Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web

Austin Hounsel* Kevin Borgolte* Paul Schmitt*
Jordan Holland* Nick Feamster†
Princeton University* University of Chicago†

DNS Privacy Has Become a Significant Concern

- On-path network observers can spy on and tamper with DNS traffic (Do53)
- Two protocols have been proposed to encrypt DNS traffic
  - DNS-over-TLS (DoT): RFC 7858
  - DNS-over-HTTPS (DoH): RFC 8484

https://arxiv.org/abs/1907.08089

Contributions

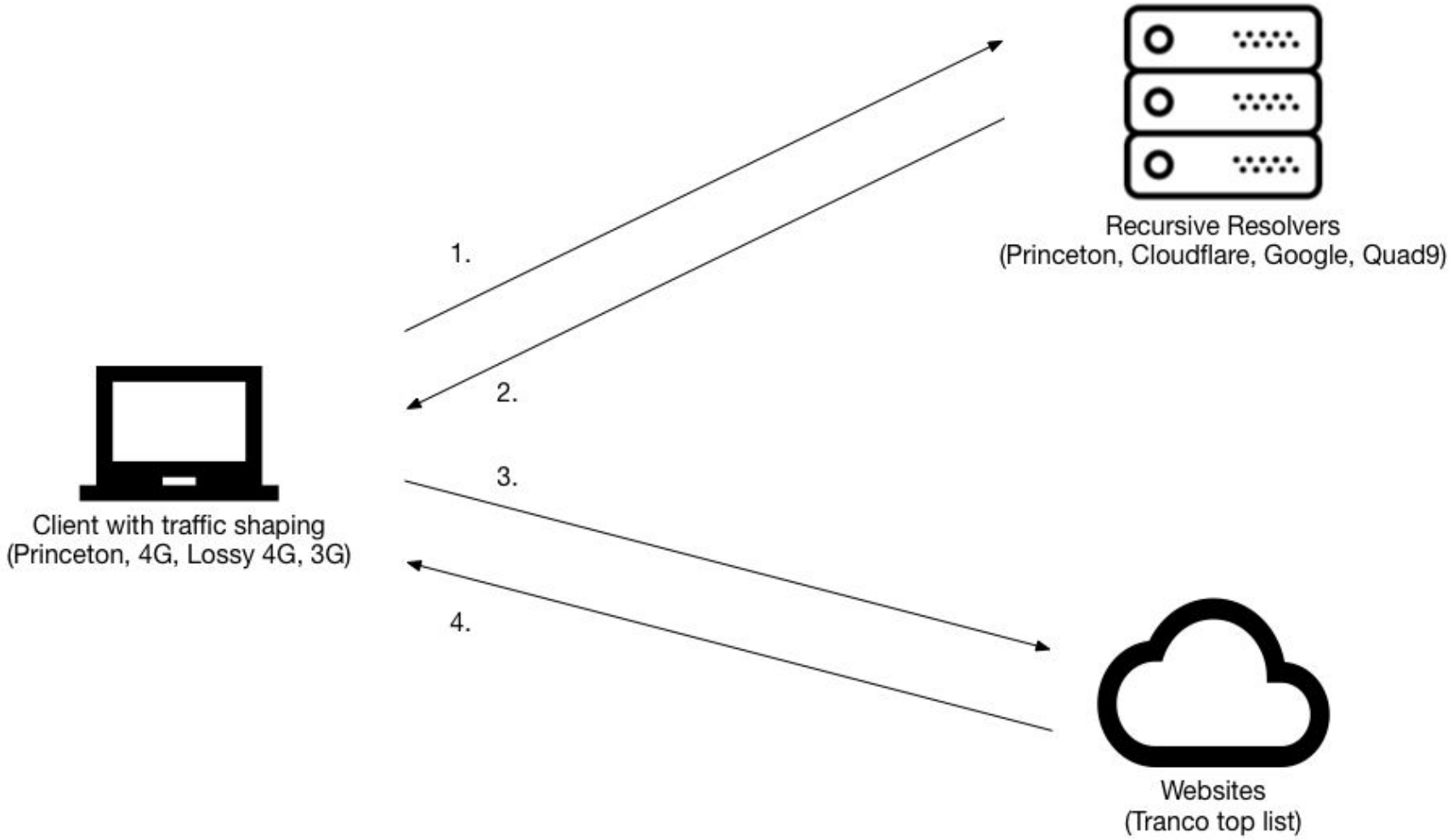
- Extensive performance study of Do53, DoT, and DoH
- Insights to optimize DNS performance

https://arxiv.org/abs/1907.08089

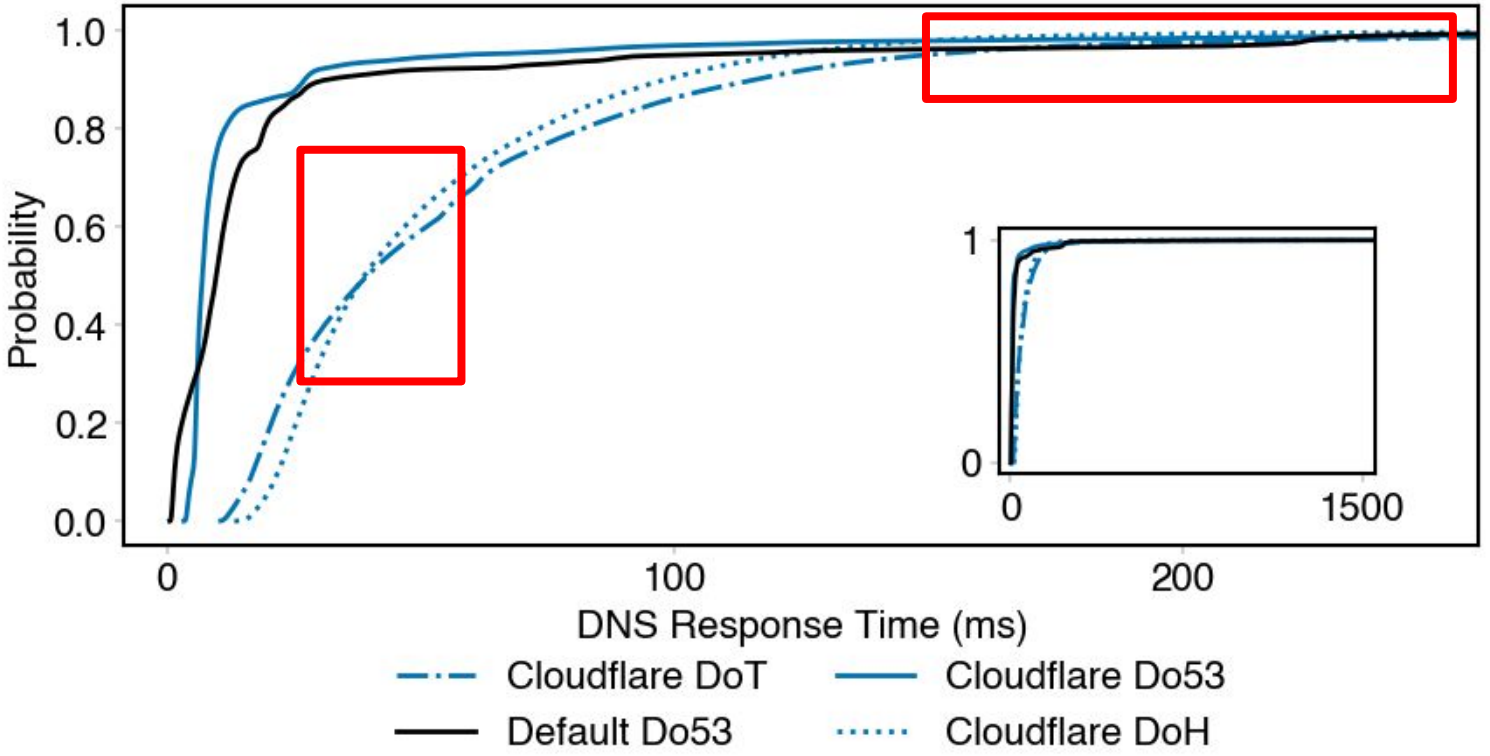
Experiment Overview

- Goal: Understand how Do53, DoT, and DoH affect user experience
  - Query response times
  - Page load times
  - Effect of changing network conditions

https://arxiv.org/abs/1907.08089

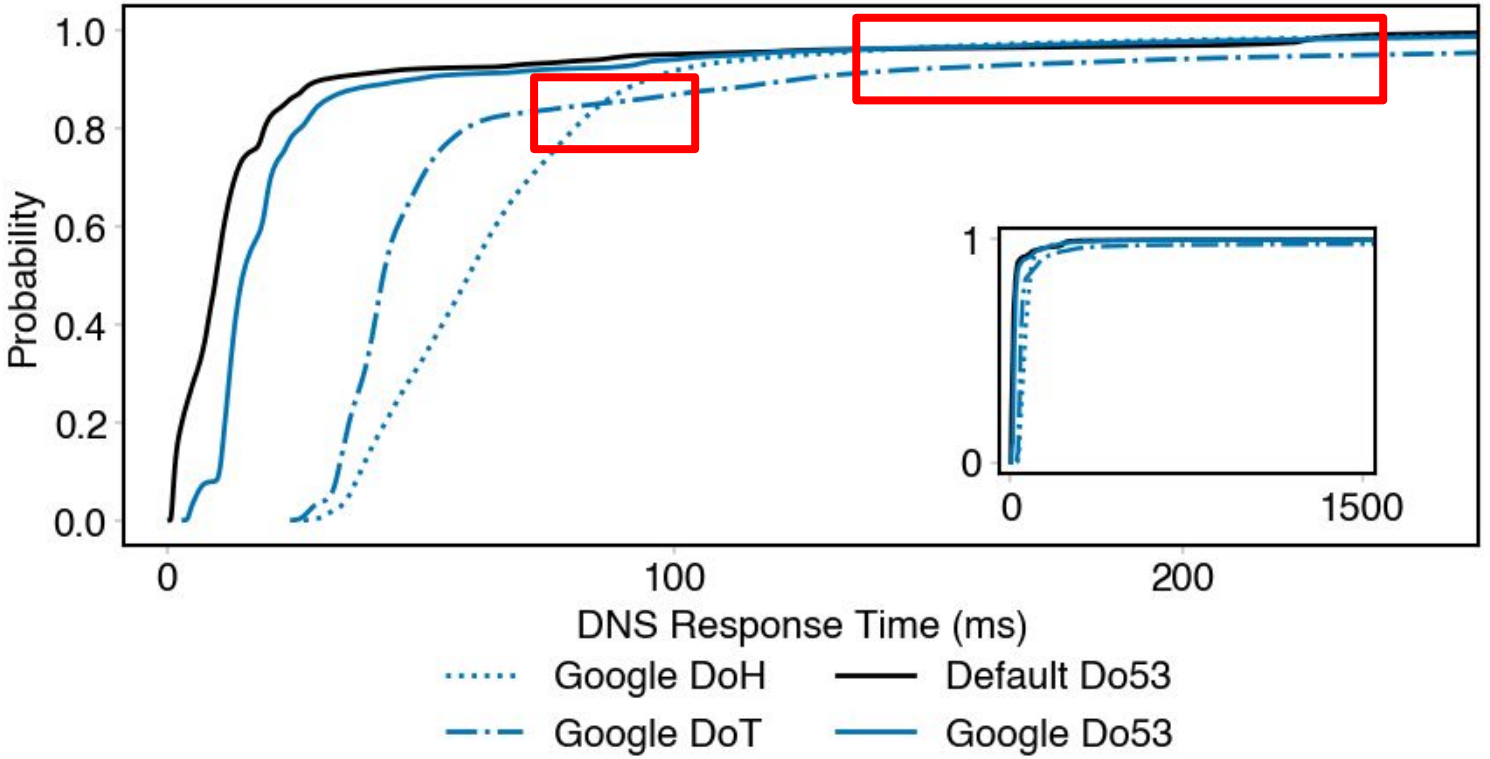

Recursive Resolvers
(Princeton, Cloudflare, Google, Quad9)
1.
2.
3.
4.
Client with traffic shaping
(Princeton, 4G, Lossy 4G, 3G)
Websites
(Tranco top list)

Response Times from Cloudflare on Princeton's Network



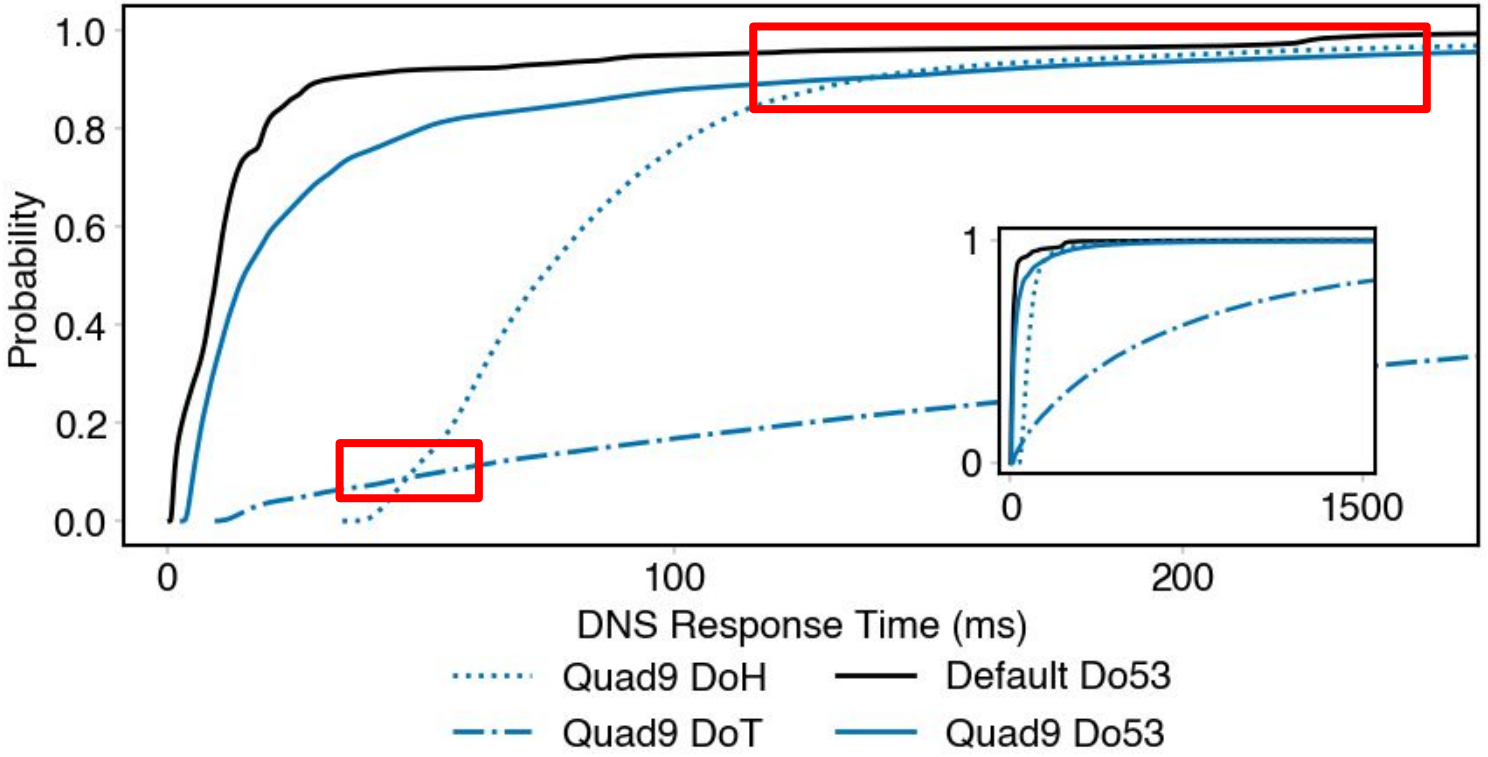
https://arxiv.org/abs/1907.08089

Response Times from Google on Princeton's Network



https://arxiv.org/abs/1907.08089

Response Times from Quad9 on Princeton's Network



https://arxiv.org/abs/1907.08089

Takeaway: DoH Can Outperform Do53

- DoH outperforms Do53 in the tail of response times
  - Caching of DNS wire format?
- This result supports Mozilla’s findings

https://arxiv.org/abs/1907.08089

Measuring Page Load Time

- We measured page load times to understand user experience
- For this talk, we're only focusing on Cloudflare
  - Fastest response times

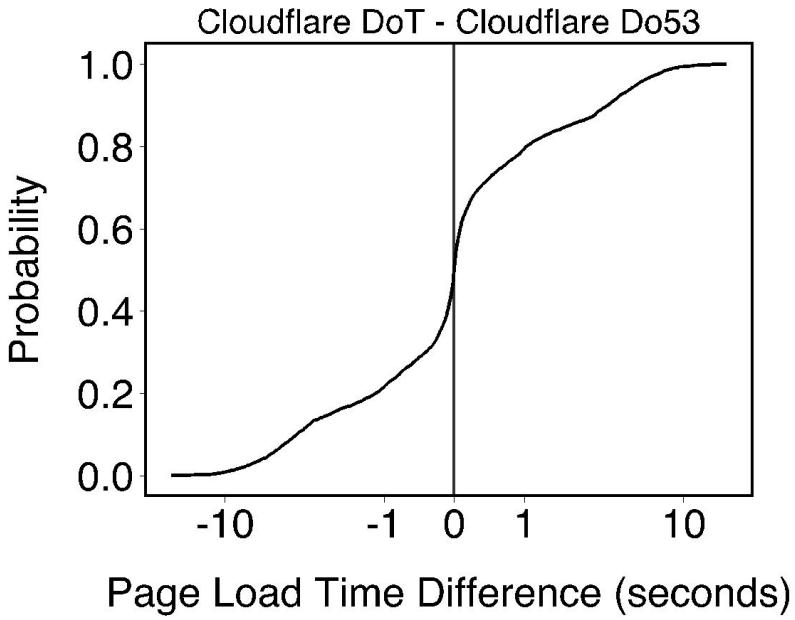
https://arxiv.org/abs/1907.08089

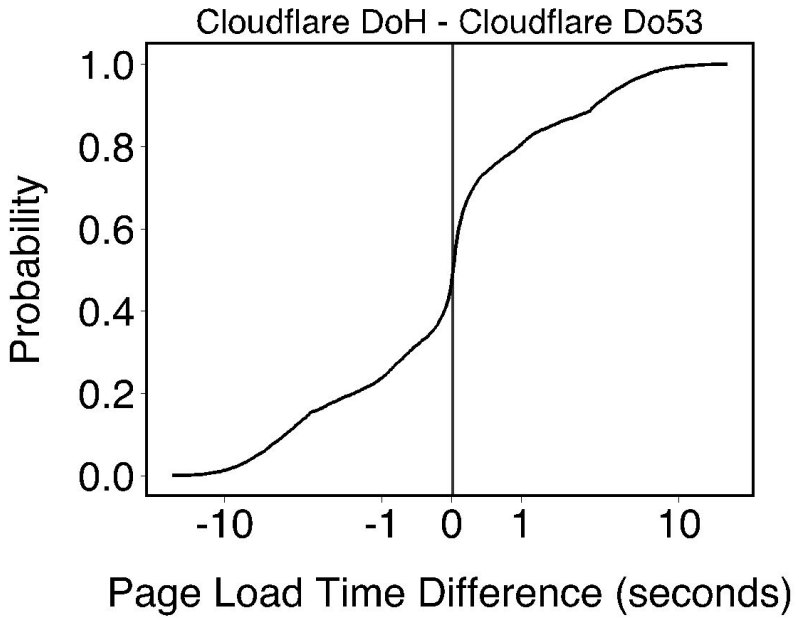
Measuring Page Load Time

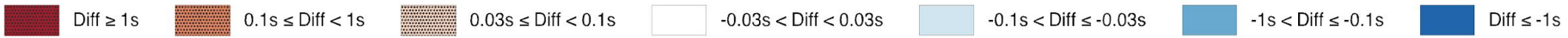
- We also performed traffic shaping
  - Princeton's network was the baseline
  - 4G: 53.3ms additional latency, 1ms jitter, 0.5% loss
  - Lossy 4G: 53.3ms additional latency, 1ms jitter, 1.5% loss
  - 3G: 150ms additional latency, 8ms jitter, 2.5% loss

https://arxiv.org/abs/1907.08089

Page Loads with Cloudflare on Princeton's Network

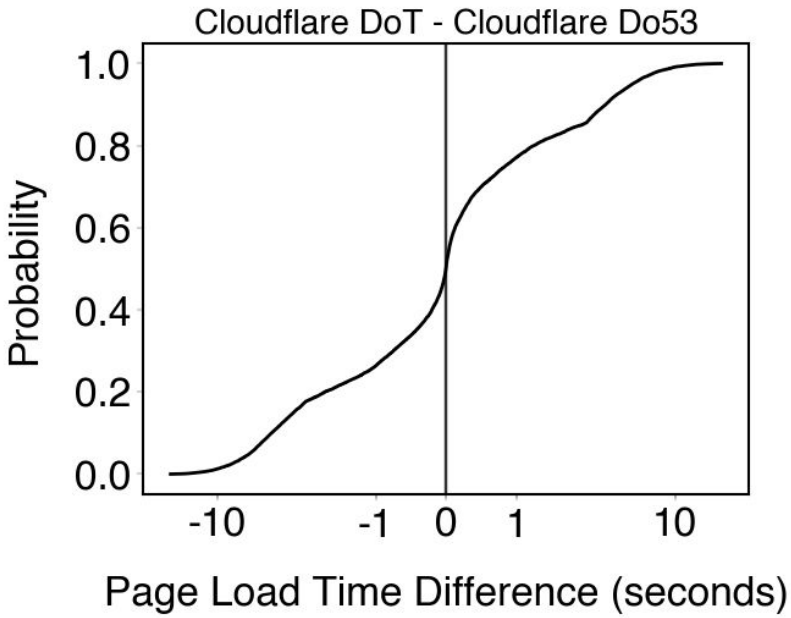


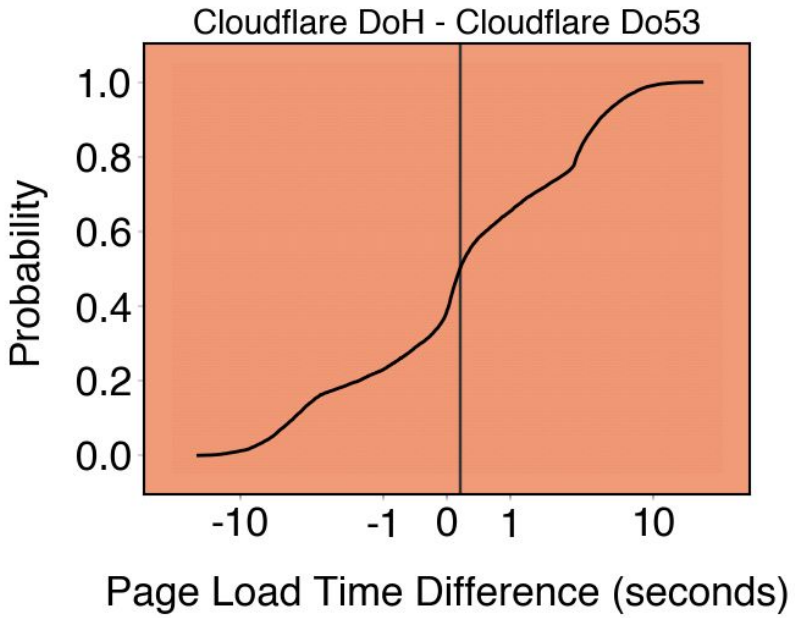


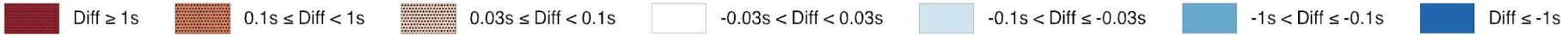


https://arxiv.org/abs/1907.08089

Page Loads with Cloudflare on Emulated 4G Network

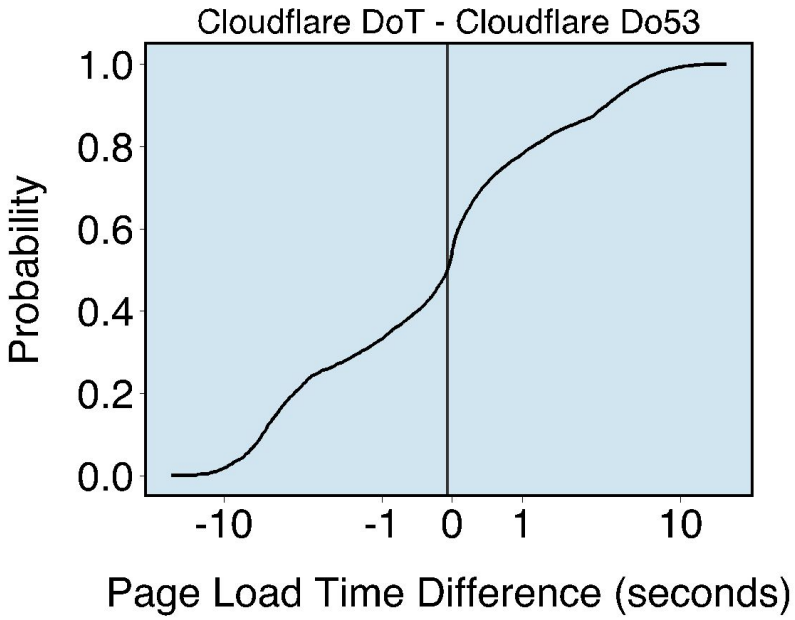


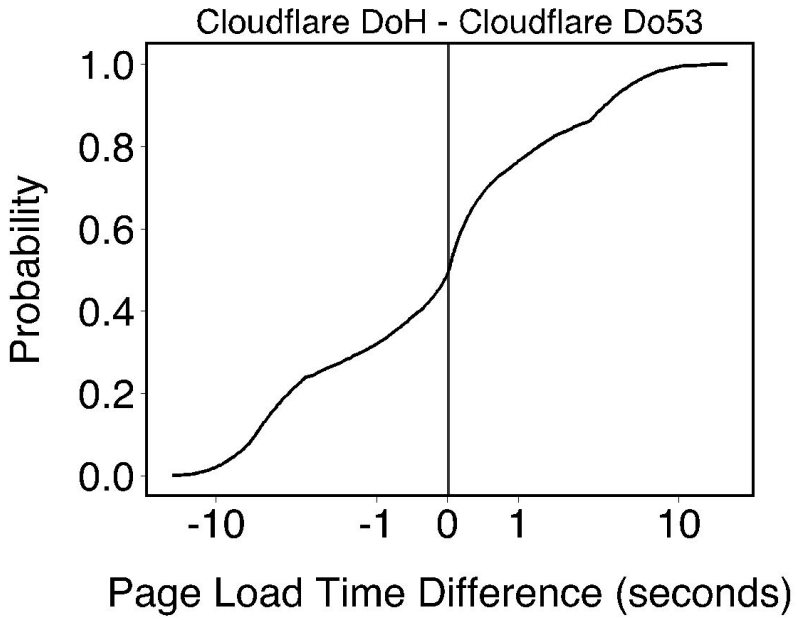


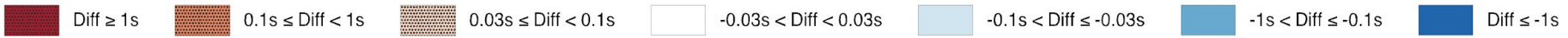


https://arxiv.org/abs/1907.08089

Page Loads with Cloudflare on Emulated, Lossy 4G Network

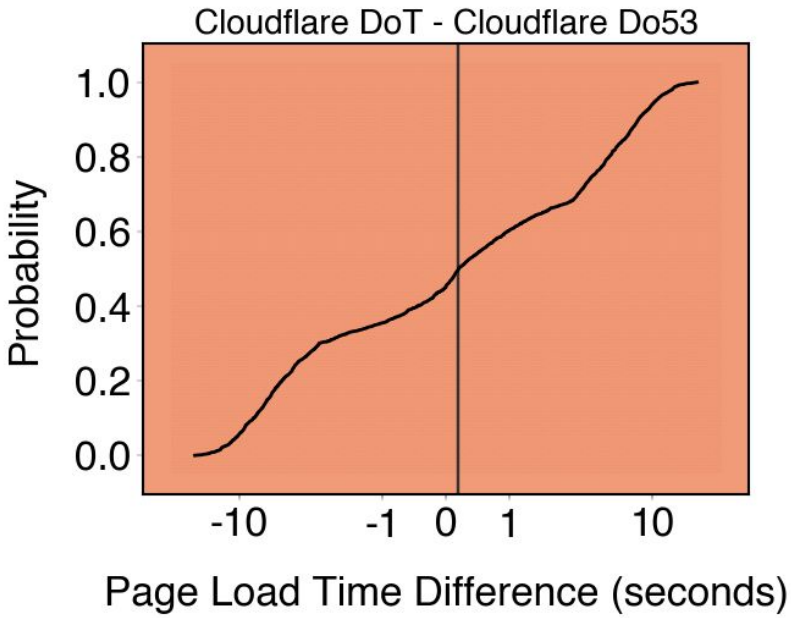


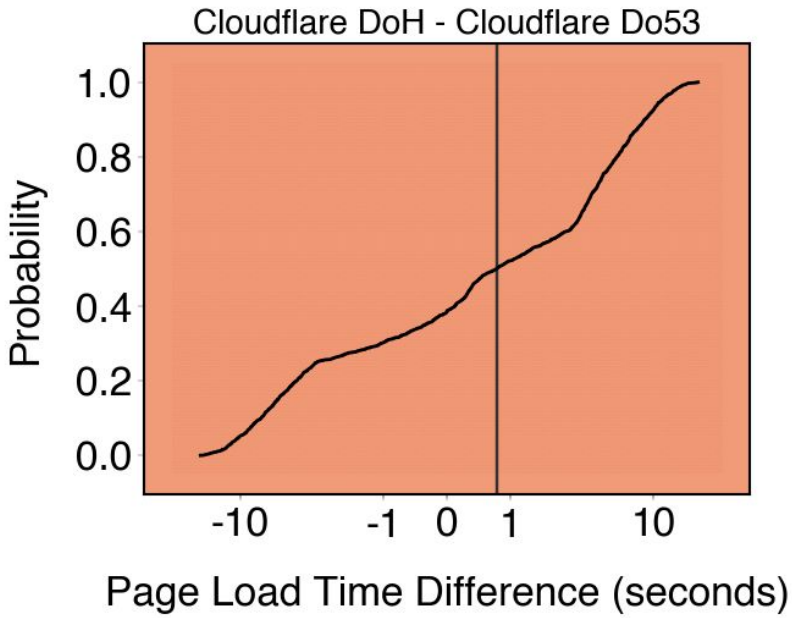


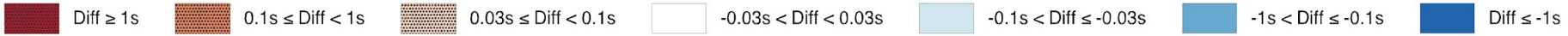


https://arxiv.org/abs/1907.08089

Page Loads with Cloudflare on Emulated 3G Network







https://arxiv.org/abs/1907.08089

Takeaway: DNS-over-TCP Can Help Page Load Times

- TCP packets can be retransmitted as soon as two round-trips
- This helps DoT/DoH perform well on lossy networks
- Timeout for Do53 implementations might be higher

https://arxiv.org/abs/1907.08089

Potential Improvements for Do53, DoT, and DoH

- Opportunistic partial responses
- Wire format caching
- HTTP/2 push for DoH

https://arxiv.org/abs/1907.08089

Conclusion

- **DoT performs better than DoH, and sometimes better than Do53**
- DoH has potential!
- Choice of recursor & network matter
- Transport characteristics of TCP should be explored

Check out the full pre-print: https://arxiv.org/abs/1907.08089