DoH Digests

draft-nottingham-doh-digests-00
DoH’s Goals (for some)

• Provide DNS resolution service that is:
  • Resistant to on-path changes = **encrypted**
  • Harder to discriminate from other traffic = **HTTP**
What’s a Good DoH Server?

- **High-Traffic** = easier to “hide” DoH traffic
- **Popular** = blocking has more impact, less likely (?)
- **Distributed** = lower latency, more reliable

*Observation: most big Web sites, CDNs fit these criteria well*
How do we encourage big sites to serve DoH?
DoH’s Benefits to Sites

- **Privacy** - removes one more party from communication

- **Performance** -
  - HTTP client *is* the DNS client
  - Future opportunities like Secondary Certificates

- **Reliability** - removes one more party from communication
The Problem

- Current DoH configuration mechanism is “select a server” — or have one told to you

- This means only one site gets the benefits of being the DoH server

- This seems like a missed opportunity; if the benefits are shared more equitably, it creates incentives for many good DoH servers to be established.
DoH Digests

• A stab at **one** way that we might address The Problem

• DoH client has pre-existing relationships with multiple DoH servers

• DoH client is periodically updated with a bloom filter indicating the hostnames that the servers prefer

• DoH client uses the bloom filters to direct traffic
Why a Bloom Filter?

• Some use cases require a large number of hosts: e.g. CDNs, AWS, Google

• Update period needs to be frequent

• Large number of clients (potentially every Web browser)

• False positives are OK if used with trusted DoH servers
Open Questions

• Is sharing the benefits of DoH a good way to encourage deployment?

• Is prior arrangement the right discovery mechanism?

• Is a bloom filter the right protocol element?

• What’s an acceptable delay before an update?

• Can this be generalised to work on even more sites?