The Current State of DNS Resolvers and RPKI Protection

By Erik Dekker and Marius Brouwer

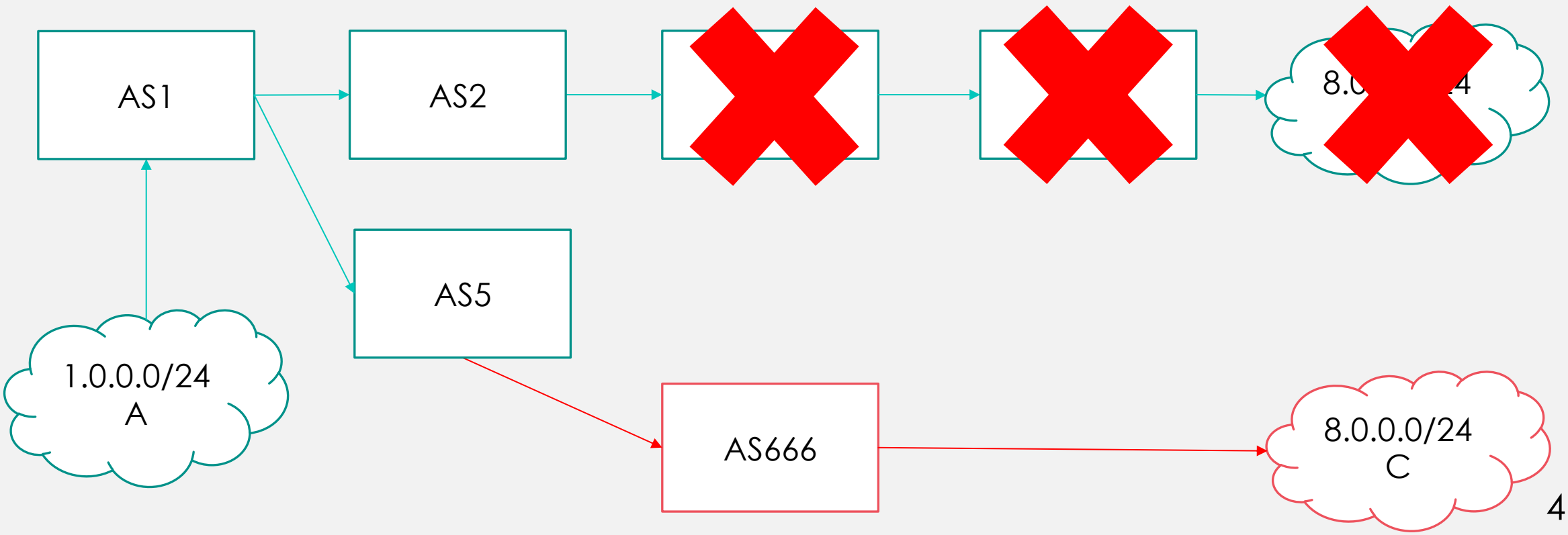
Motivation

- Why is this research important?

Motivation

- BGP is old
- First RFC was published in 1989 (RFC 1105)
- BGP was developed in times when security problems were less prevalent
- And is vulnerable for certain attacks
- For example, BGP is prone to IP Prefix Hijacks

BGP IP Prefix Hijack



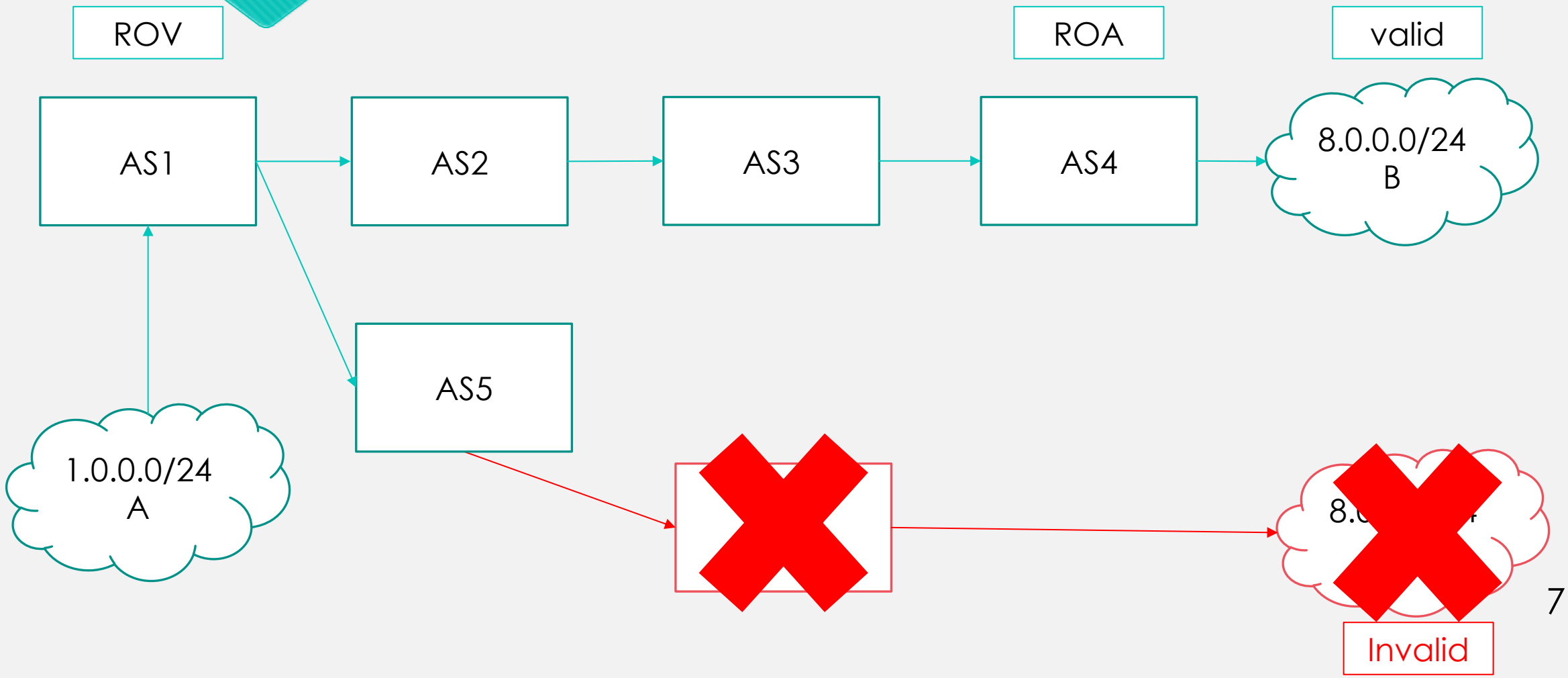
Resource Public Key Infrastructure

- RPKI comes to the rescue!
- Documented in RFC 6480
  - But also in RFC 6481,6482, 6483, 6484, 6485, 6486, 6487, 6488, 6489, 6490, 6491, 6492, and 6493

How does RPKI work?

- RIRs assign IP prefixes to network operators
  - For example RIPE assigns prefixes to SURFnet
- RPKI allows network operators to sign their assigned IP prefixes
  - To prove that they have the right to originate this prefix
  - The RIRs host the Trust Anchors
  - This results in a Route Origin Authorization (ROA) record
    - Which contains the AS number, Prefix(es) and optionally prefix length
- Routers can validate ROA records (Route Origin Validation)
  - ROV == RPKI filtering

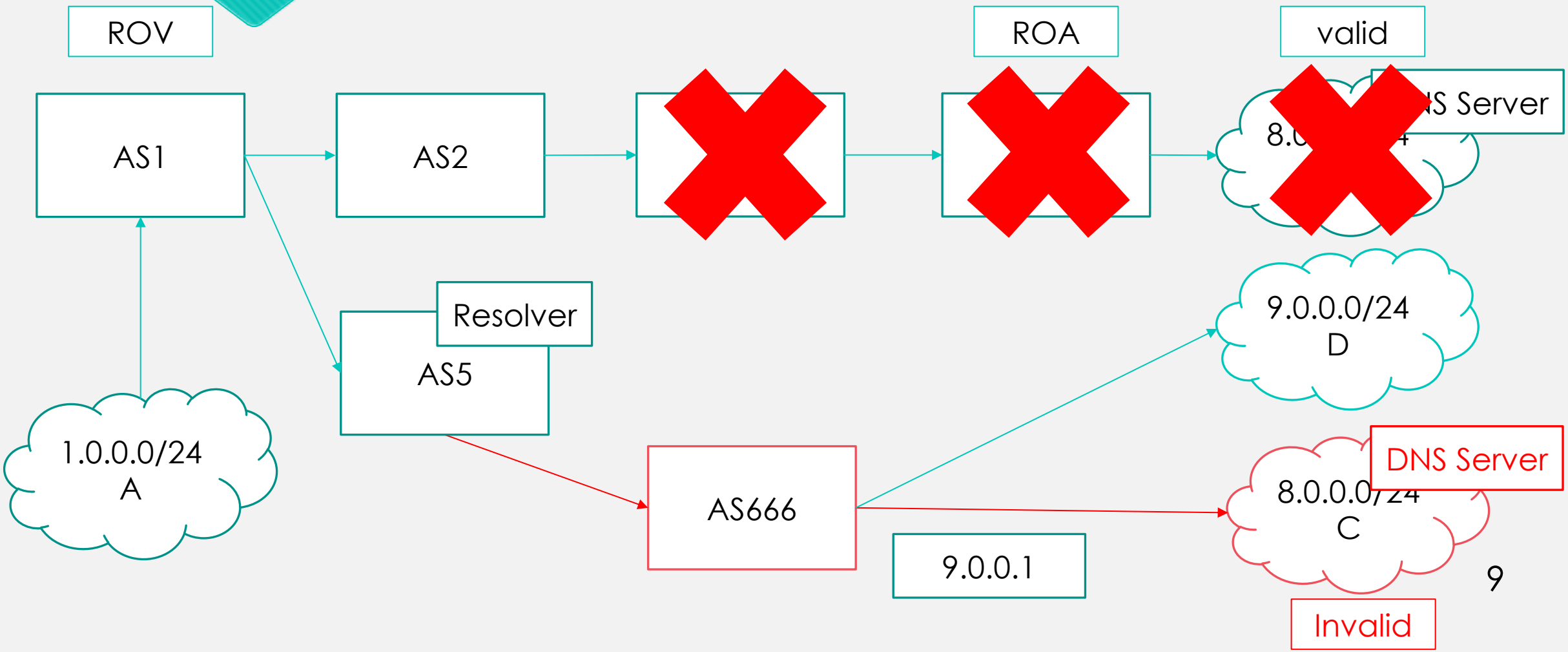
BGP IP Prefix Hijack with RPKI



DNS

- What does this have to do with DNS resolvers?

BGP IP Prefix Hijack



Example

- Amazon Route 53 BGP Hijack
  - All traffic directed to MyEtherWallet was hijacked

Research question

- Main question:
  - "What is the state of RPKI filtering on DNS resolvers?"

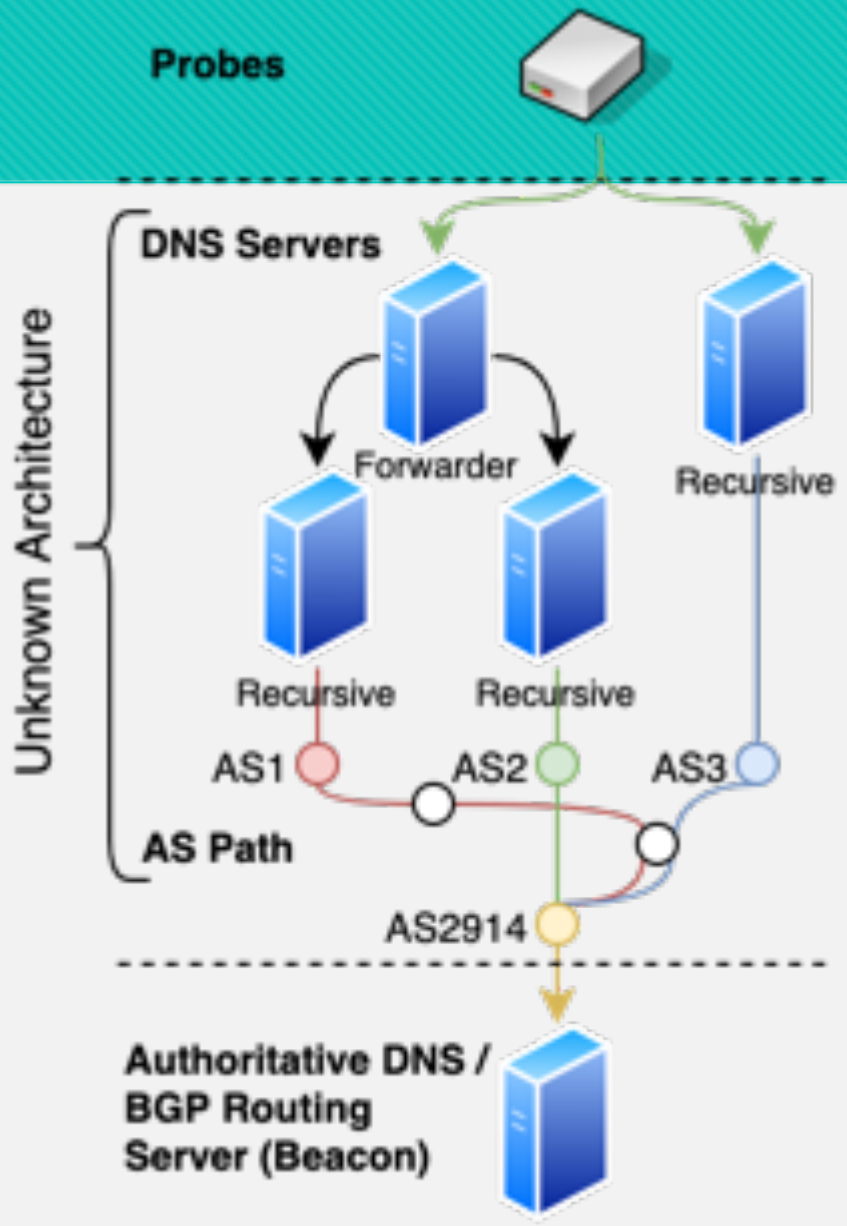
- Sub questions:
  - How does the length of the AS path between resolver and authoritative DNS server influence the level of RPKI protection?
  - How does anycast influence the protection of DNS resolvers?

Scope

- No DNSSEC
- No IPv6

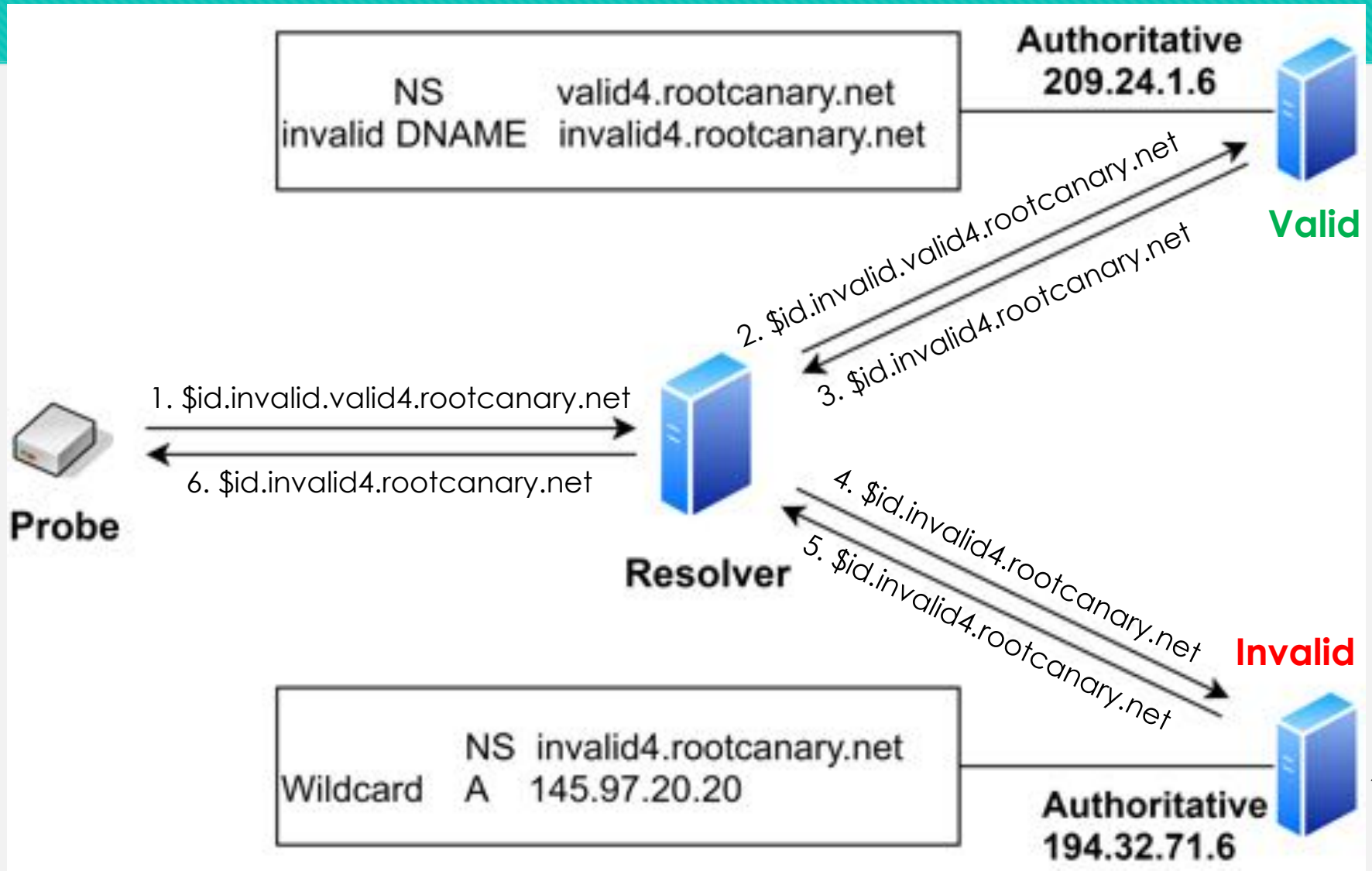
Method – test setup

- RIPE Atlas Probes
  - Can send DNS queries to their resolvers
  - Who query our authoritative DNS servers
- Beacon
  - TCPdump of all the queries
  - Made a BGP dump



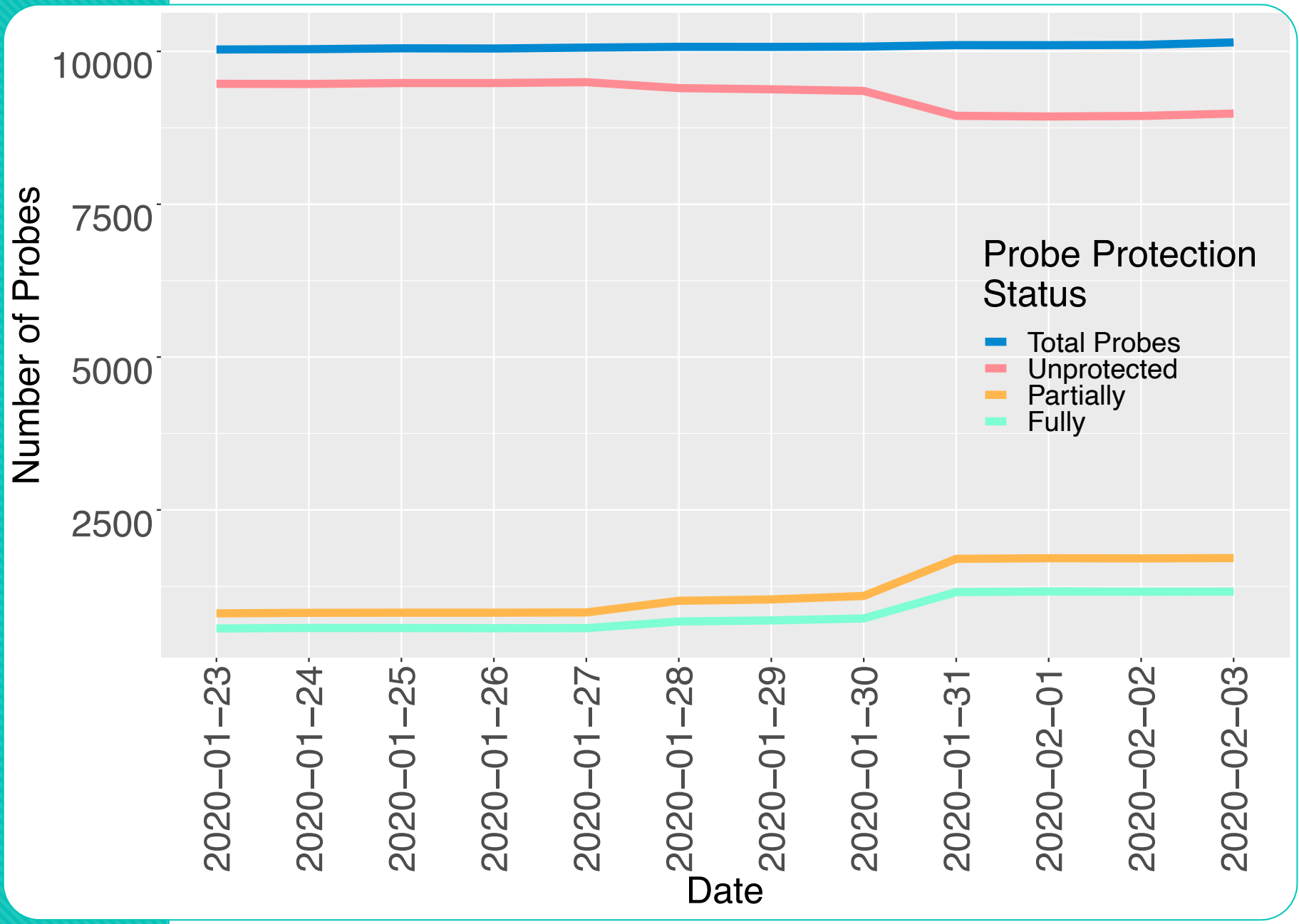
Method – experiment

1. A record
2. A record
3. Synthesized CNAME
4. A record
5. Answer
6. Answer

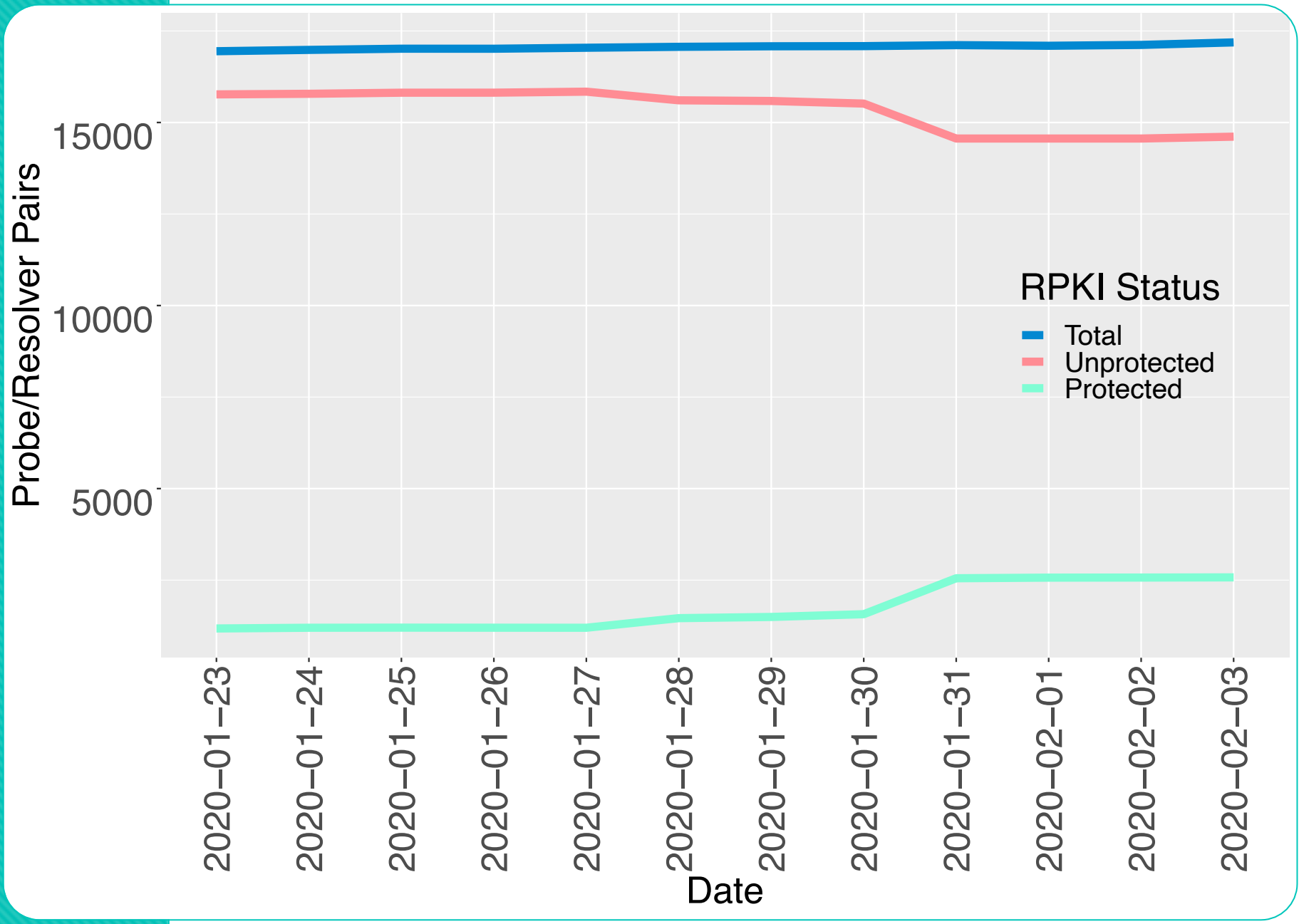


Results

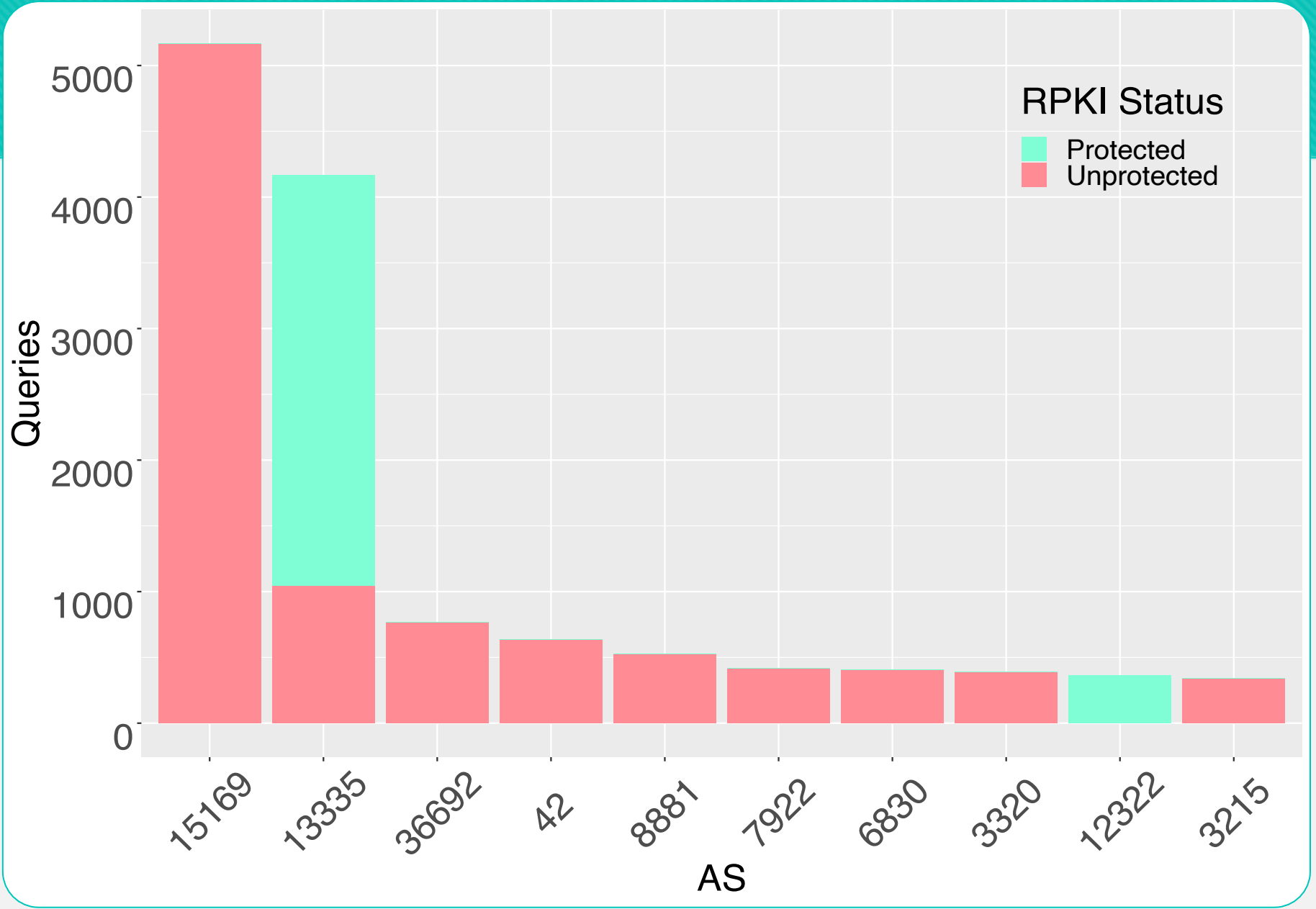
Results – Probe RPKI Coverage



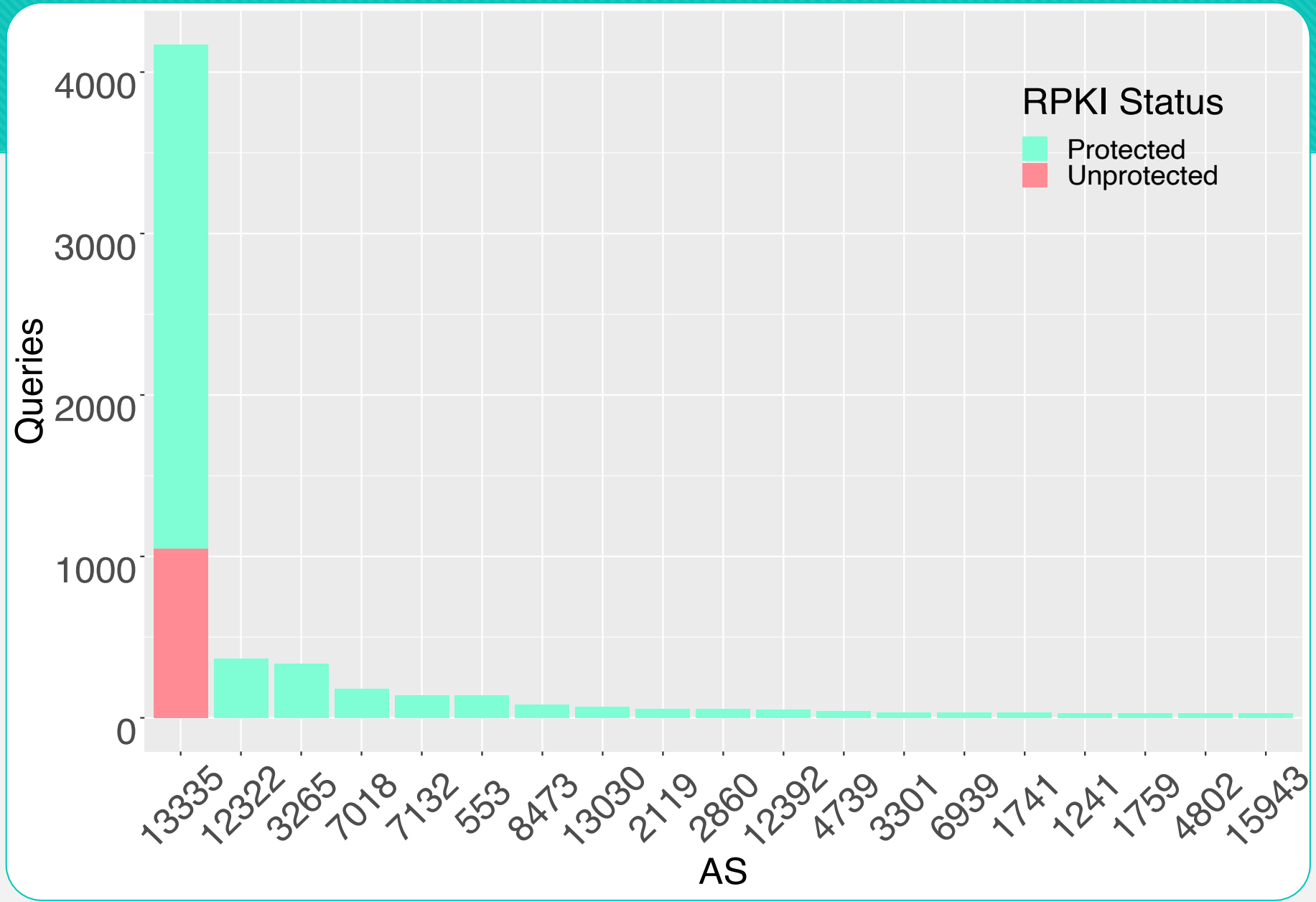
Results – Probe/ Resolver RPKI Coverage



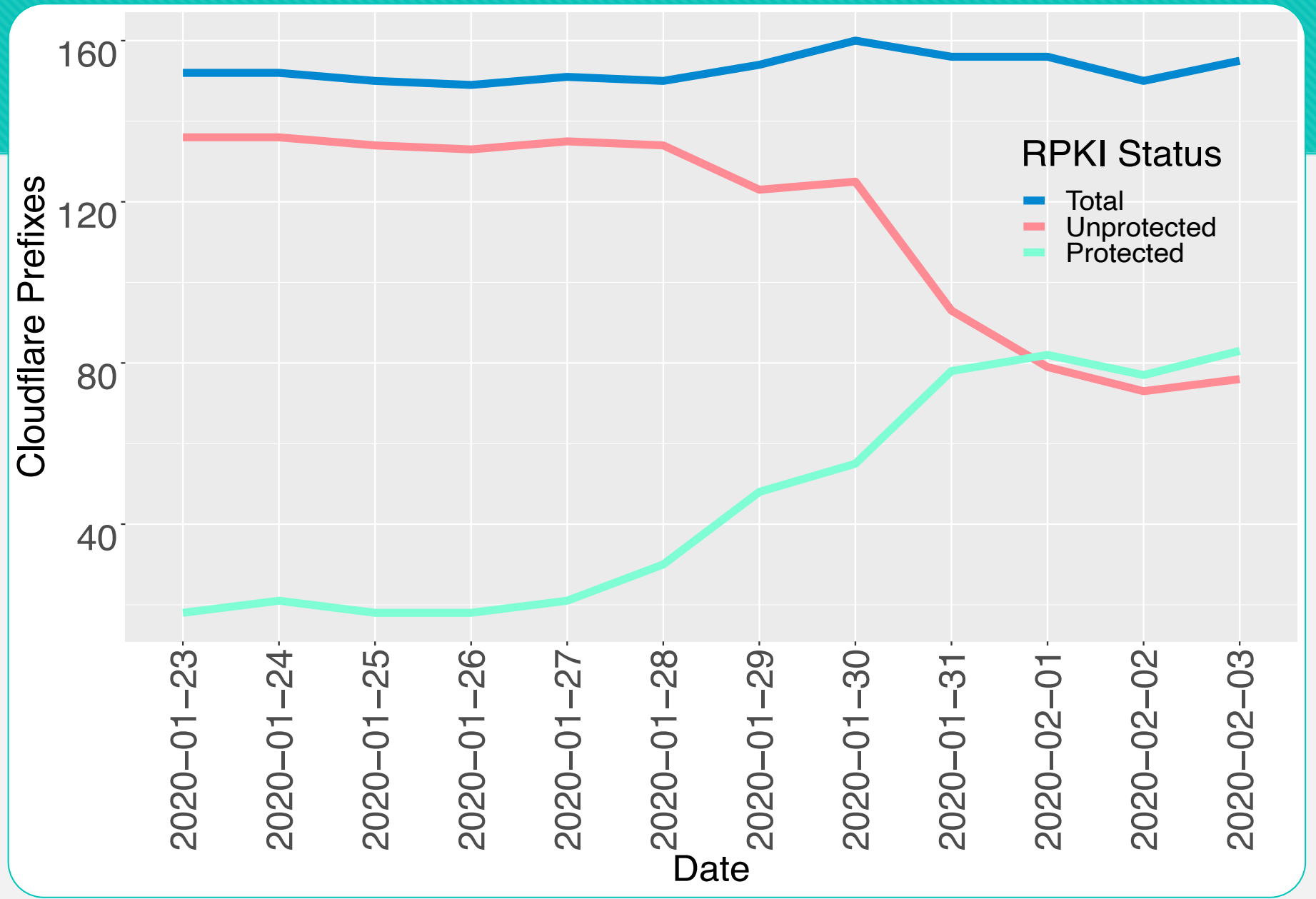
Results – Top 10 AS



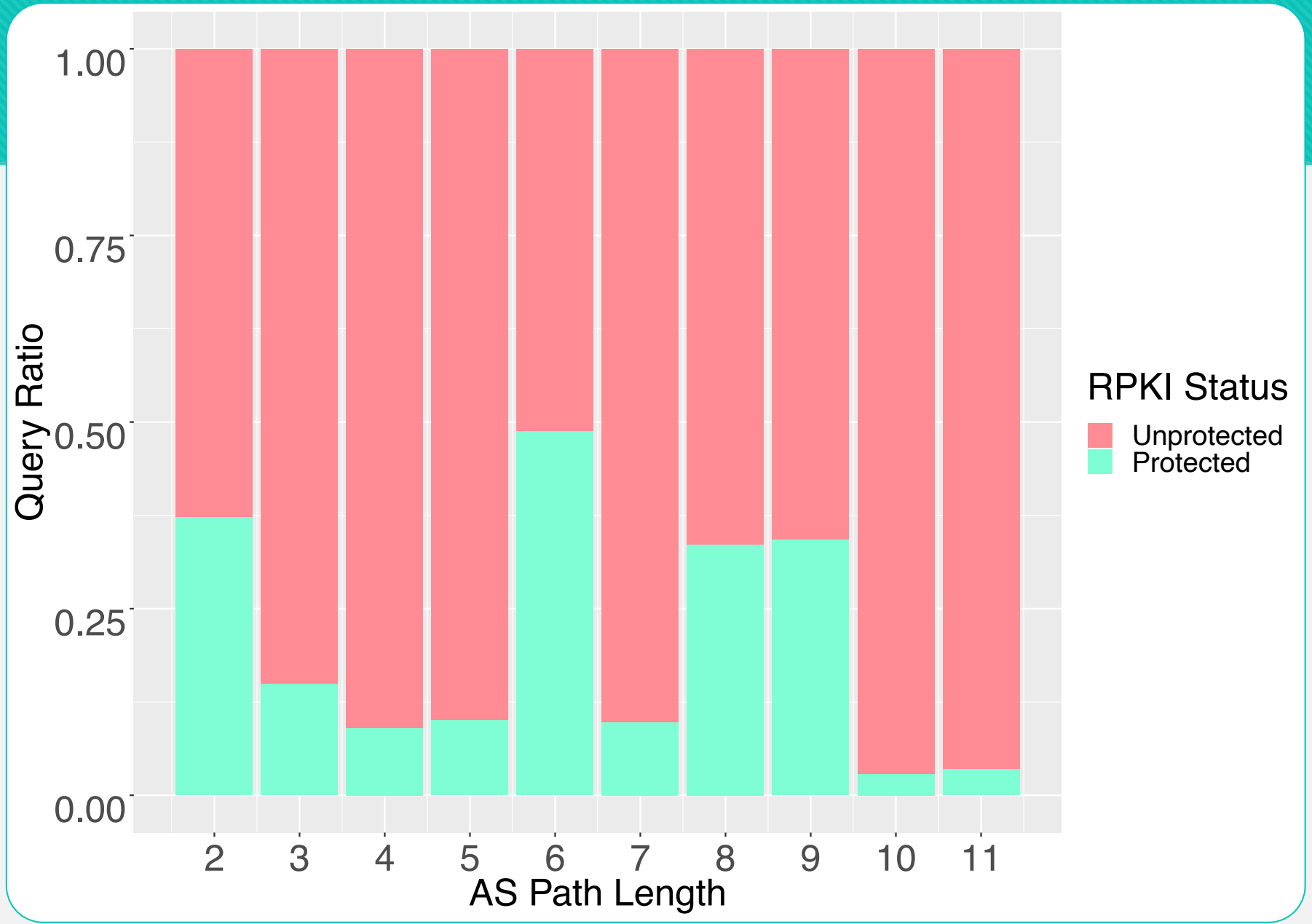
Results – Top 19 AS highest filtering ASes



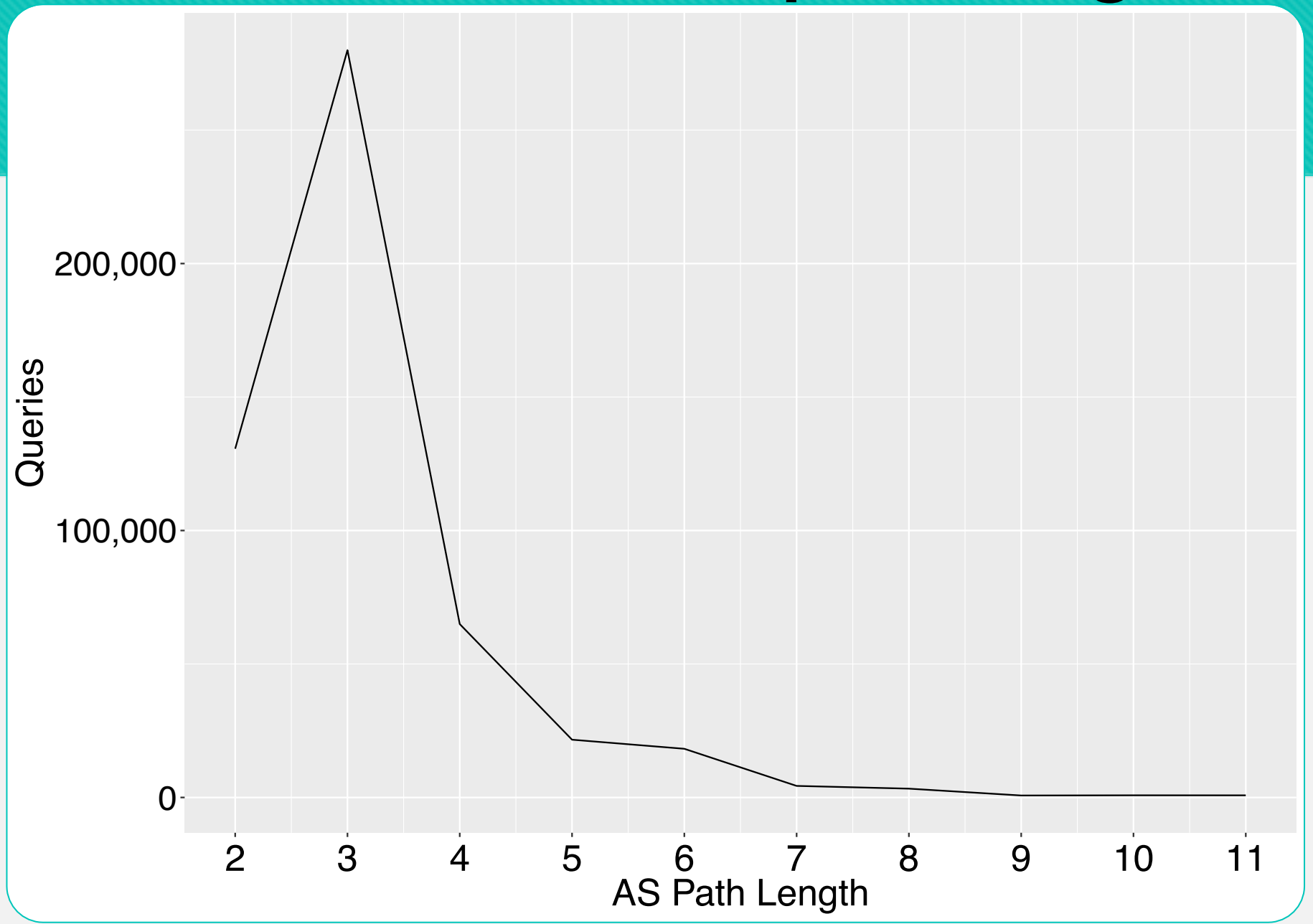
Results – Influence of Cloudflare anycast



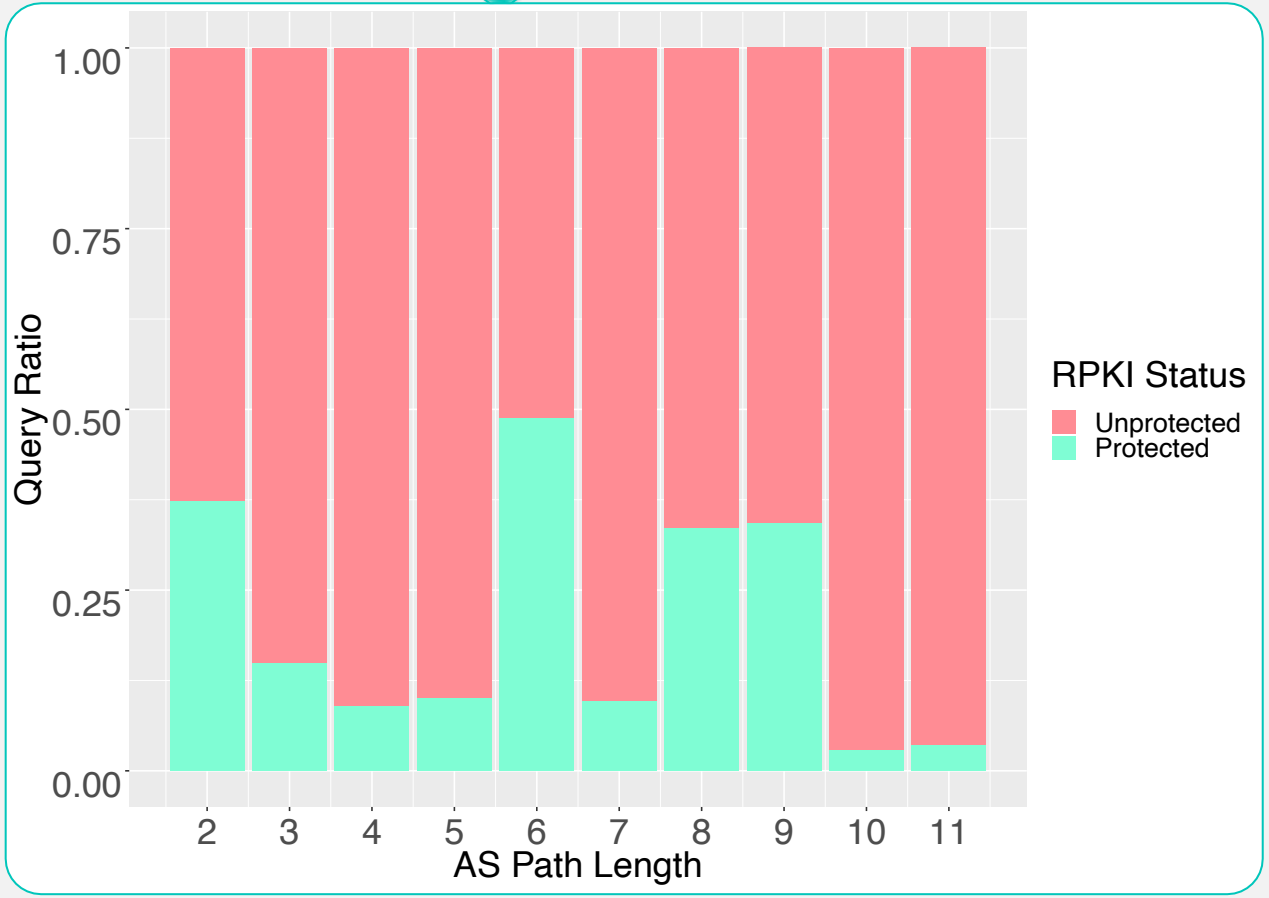
Results – Influence of AS path length

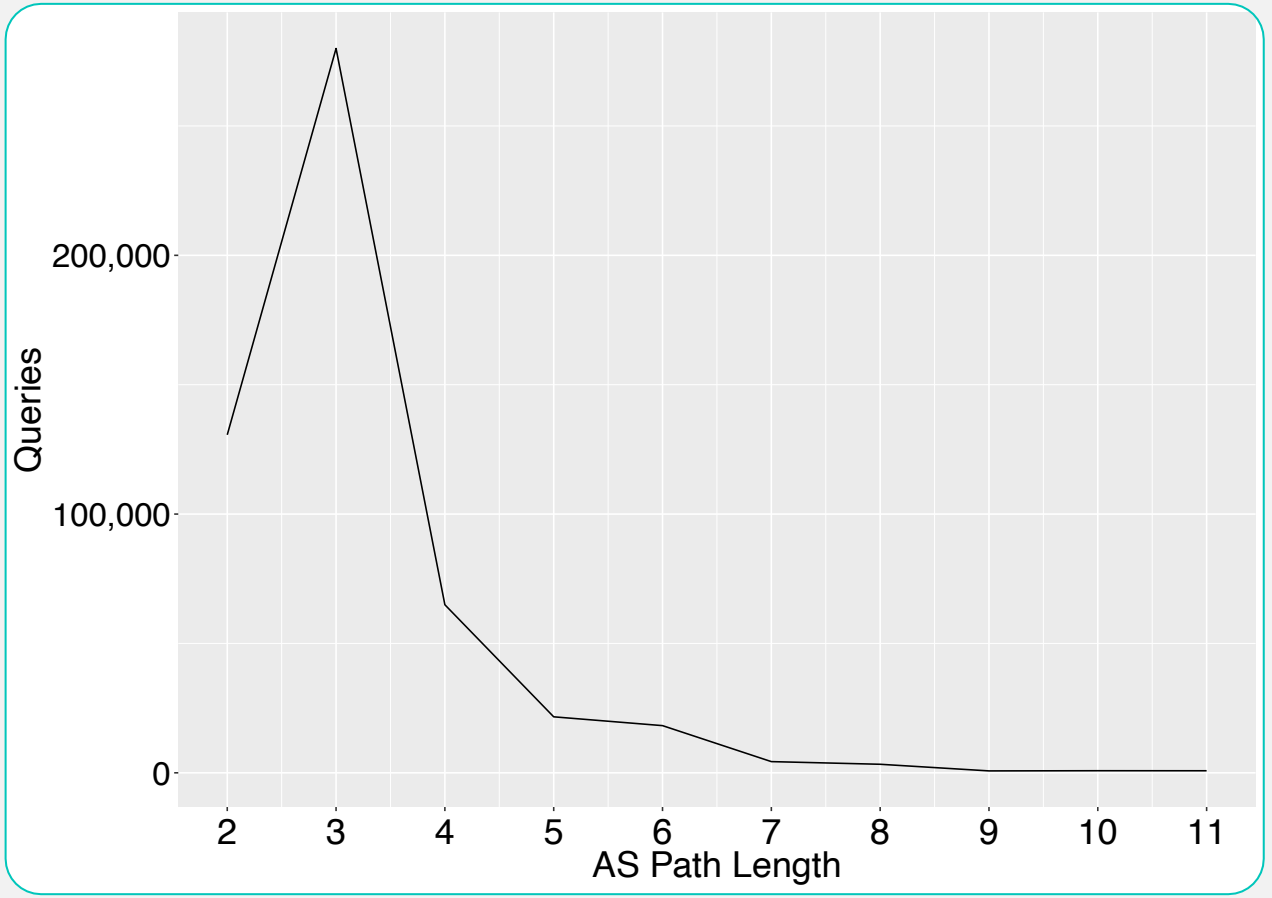


Results – Influence of AS path length



Results – Influence of AS path length





Conclusions

Main Research Question:
“ What is the state of RPKI filtering on DNS resolvers? ”

• How does the length of the AS path between resolver and authoritative DNS server influence the level of RPKI protection?

•How does anycast influence the protection of DNS resolvers?

Discussion

- RPKI query coverage ≠ RPKI protected clients
- Atlas probe AS could still be hijacked.
- Small amount of ASes are fully protected
- Expectation: Longer AS path more RPKI protection
  - Based on reverse path
- Influence of anycast DNS relatively high and growing
- Population of experiment is western oriented and geek biased

Future Work

- Take DNS forwarders into account in future research
- Make use of another query generator other than RIPE Atlas for a different population
- Place more beacons in different regions/AS
- Focus on specific open DNS resolvers e.g. Cloudflare and Verisign Public DNS
- Longitudinal study of ongoing data capture
- Analyze which DNS resolvers are aided by filtering along the path.

Acknowledgements

Questions?