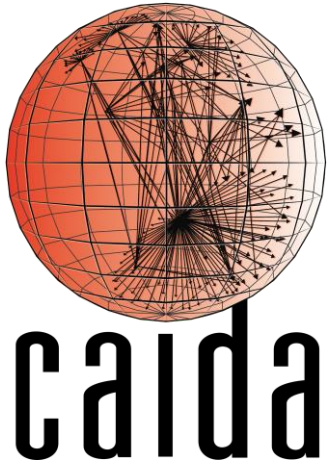
IRR Hygiene in the RPKI Era

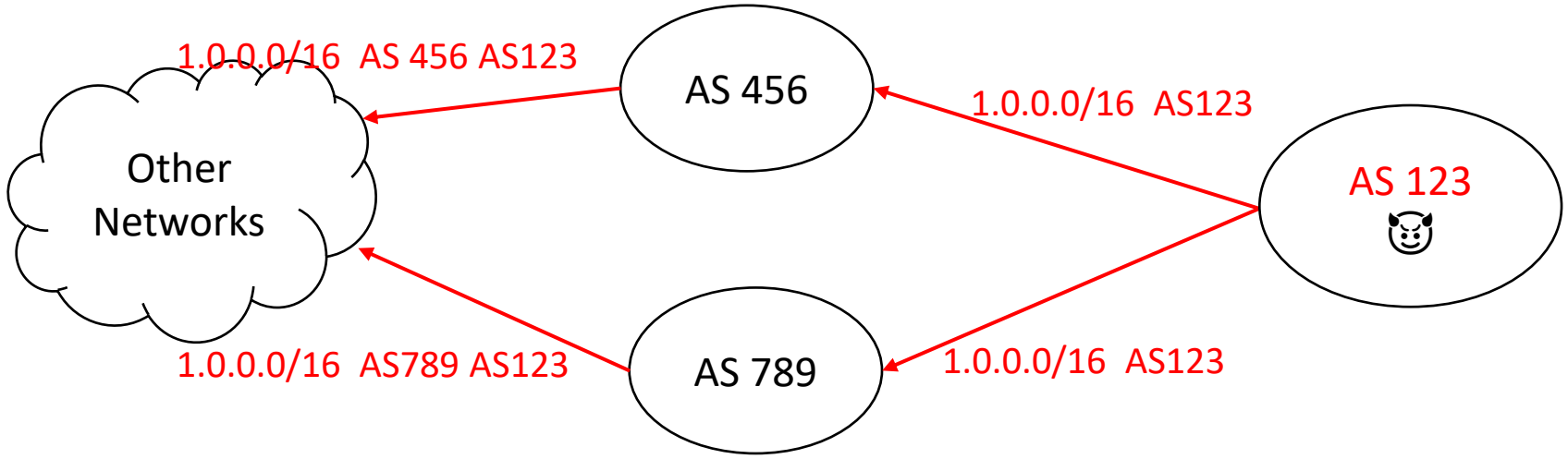
Ben Du, Gautam Akiwate, Thomas Krenc, Cecilia Testart, Alexander Marder, Bradley Huffaker, Alex C. Snoeren, KC Claffy

UC San Diego



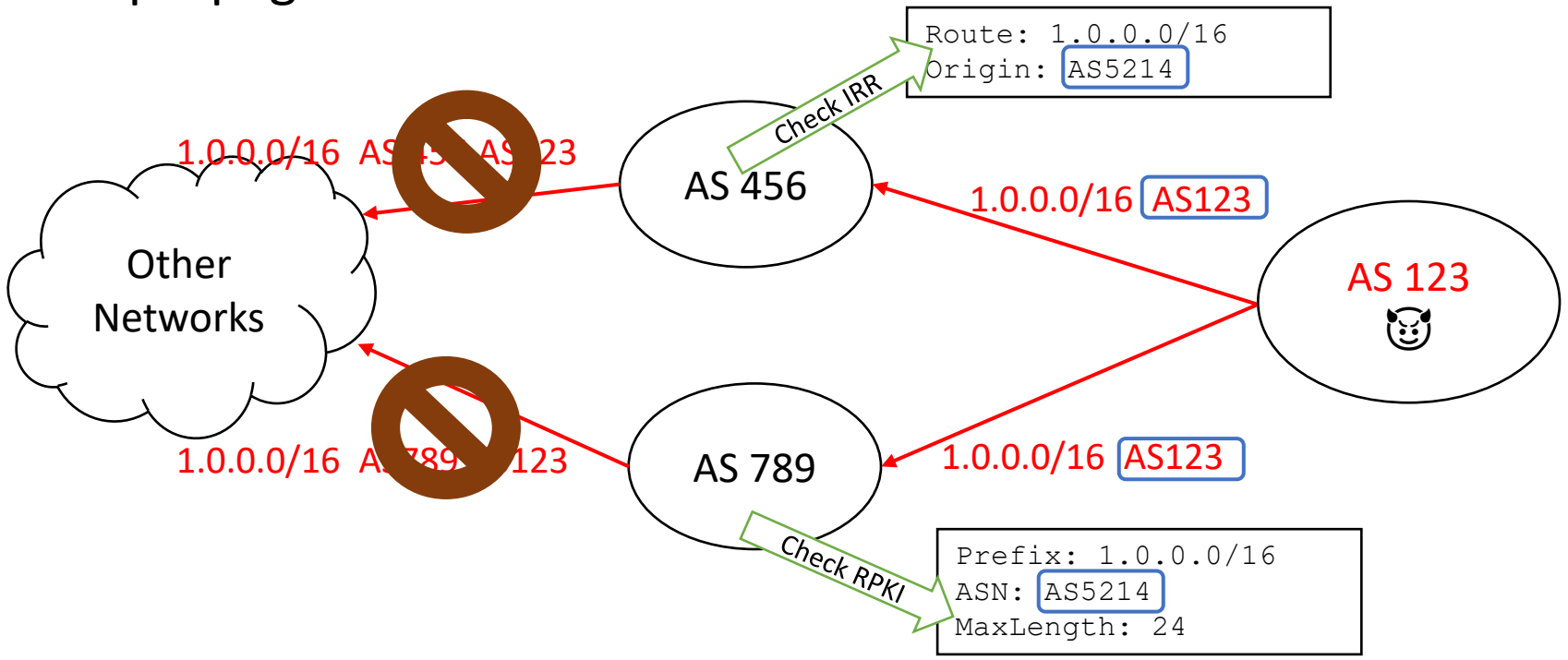
Introduction

- The Internet Routing Registry (IRR) is designed for sharing routing policy
- The Resource Public Key Infrastructure (RPKI) is designed to improve routing security
- Network operators can use those 2 databases to verify BGP information and prevent the propagation of false BGP announcements



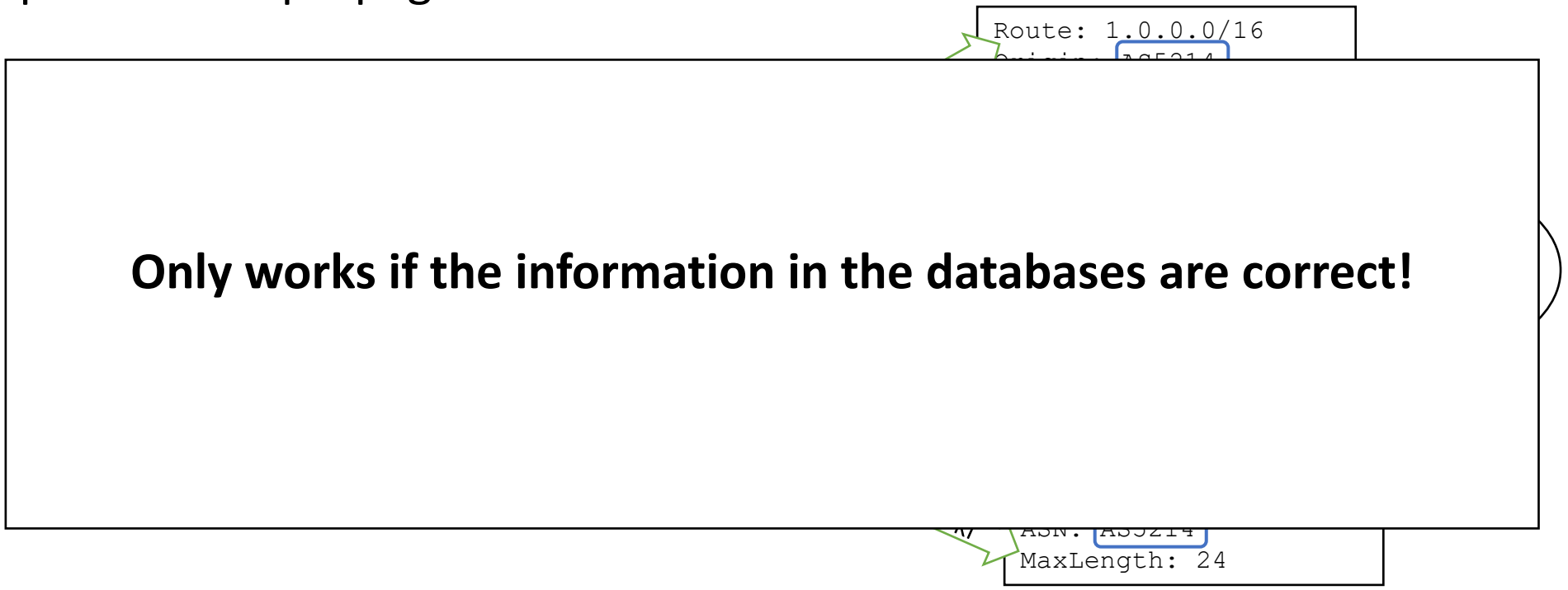
Introduction

- The Internet Routing Registry (IRR) is designed for sharing routing policy
- The Resource Public Key Infrastructure (RPKI) is designed to improve routing security
- Network operators can use those 2 databases to verify BGP information and prevent the propagation of false BGP announcements



Introduction

- The Internet Routing Registry (IRR) is designed for sharing routing policy
- The Resource Public Key Infrastructure (RPKI) is designed to improve routing security
- Network operators can use those 2 databases to verify BGP information and prevent the propagation of false BGP announcements



Focus of this Work

- Accuracy of IRR information is not guaranteed

IRR

- No root of trust
- Prone to negligence

RPKI

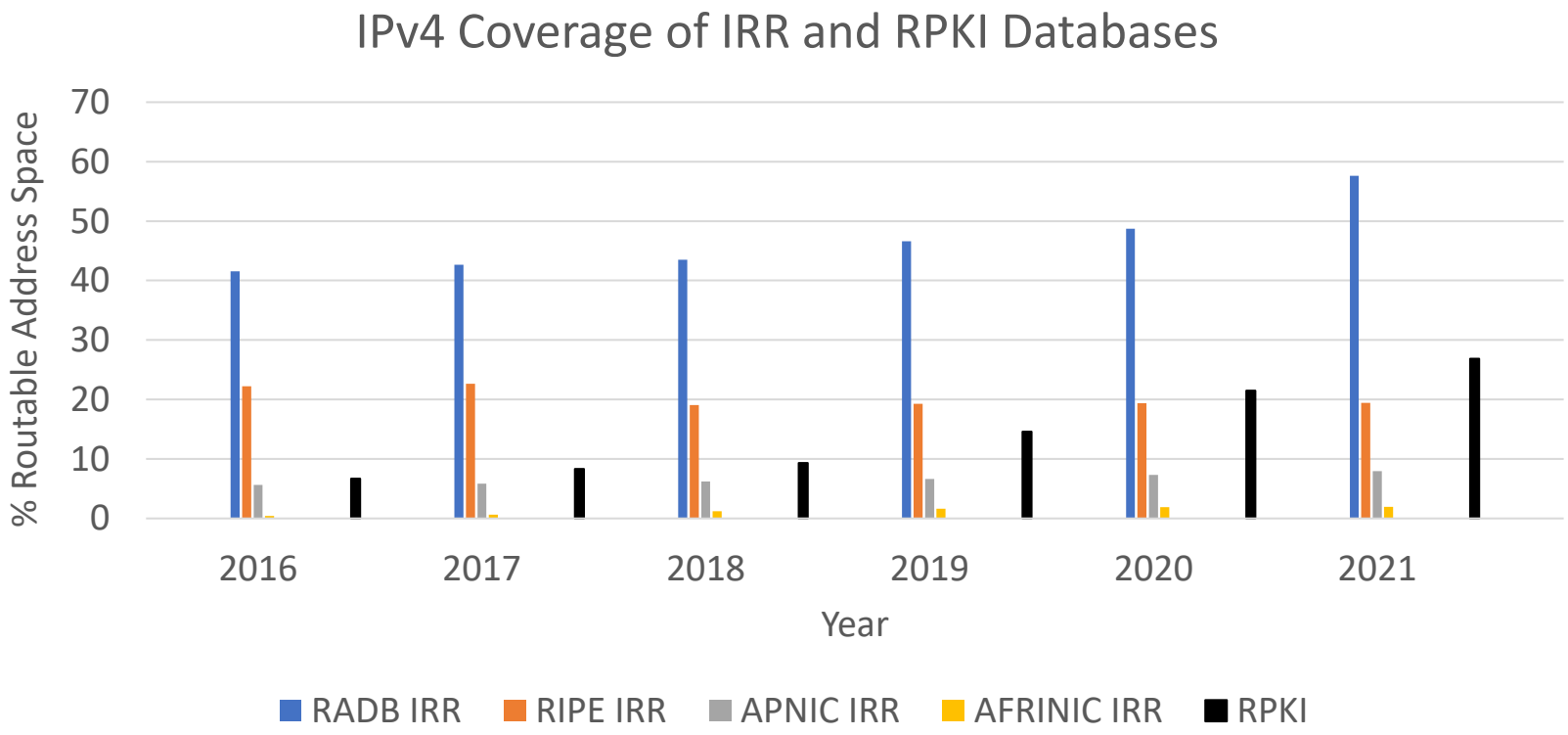
- Cryptographically attested
- 5 RIRs as Trust Anchors
- Records expire if not maintained

- Inaccurate IRR information may pose a risk in routing security
  - Networks that only use IRR may develop incorrect route filters
- Need to study the scale of inaccurate IRR information

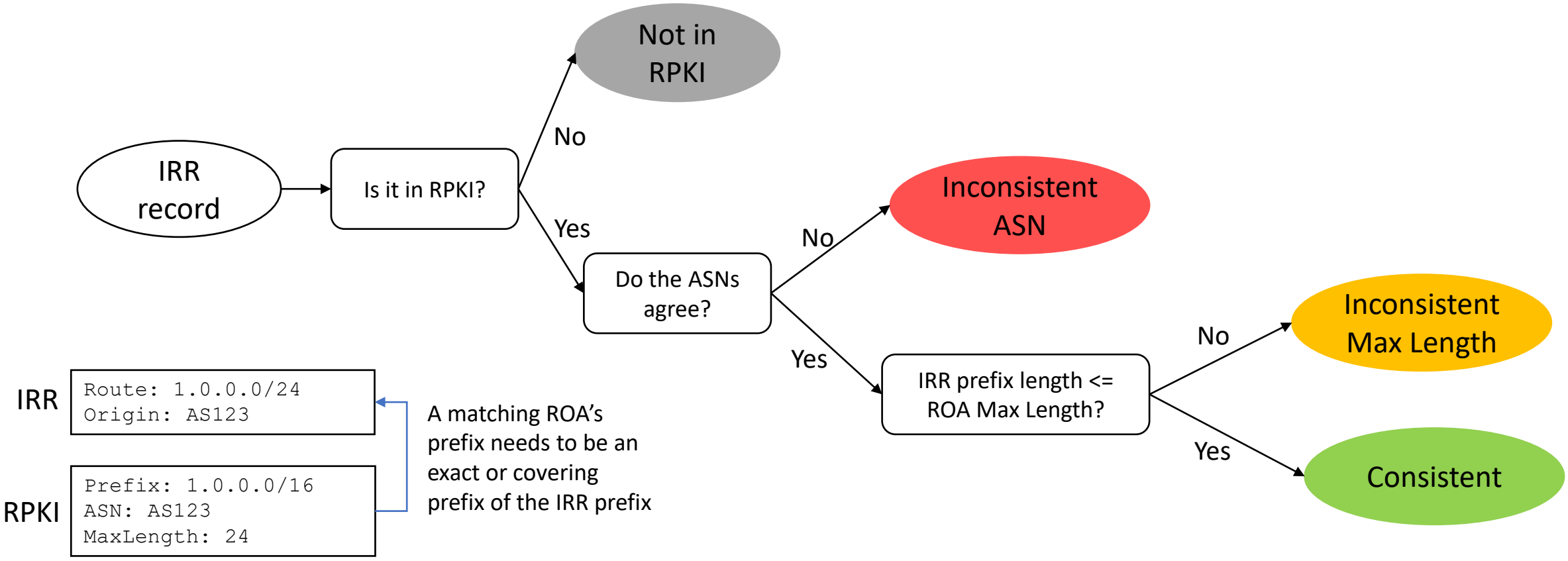
we quantify and analyze the main reasons for inconsistency between IRR and RPKI.

Datasets

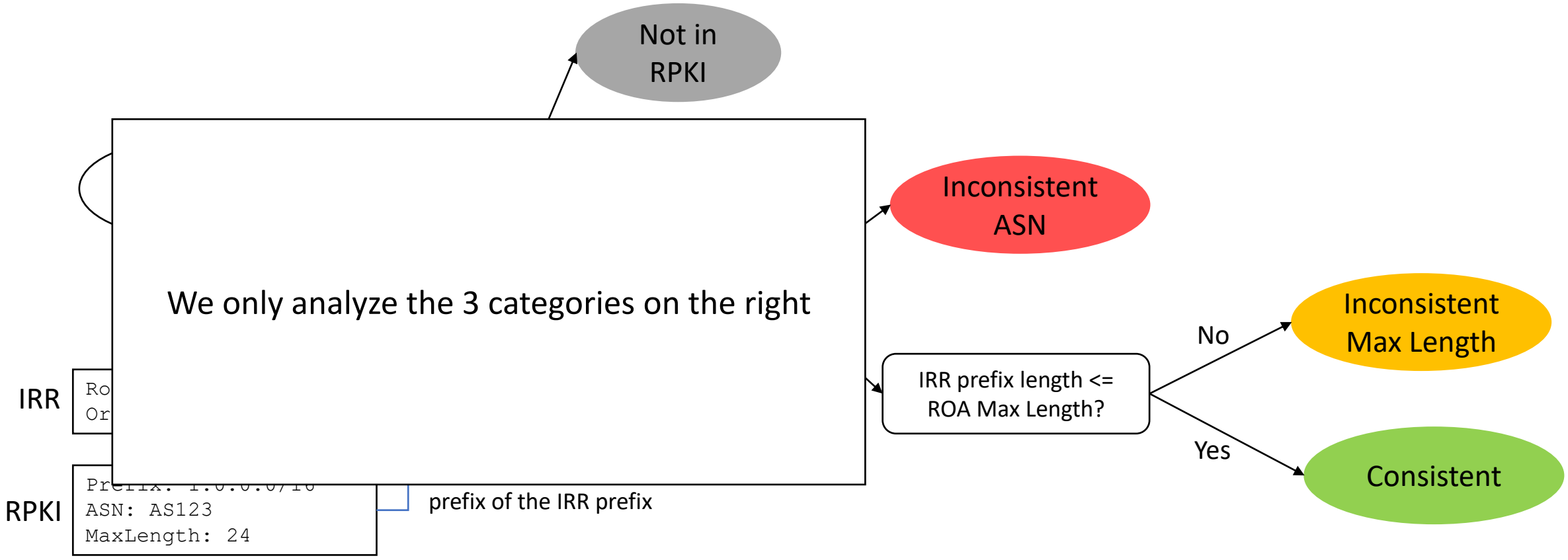
- IRR databases: RADB, RIPE, APNIC, and AFRINIC
- RPKI database: Validated ROA Payloads (VRPs) from all 5 Trust Anchors, published by the RIPE NCC



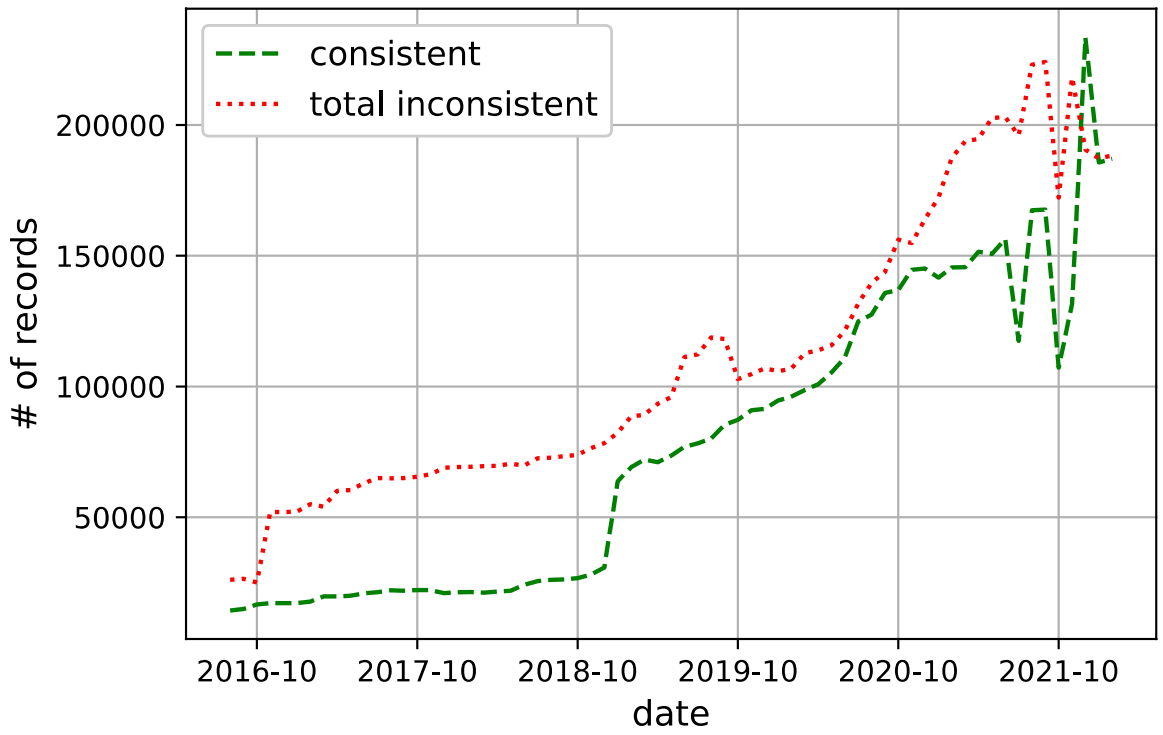
Methodology – Record Classification



Methodology – Record Classification

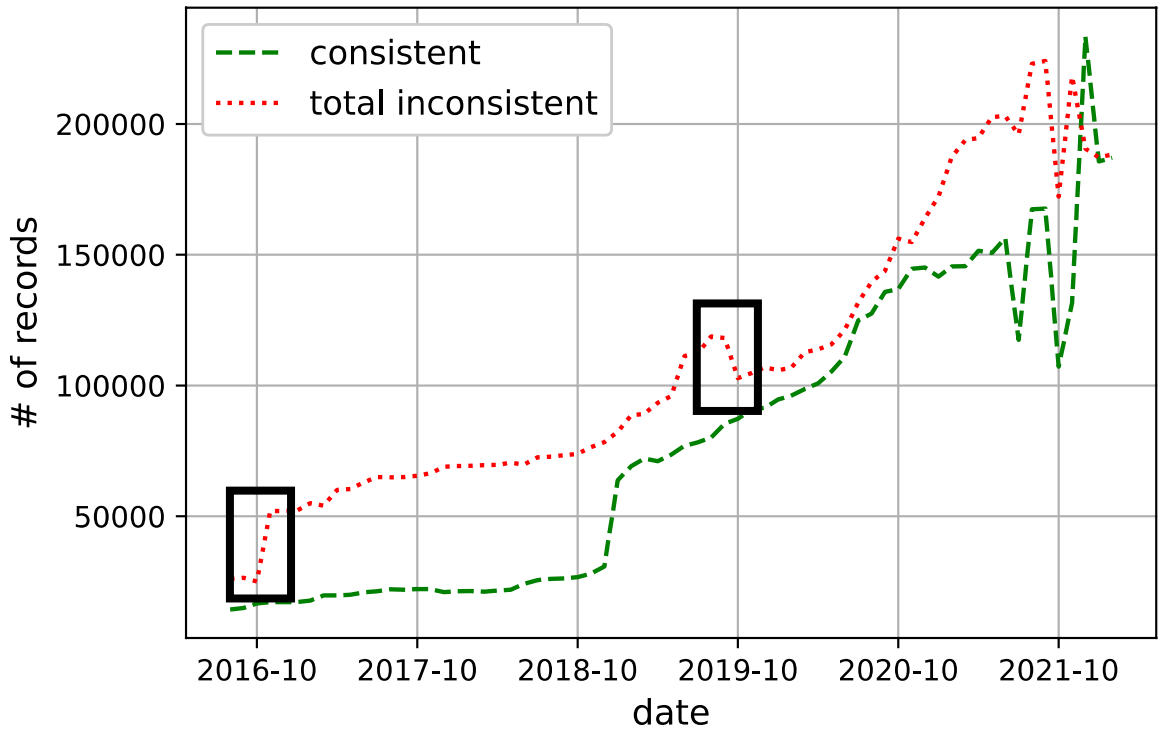


RADB Has More Inconsistency than Consistency



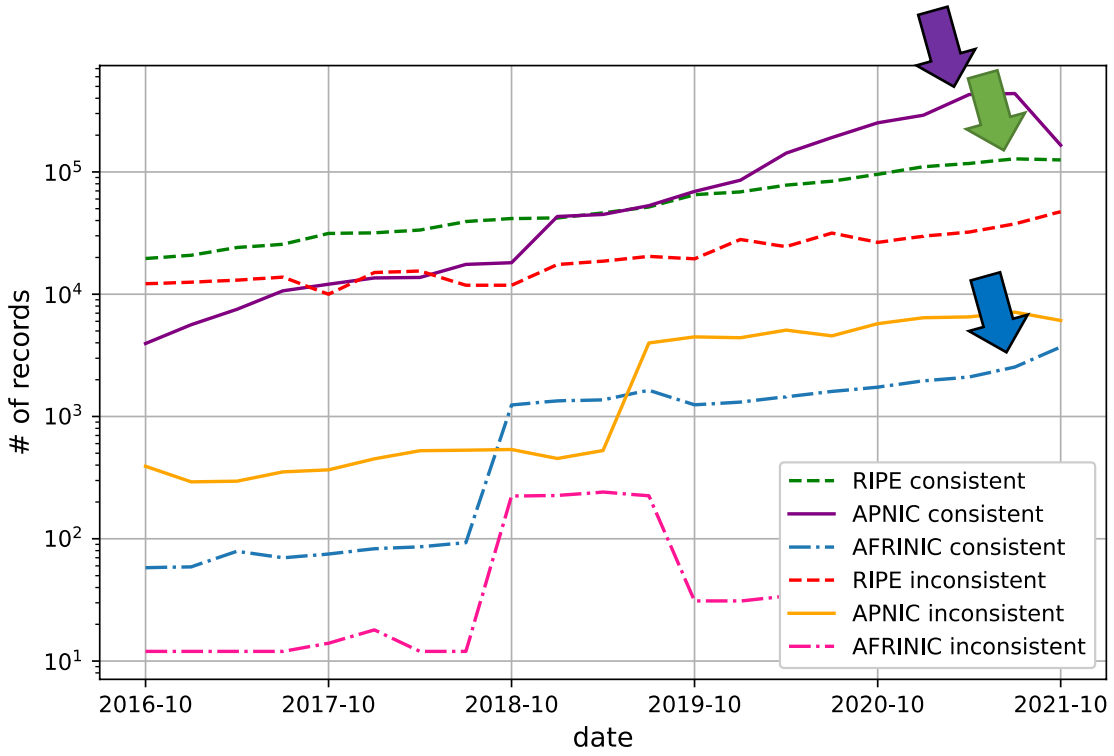
- As of October 2021, **38%** of v4 records in RADB with matching ROAs are consistent with RPKI
- We identify some potential causes in the paper
  - Stale records

RADB and RPKI Inconsistency – Verisign Customers



- Verisign customers registered their prefixes and ASes in RPKI in Oct. 2016
- Verisign removed inconsistent records in Sept. 2019
- Around 26k records were involved in each event

Authoritative IRR Databases Have More Consistency



- As of Oct 2021:
- **73%** RIPE IRR records with matching ROAs are consistent with RPKI
- **98%** APNIC IRR records are consistent
- **93%** AFRINIC IRR records are consistent
- RIRs run an authorization process every time a route object is created

Conclusion

- 62% of RADB v4 records with matching ROAs are inconsistent with RPKI
  - Fragmented prefixes registered in RADB
  - Stale records
  - Neglected customer-provider dynamics
- 27% of RIPE, 2% of APNIC, and 7% of AFRINIC authoritative IRR records with matching ROAs are inconsistent with RPKI
  - IRR database providers could adopt policies that promote good hygiene
- Networks that register in IRR databases should regularly update their records