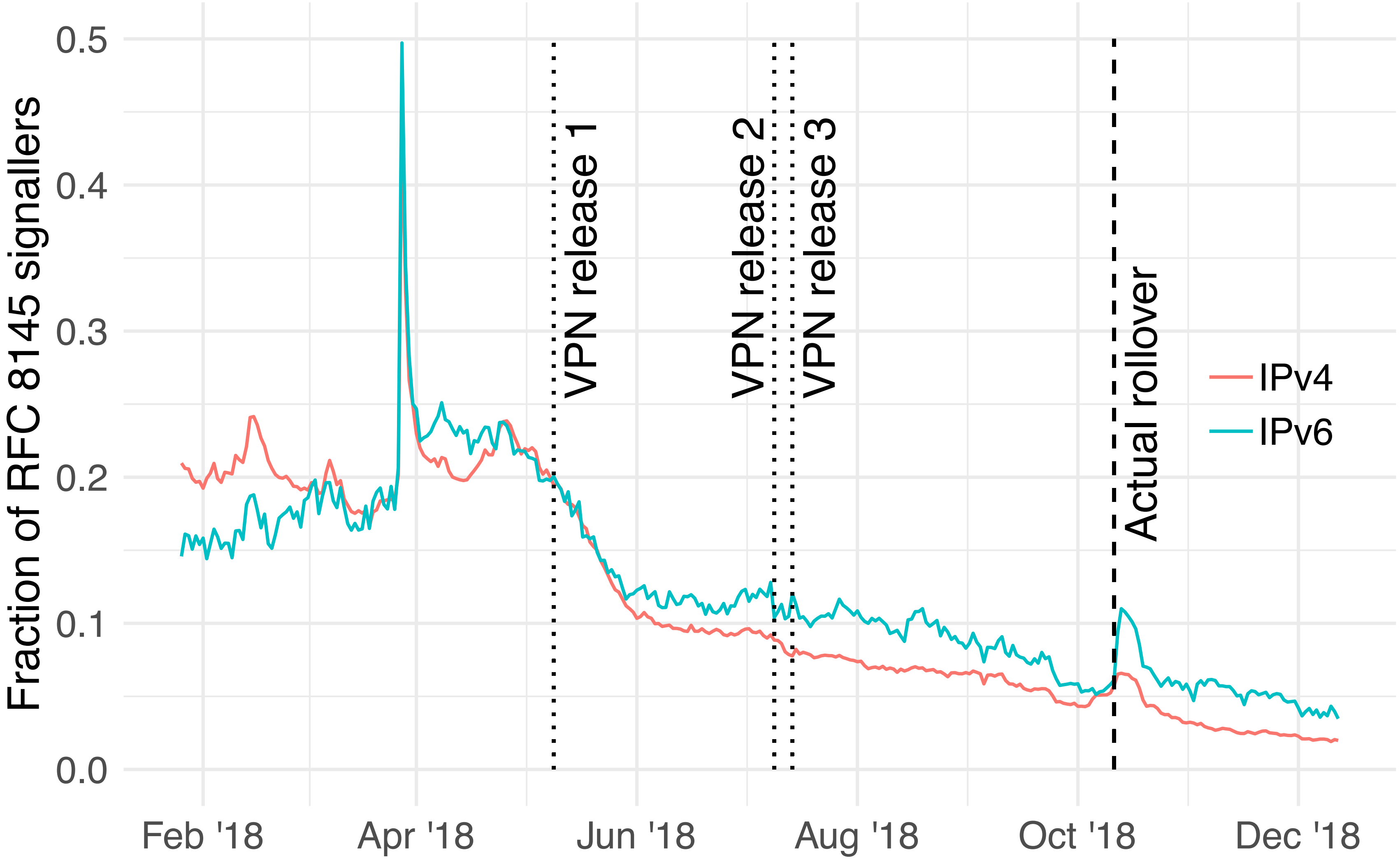
VPN Provider Software sourcing 8145 Signals

- Noticed a lot of 8145 sources (16,403) sending just one signal
  - likely dynamic address assignment
- Further noticed many of these sources (6,702) send only a small number of DNS queries to root at the same time

Query	Count
_ta-4a5c	15,447
.	9,182
VPN domain	3,156
VPN alternate domain	415
_sip._udp.otherdomain	86

- Outreach confirmed that this smartphone VPN software was using libunbound and a hard-coded trust anchor.

VPN software updates through 2018

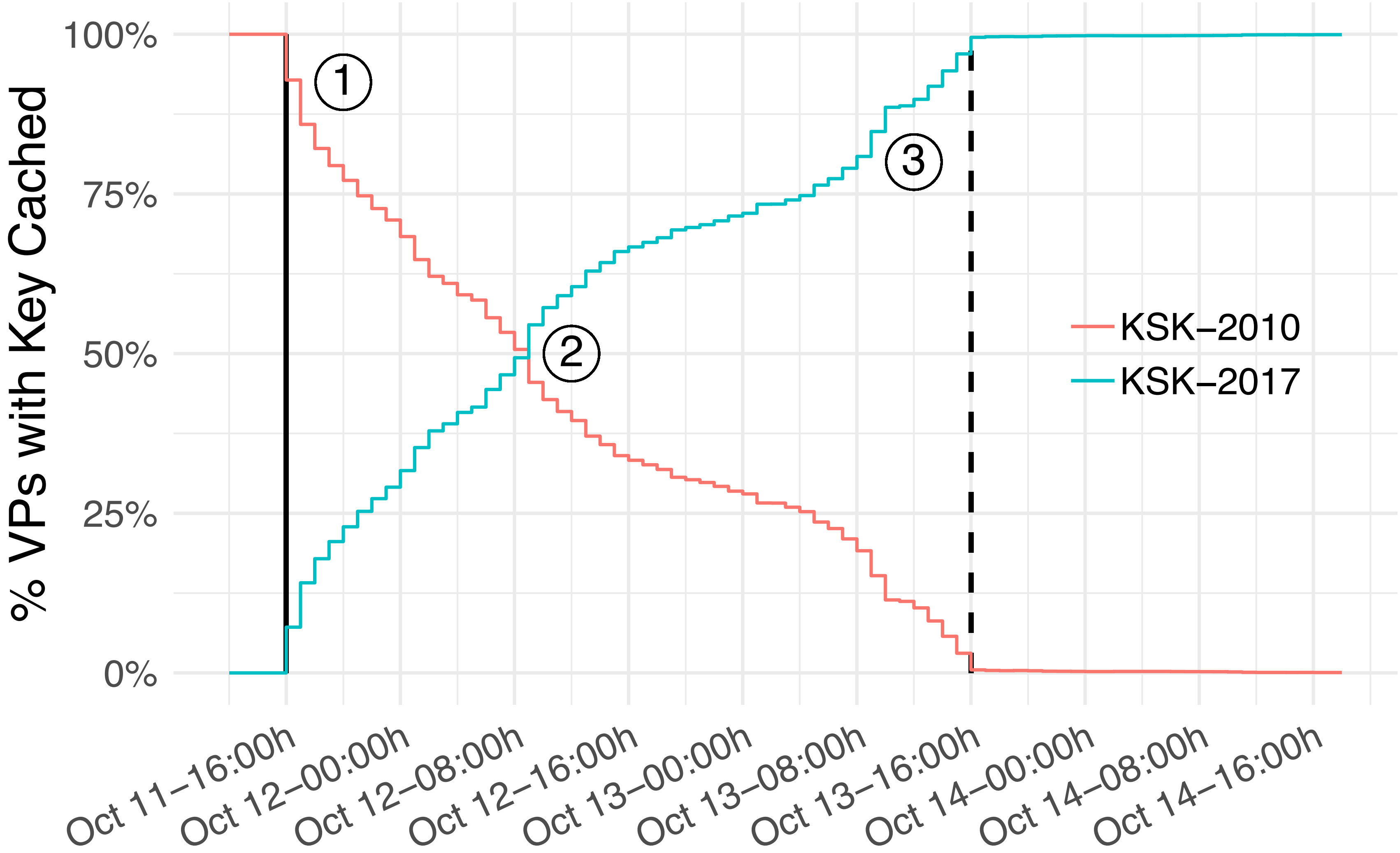


Root Canary Data

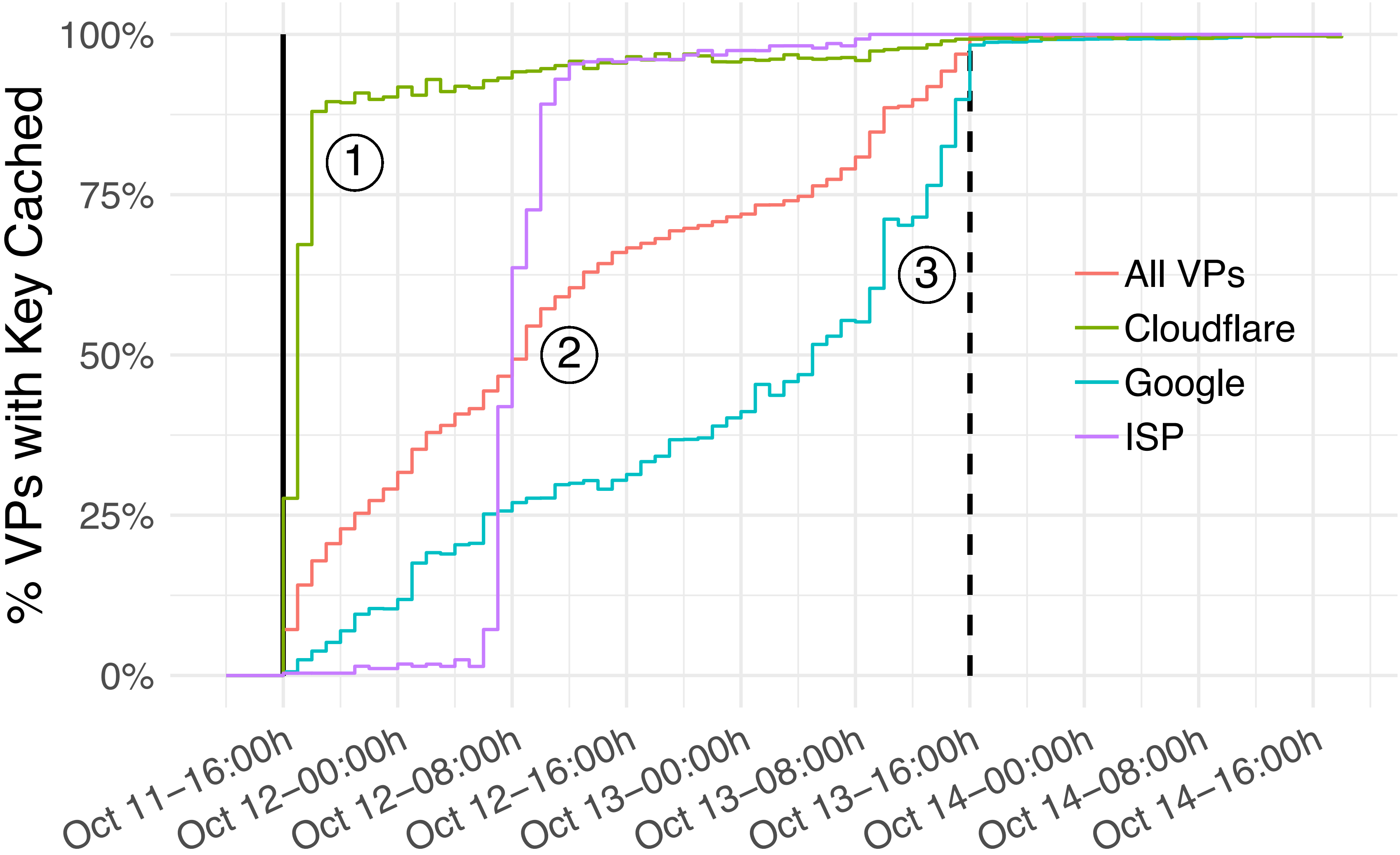
Root Canary Project

- Uses RIPE Atlas probes
- Querying the probe's local resolver, once per hour, for:
    1. an A record with valid signature
    2. an A record with a bogus signature
    3. the root DNSKEY RRset
- 18,277 vantage points in 3,647 autonomous systems
    - 35,719 resolver addresses in 3,141 autonomous systems
- Queries 1 & 2 measure the validation state of the resolver
    - secure, insecure, or bogus
- Query 3 measures uptake of new KSK signatures into caches

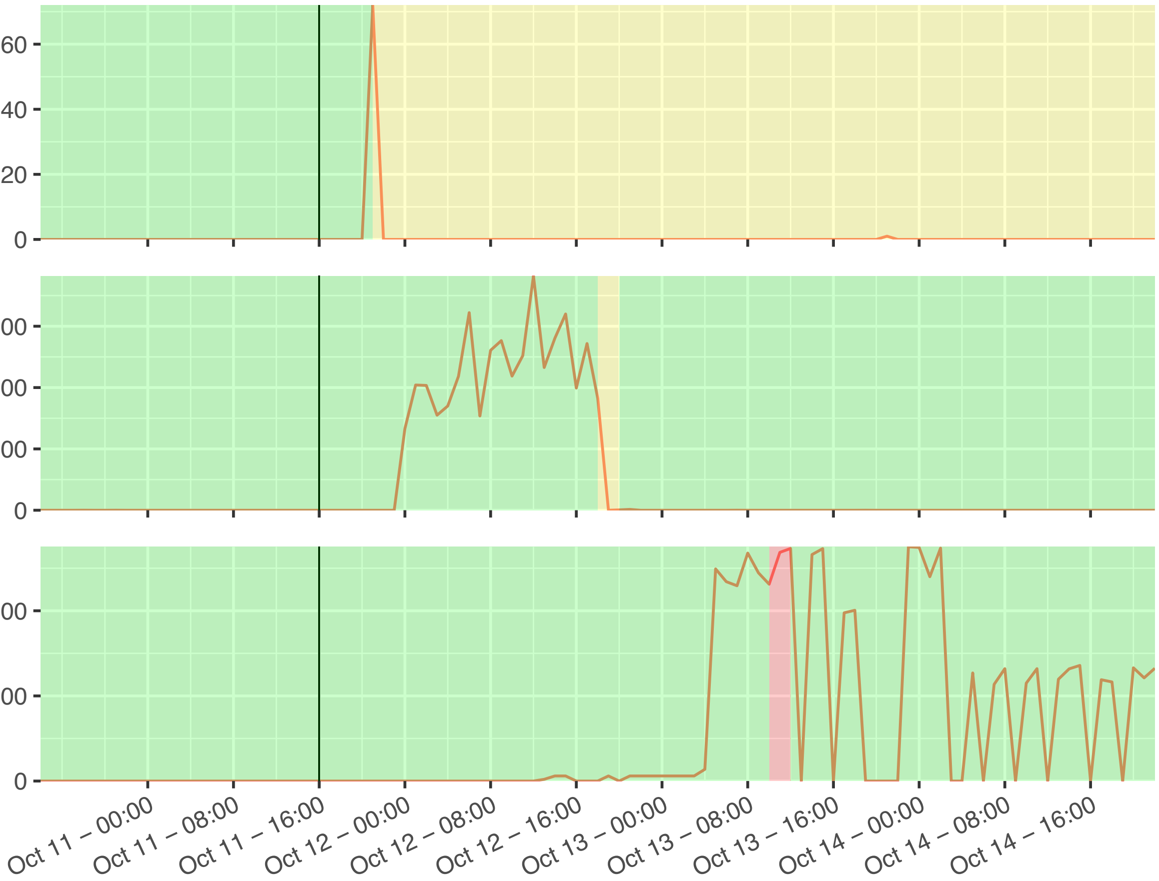
KSK Uptake – All Vantage Points



Vantage Points Using Large Recursive Providers



Changes in Validation State for Some Probes

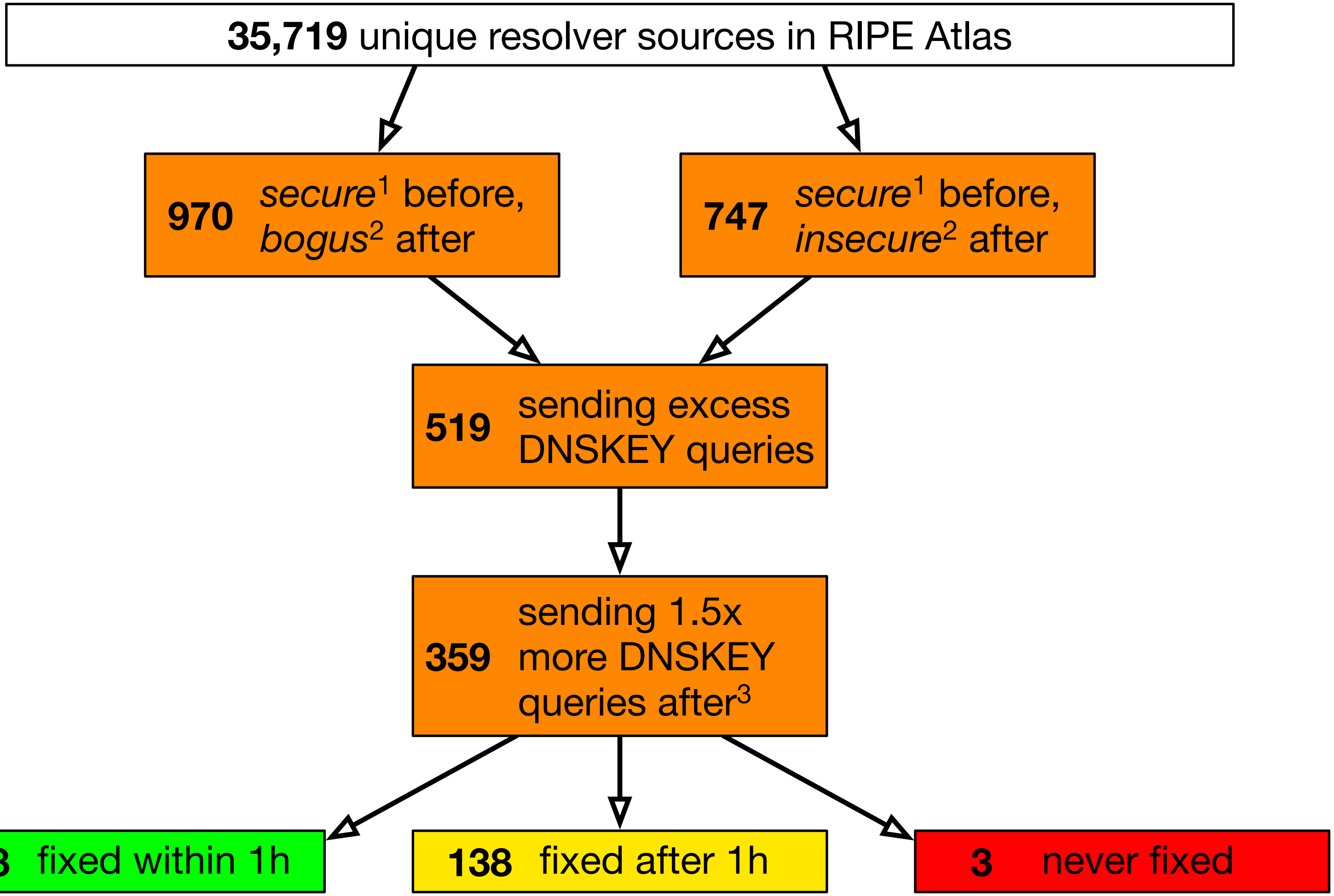


Behavior of three individual RIPE Atlas probes observed shortly after rollover.

Background color:
green = secure
yellow = insecure
red = bogus

red line = DNSKEY queries per second to root servers (from DITL data)

Changes in Validation State for All Probes



35,719 unique resolver sources in RIPE Atlas

970 *secure*[1] before, *bogus*[2] after

747 *secure*[1] before, *insecure*[2] after

519 sending excess DNSKEY queries

359 sending 1.5x more DNSKEY queries after[3]

218 fixed within 1h

138 fixed after 1h

3 never fixed

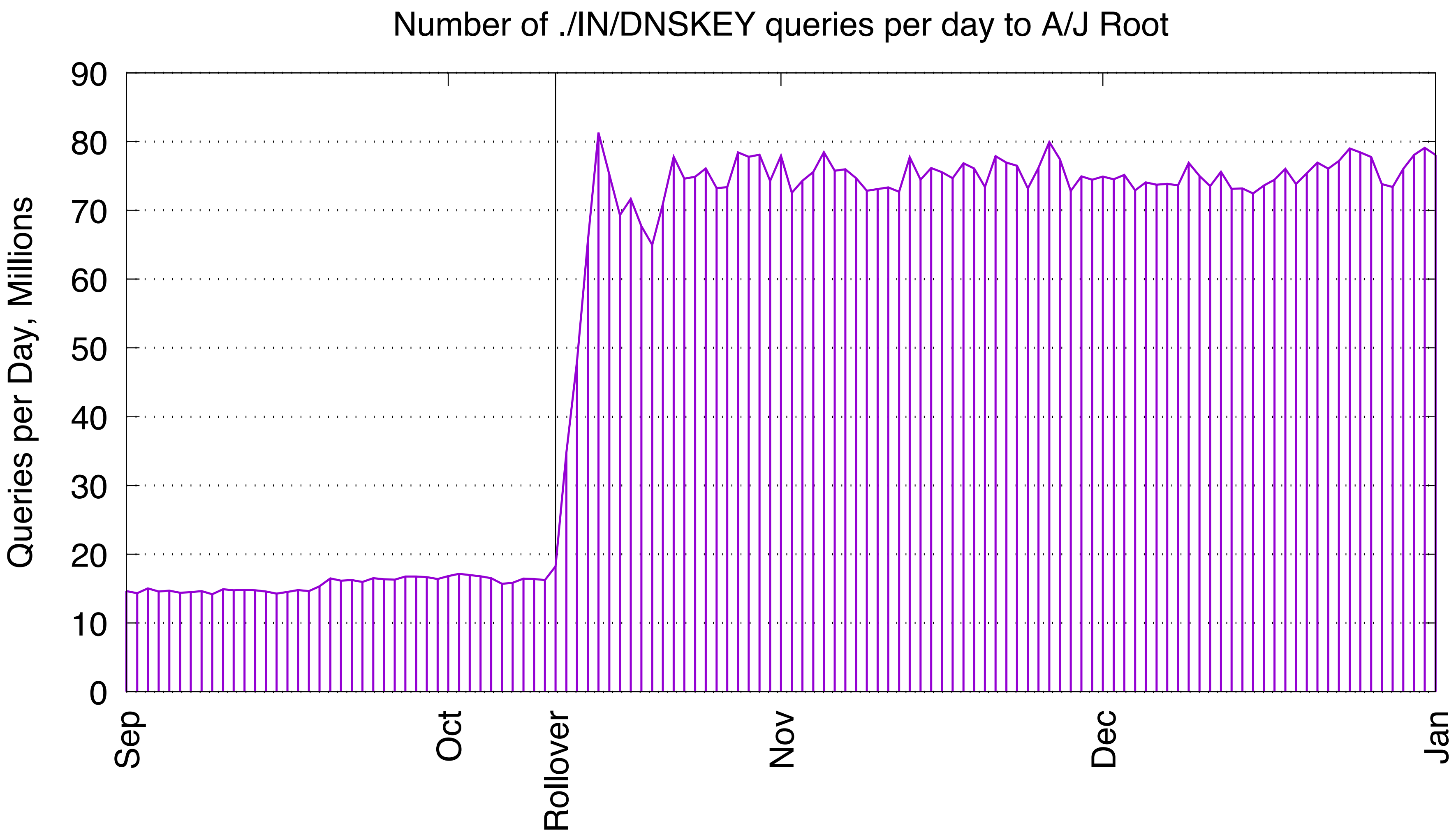
[1] at every point 88 hours before the rollover

[2] at any point 56 hours after the rollover

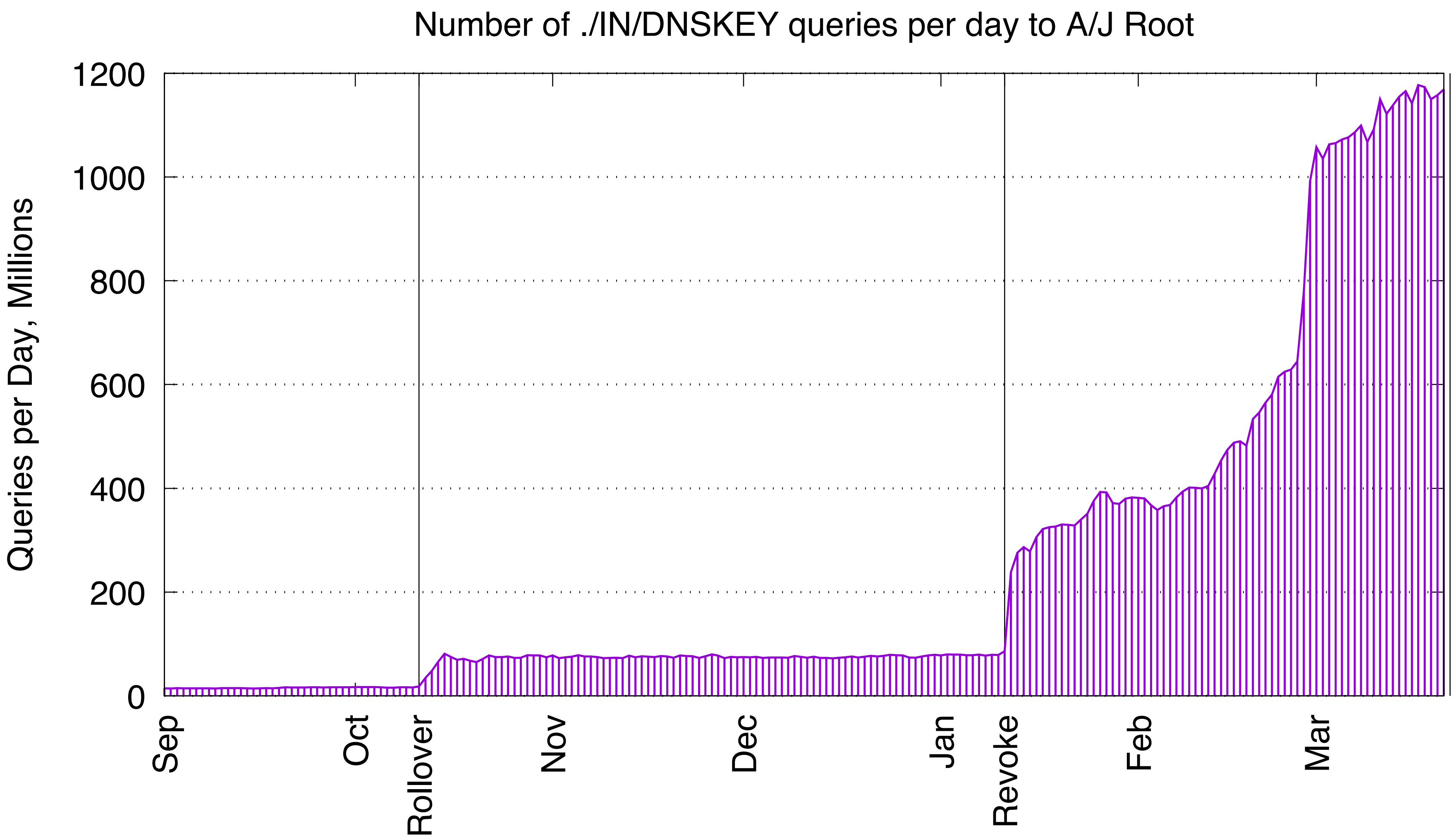
[3] from DITL data

./IN/DNSKEY Query Rates

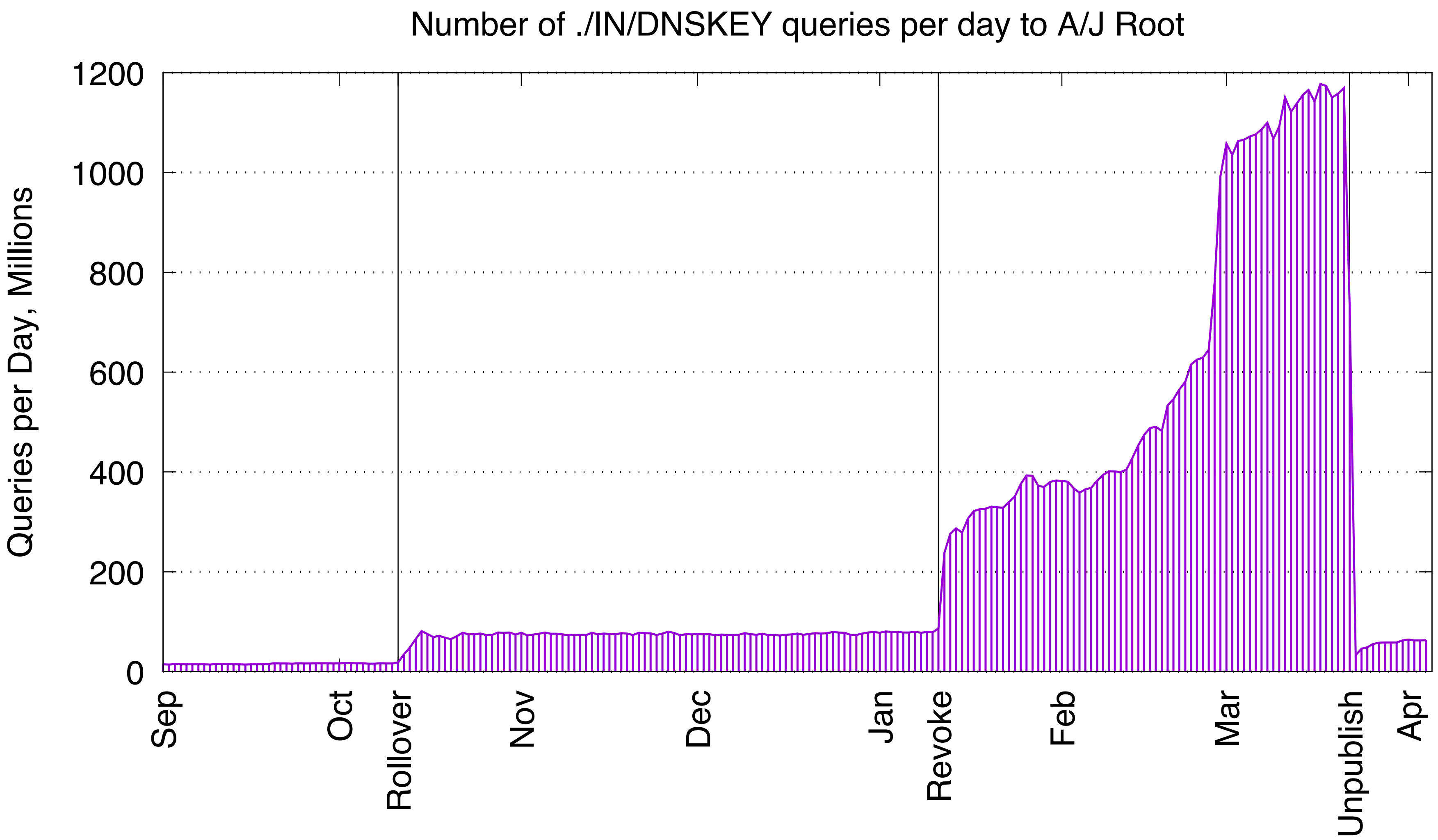
Rollover


Number of ./IN/DNSKEY queries per day to A/J Root
Queries per Day, Millions
90
80
70
60
50
40
30
20
10
0
Sep
Oct
Rollover
Nov
Dec
Jan

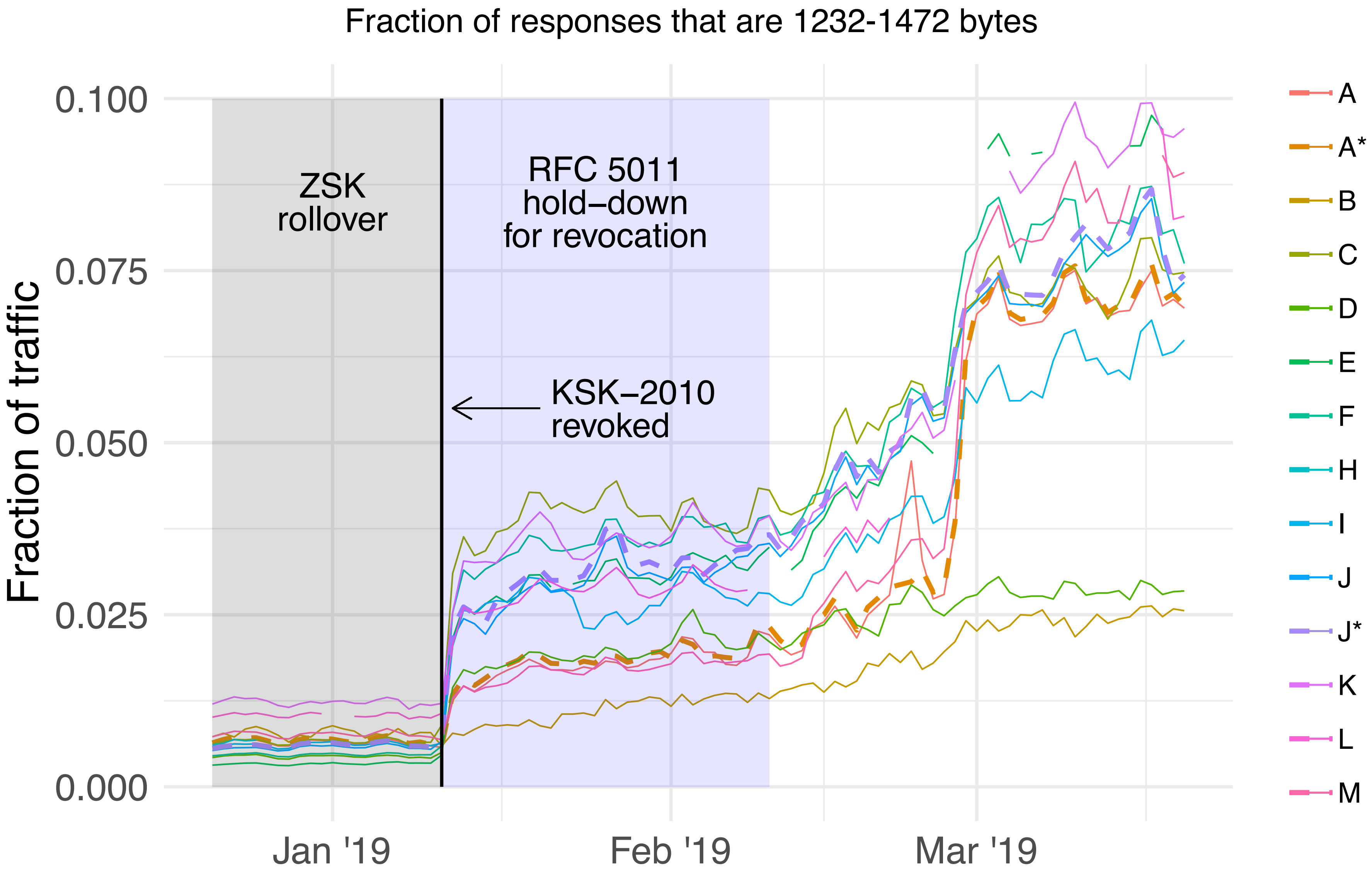
Revocation


Number of ./IN/DNSKEY queries per day to A/J Root
Queries per Day, Millions
1200
1000
800
600
400
200
0
Sep
Oct
Rollover
Nov
Dec
Jan
Revoke
Feb
Mar

Removal from Zone



RSSAC 002 Response Size Data



Software behind DNSKEY query floods?

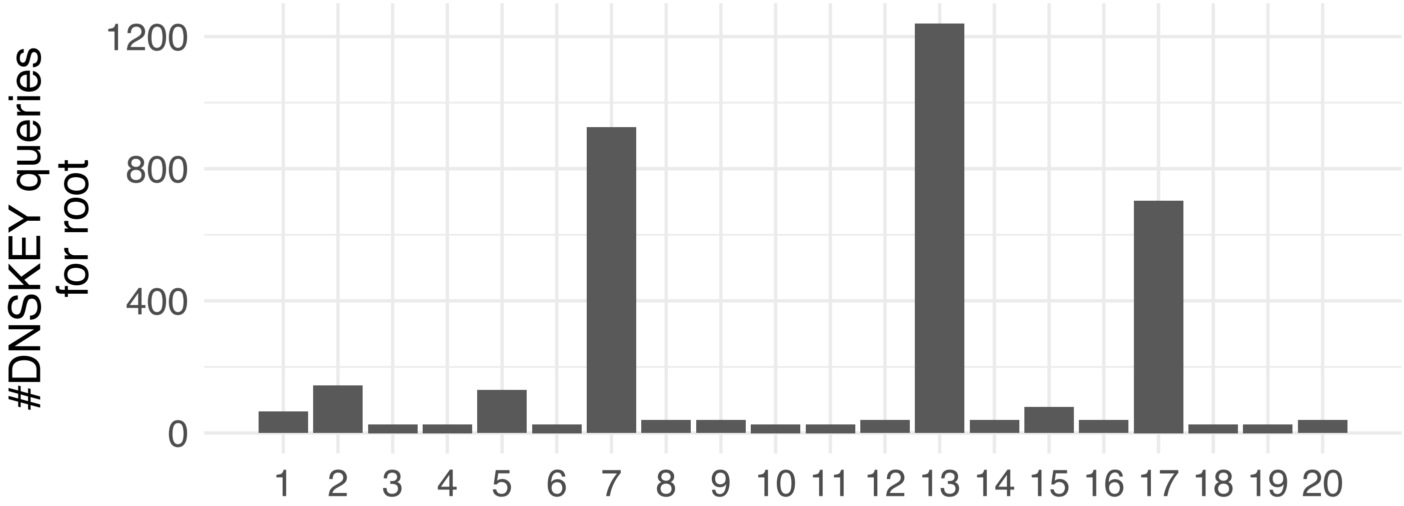
- Sent HOSTNAME.BIND queries to 18,000 query sources
- About 775 responses
- Mostly older BIND versions
  - 34% BIND 9.8.x
  - 45% BIND 9.9.x
  - 13% BIND 9.10.x

Outreach to Particular Sources

- Contacted large French cloud computing company
  - Confirmed a source running BIND 9.8.2 on CentOS
- Contacted a large US midwestern univerisity
  - Confirmed student DNS lab exercise left running in VMs
  - Provided BIND configuration files

BIND Behavior Confirmed

- Conditions for reproducing DNSKEY floods with BIND:
  1. DNSSEC managed keys contains KSK-2010, but not KSK-2017
  2. The dnssec-enable flag was set to false
  3. The dnssec-validation flag was unset, leaving it in its default state of “yes.”
- However, the probability and severity of the condition varies among different runs of this experiment

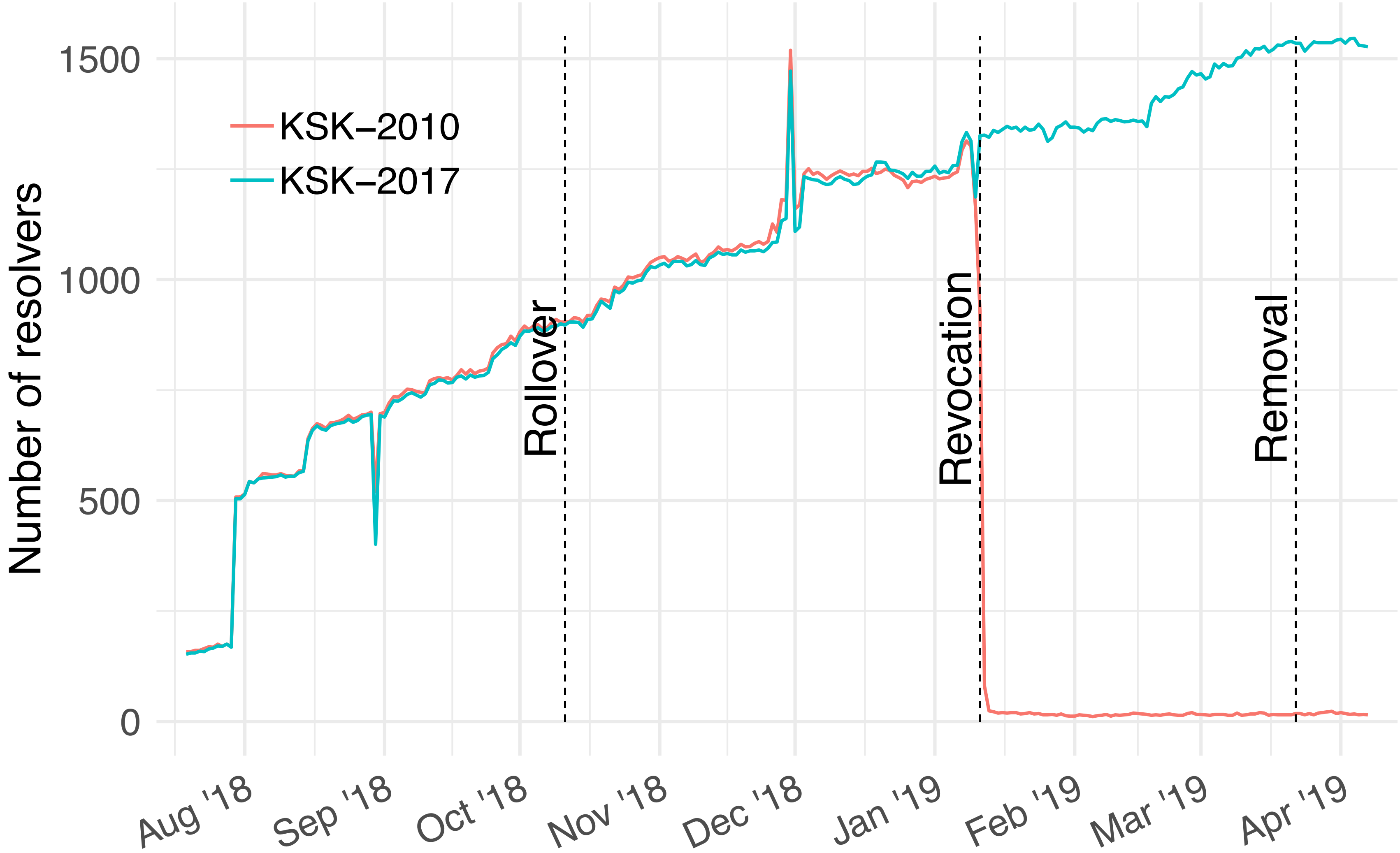


RFC 8509 Root Sentinel

About RFC 8509

- Recursive resolvers implement special query processing
  - root-key-sentinel-is-ta-<key-tag>
  - root-key-sentinel-not-ta-<key-tag>
- By sending specific queries, you can determine
  - If the resolver supports 8509
  - If the resolver has specific keys as a root trust anchor
- We measured 8509 adoption through RIPE Atlas and Luminati

Sentinel Probes via DNSThought / RIPE Atlas



https://dnsthought.nlnetlabs.nl/

Sentinel Measured by DNSThought / Luminati

As of April 2019

Measurement	DNSThought	Luminati
Number of vantage points	10,396	385,520
Number of resolvers	19,583	21,563
Percent of resolvers supporting 8509	8%	2.3%
Percent of resolvers with KSK-2017	8%	2.3%
Percent of resolvers with KSK-2010	0.07%	0.18%

Conclusions

- The first ever KSK rollover was an overall success
  - Very few “reported problems”
- But not without challenges
  - Failures to update trust anchors
  - Revocation not well understood
    - DNSKEY query floods
    - Software bugs?
    - Revoked key reappearing in trust anchors
  - Validation failures seen via active probing

VERISIGN®