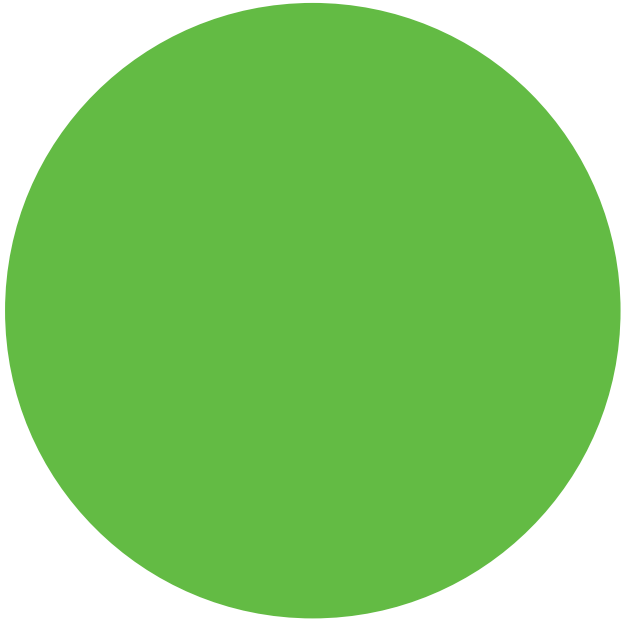
ECH PUBLIC NAMES

ECH ANONYMITY SETS

Ideal: **all public names** are the same

Any name would be equivalent to any other

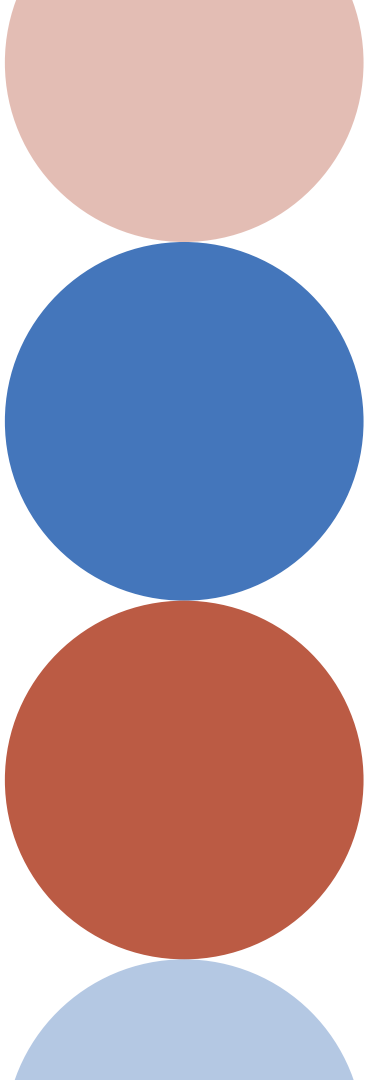
Public names would carry zero information



IN PRACTICE

Different operators have different constraints

and ...

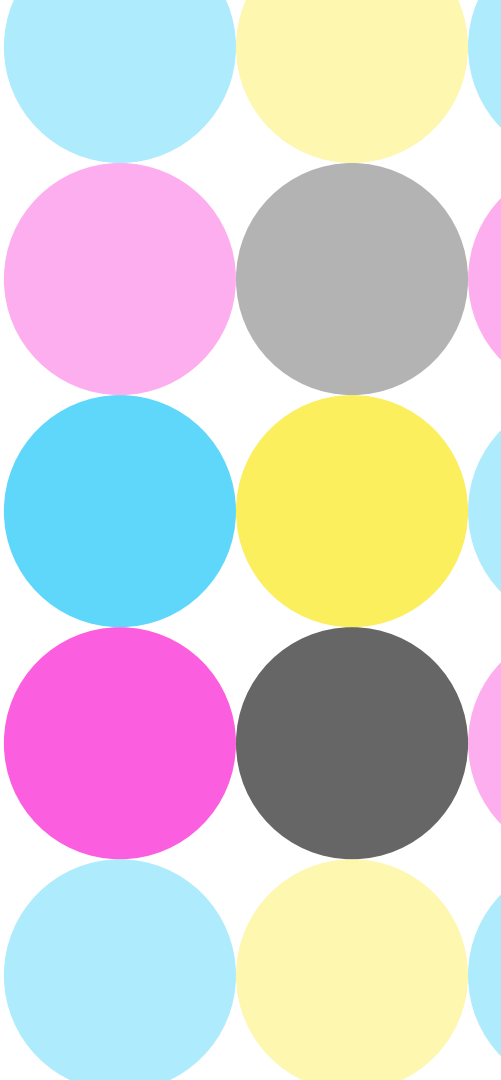


IN PRACTICE

Different operators have different constraints

and configuration management is complex

so anonymity sets might be smaller than ideal



WHAT IF:

EVERY CONNECTION USED A DIFFERENT PUBLIC NAME? 🤔

PER-CONNECTION PUBLIC NAMES

Each public name could be an encryption
of an identifier for the ECH configuration (`CONFIG_ID`)

```
PUBLIC_NAME = E(CONFIG_ID)
```

Or, if `CONFIG_ID` is unique to a `HIDDEN_NAME`

```
PUBLIC_NAME = E(HIDDEN_NAME)
```

Use a fresh encryption for every connection attempt

IDEAL

The anonymity set for

```
PUBLIC_NAME = E(HIDDEN_NAME)
```

is every connection where the mapping is unknown to an adversary

No good if the adversary learns the mapping

```
PUBLIC_NAME -> HIDDEN_NAME
```

so try to keep that secret

KEEPING MAPPINGS SECRET

Attacker only learns hidden names if

- They can decrypt
- They can infer (from side channels, like IP or website fingerprinting)
- They have the mapping

Therefore, the public-facing server must be the only one able to decrypt

KEEPING MAPPINGS SECRET

Attacker only learns hidden names if

- They can decrypt
- They can infer (from side channels, like IP or website fingerprinting)
- They have the mapping

Real problem, but not in scope here

KEEPING MAPPINGS SECRET

Attacker only learns hidden names if

- They can decrypt
- They can infer (from side channels, like IP or website fingerprinting)
- They have the mapping

We put ECH configurations in DNS, which uses shared caches, ∴ SERIOUS

RETRY CONFIGURATIONS

ECH configurations delivered using Retry

- Each is received by just one client
- Each could be freshly generated

Not really perfect

- Still need a public name (or something) to anchor to
- Can’t deliver a configuration over a successful connection
- Can’t split a single public name into multiple ECH configurations

BOOTSTRAPPING PROBLEM

Getting a retry configuration still requires a public name

… and public names come from DNS records

… DNS records end up in caches at resolvers

… and adversaries probably use the same resolvers

VISITS FROM THE BAD IDEA FAIRY

🧚DISABLE DNS SHARED CACHING

Terrible idea for the health of DNS generally

Might be OK if the authoritative is willing

🧚Authoritative might signal that the zone can be queried directly

🧚EDNS(0) option to disable all caching

🧚LOOSEN RETRY CONFIG AUTHORITY

Today, retry configurations have to come from the public facing server

If they could come from the back end,
successful connections could include updated details

🧚ECH config could be delivered in

- The TLS NewSessionTicket message
- Or even HTTP messages (think `/.well-known/ech-config`)

🧚 ENCRYPT ANYWAY

IN THE DRAFT

Hand out encrypted public names in DNS anyway

Create some plausible deniability for known mappings

- Names that share a config (i.e., those in the true anonymity set) get identical names with non-negligible probability
- Adversary observing a name might be wrong about true mapping NEW
- Adversary observing a name that it couldn't obtain learns nothing BASELINE

Bet on adversaries not having a panopticon
or at least make it expensive for them

🤪 USE RFC 7871
€ KEY ON SOURCE IP