

Measured Approaches to IPv6 Address Anonymization and Identity Association

ACM IMC PRIME Workshop – Madison, WI – 27 Oct 2025

David Plonka <plonka@wiscnet.net|research@wiscnet.net> & Arthur Berger

<https://research.wiscnet.net/~plonka/pubs.html>

“The agurify Tool: a kIP reference implementation” (IETF 105 Hackathon, 2019)

“kIP: a Measured Approach to IPv6 Address Anonymization” (2017)

<https://arxiv.org/abs/1707.03900>



Premise: an Intersection of Privacy and Security

- **Privacy: Truncation and/or aggregation-based anonymization**
i.e., for reporting traffic data, *e.g.*, correlating with network topology, routing, service providers, and geographic locations.
- **Security: in coordinated attack response**
 - Sharing IP address info while respecting victim or suspect attacker's privacy.
 - Mitigating abuse by blocking traffic associated with a victim and/or attacker.

Effectiveness depends on knowledge - or on assumptions - about globally-routed IP address prefixes – the *Identity Associations* (or IAs) – of the victims or attackers.

IP Address Anonymization and Identity Association

Consider these questions:

- *How can Internet measurements inform decisions about address anonymization and identity association?*

IP Address Anonymization and Identity Association

Consider these questions:

- How can passive and active Internet measurements inform decisions about address anonymization and identity association?
- *Is there any reason to believe that any one IP prefix length would perform satisfactorily for either? e.g., /24 in IPv4 or /48 in IPv6?*

IP Address Anonymization and Identity Association

Consider these questions:

- How can passive and active Internet measurements inform decisions about address anonymization and identity association?
- Is there reason to believe that any one IP prefix length would perform satisfactorily for either? e.g., /24 in IPv4 or /48 in IPv6?

IP Address Anonymization

- ***Truncation-based anonymization is ideal if, and only if, it can be guaranteed to improve privacy.***

**We propose k IP anonymization, *i.e.*,
make an individual appear indistinguishable amongst a set of $[k]$ individuals,
an *anonymity set***

[<https://en.wikipedia.org/wiki/K-anonymity>,
RFC 6973: “Privacy Considerations for Internet Protocols”]

IP Address Anonymization in Practice, Today

Announcing the Results of the 1.1.1.1 Public DNS Resolver Privacy Examination

2020-03-31

 John Graham-Cumming

6 min read

This post is also available in [简体中文](#), [Deutsch](#) and [Français](#).



address) will not be stored in non-volatile storage. Cloudflare will anonymize source IP addresses via IP truncation methods (last octet for IPv4 and last 80 bits for IPv6). Cloudflare will delete the truncated IP address within 25 hours.

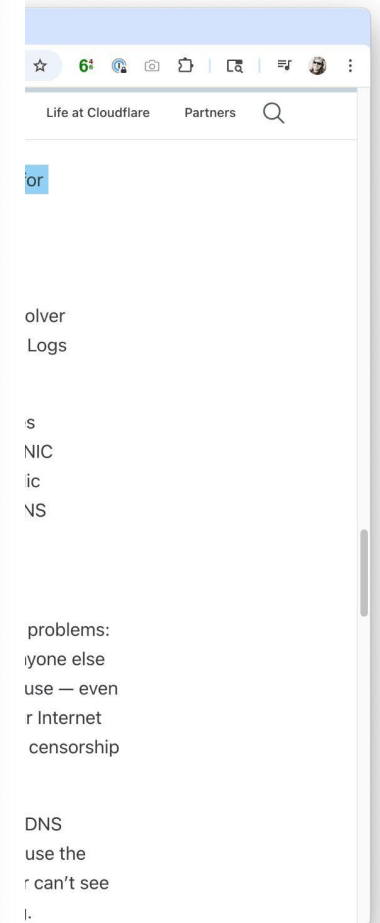
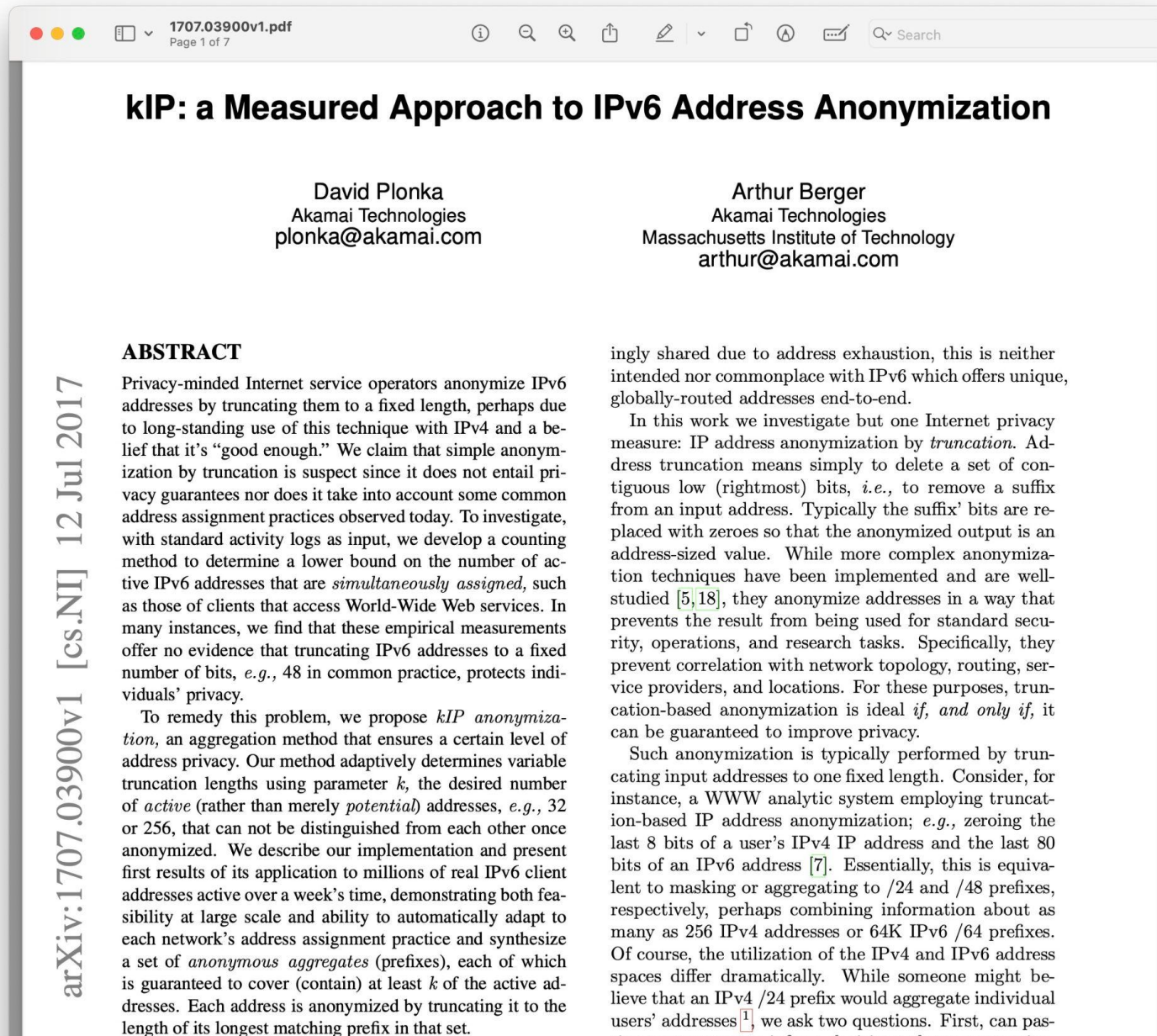
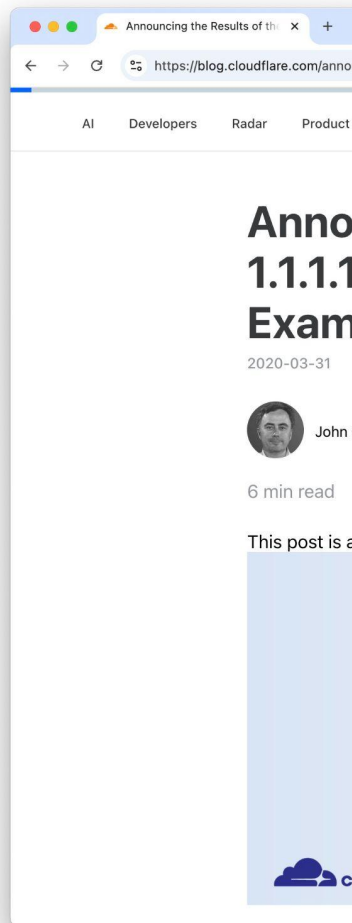
4. Cloudflare will retain only the limited transaction and debug log data ("Public Resolver Logs") for the legitimate operation of our Public Resolver and research purposes, and Cloudflare will delete the Public Resolver Logs within 25 hours.
5. Cloudflare will not share the Public Resolver Logs with any third parties except for APNIC pursuant to a Research Cooperative Agreement. APNIC will only have limited access to query the anonymized data in the Public Resolver Logs and conduct research related to the operation of the DNS system.

Proving privacy commitments

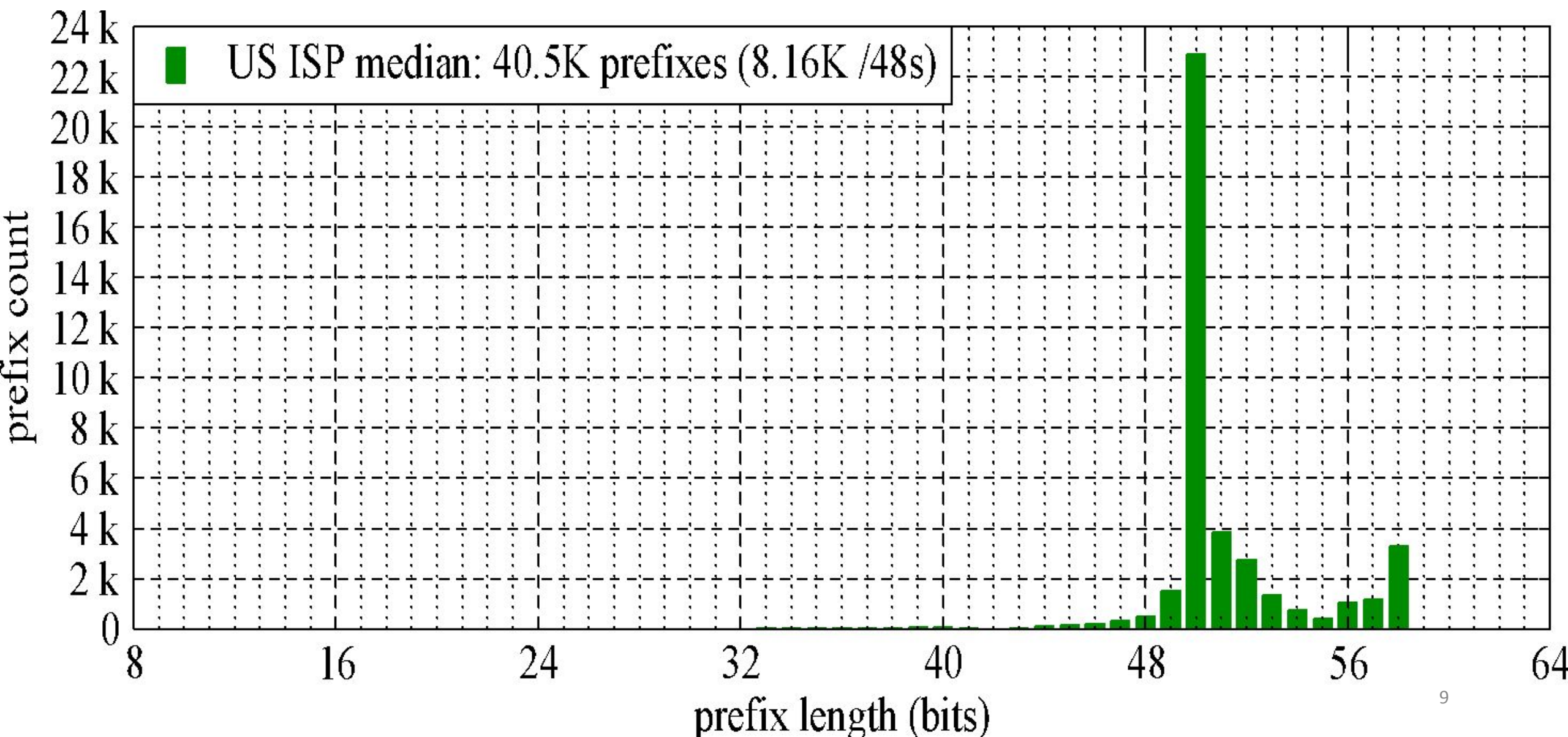
We created the 1.1.1.1 resolver because we recognized significant privacy problems: ISPs, WiFi networks you connect to, your mobile network provider, and anyone else listening in on the Internet can see every site you visit and every app you use — even if the content is encrypted. Some DNS providers even sell data about your Internet activity or use it to target you with ads. DNS can also be used as a tool of censorship against many of the groups we protect through our [Project Galileo](#).

If you use DNS-over-HTTPS or DNS-over-TLS to our 1.1.1.1 resolver, your DNS lookup request will be sent over a secure channel. This means that if you use the 1.1.1.1 resolver then in addition to our privacy guarantees an eavesdropper can't see your DNS requests. We promise we won't be looking at what you're doing.

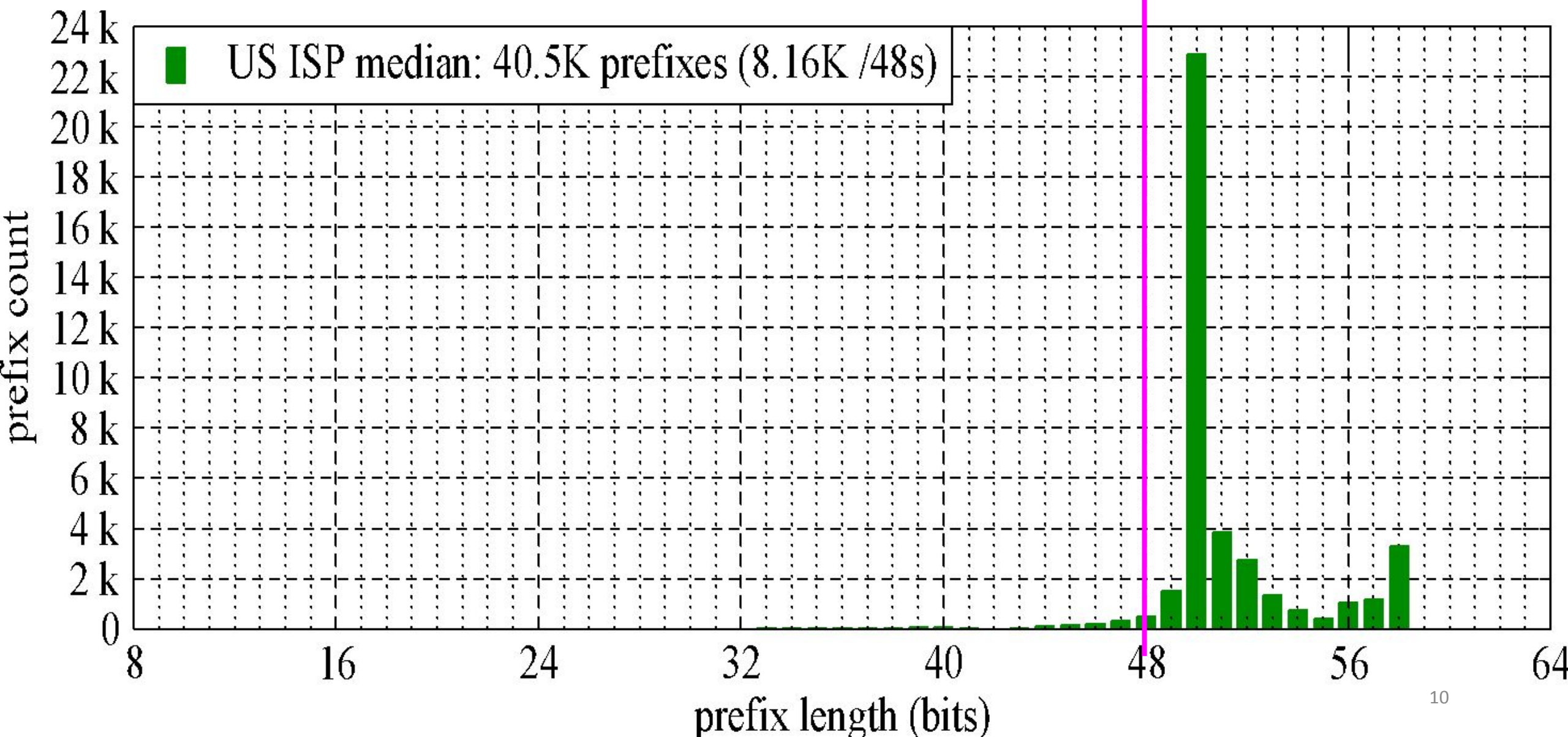
IP Address Anonymization in Practice, Today



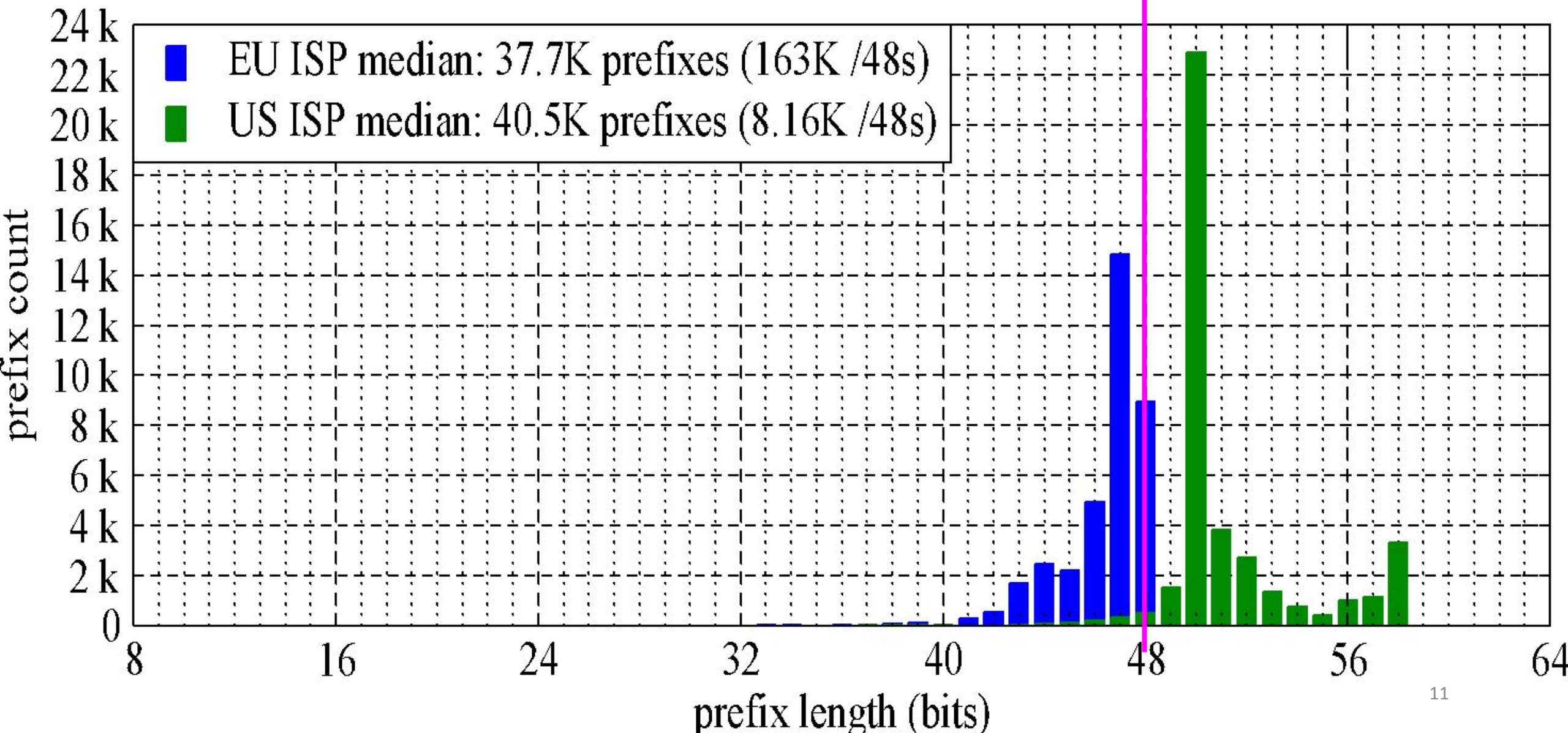
Histogram: **k=32** anonymous aggregate prefix lengths (w=7d, i=1h)



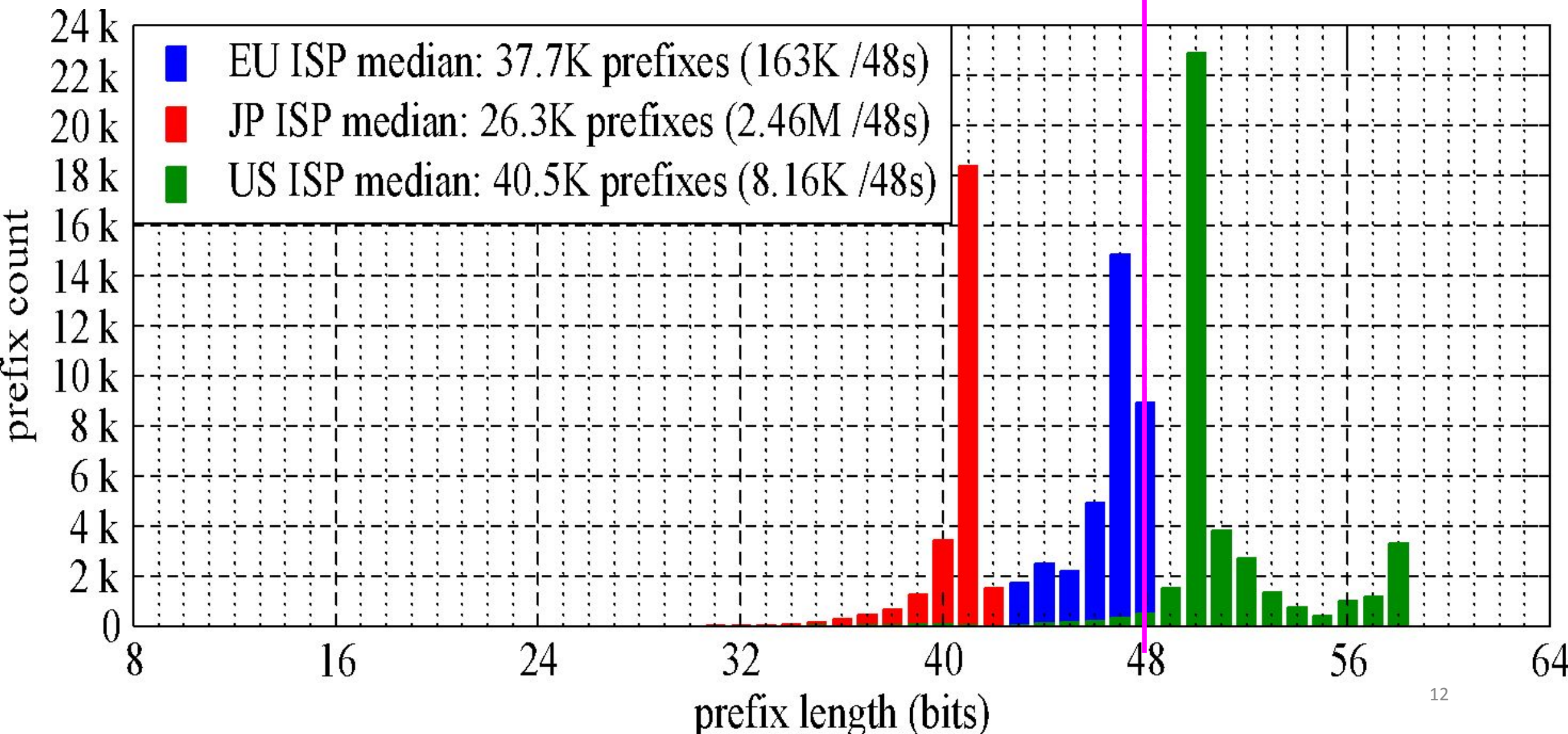
Histogram: **k=32** anonymous aggregate prefix lengths (w=7d, i=1h)



Histogram: k=32 anonymous aggregate prefix lengths (w=7d, i=1h)



Histogram: k=32 anonymous aggregate prefix lengths (w=7d, i=1h)



Some Prompts for Discussion

- Should there be a way to remotely **query for an IP address' preferred prefix length** to *(a)* **anonymization by truncation** or for its *(b)* **identity association**?

If this were implemented, e.g., in the DNS similarly to `ip6.arpa`, the default value on lookup failure could be the length of the covering BGP prefix that must exist for globally-routable addresses.

Is this a reasonable mechanism to also advertise different prefix lengths for different uses, e.g., anonymization within an organization (TLP:AMBER) versus outside (TLP:CLEAR)?

Some Prompts for Discussion

- Should there be a way to remotely **query for an IP address' preferred prefix length** to (a) **anonymization by truncation** or for its (b) **identity association**?

If this were implemented, e.g., in the DNS similarly to `ip6.arpa`, the default value on lookup failure could be the length of the covering BGP prefix that must exist for globally-routable addresses.

Is this a reasonable mechanism to also advertise different prefix lengths for different uses, e.g., anonymization within an organization (TLP:AMBER) versus outside (TLP:CLEAR)?

- Should administrative policy require **auditing** of the preferred prefix length to measure its effectiveness in **making an individual appear indistinguishable amongst a set of individuals**?

Measured Approaches to IPv6 Address Anonymization and Identity Association

ACM IMC PRIME Workshop – Madison, WI – 27 Oct 2025

David Plonka <plonka@wiscnet.net|research@wiscnet.net> & Arthur Berger

<https://research.wiscnet.net/~plonka/pubs.html>

“The agurify Tool: a kIP reference implementation” (IETF 105 Hackathon, 2019)

“kIP: a Measured Approach to IPv6 Address Anonymization” (2017)

<https://arxiv.org/abs/1707.03900>



Histogram: **k=256** anonymous aggregate prefix lengths (w=7d, i=1h)

