

# Anonymity Sets in ECH

...

Jonathan Hoyland

# Anonymity Sets

In ECH the public name, a.k.a. the outer SNI, reveals the operator of the ECH system

The size of the anonymity set is capped by the number of hidden names per public name

Can we make the different anonymity sets (i.e. public names) indistinguishable?

- Across all servers?
- Across all operators?

# Client Re-randomisation

Some encryption schemes can be re-randomised

$$\text{decrypt}(\text{rerandomise}^*(\text{encrypt}(x, \text{pk})), \text{sk}) = x$$

Let the authoritative DNS set the public name to

$$\text{encrypt}(x, \text{pk})$$

Let the client set the outer SNI to

$$\text{rerandomise}(\text{encrypt}(x, \text{pk}))$$

# Benefits

- Every connection uses a unique outer SNI
- The outer SNI never appears in an ECHConfig
- Two connections to the same website are indistinguishable from two connections to different websites
- **Traffic to all anonymity sets has exactly the same outer SNI format**
- Without extra metadata (e.g. destination IP) all PNs are indistinguishable

# Client Blinding

A simpler approach is to use blinding

Let the authoritative DNS set the public name to

$g^y, pn$

Let the client set the outer SNI to

$g^x, h(g^{xy}, pn)$

This achieves the same goals, but is easier to reason about

Adding the client key share in to the hash prevents cut-and-paste attacks

$g^x, h(g^{xy}, \text{key share}, pn)$

# Issues

## No GREASE?

- This makes GREASE traffic easily distinguishable from regular traffic. Just check if the PN appears to be random bytes.
- You could try using rerandomisation to encrypt the GREASE PN, but at that point you're just recreating ECH

## Fallback termination

- The server won't have a certificate for terminating an arbitrary, unpredictable string of bytes
- Use MTs suggestion of including the SPKI of an acceptable certificate in the DNS record