

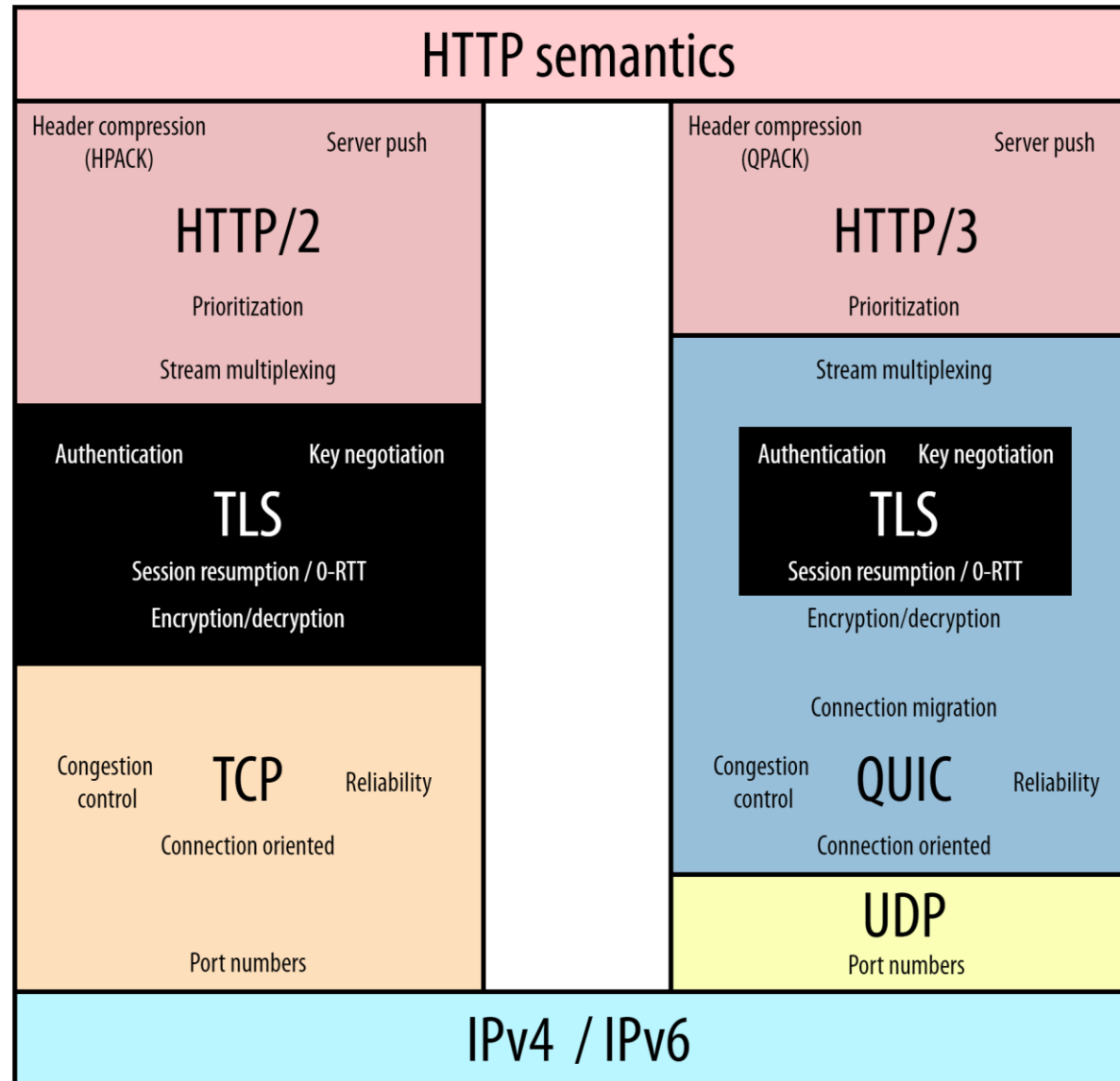
QUIC and HTTP/3 Security

Robin Marx

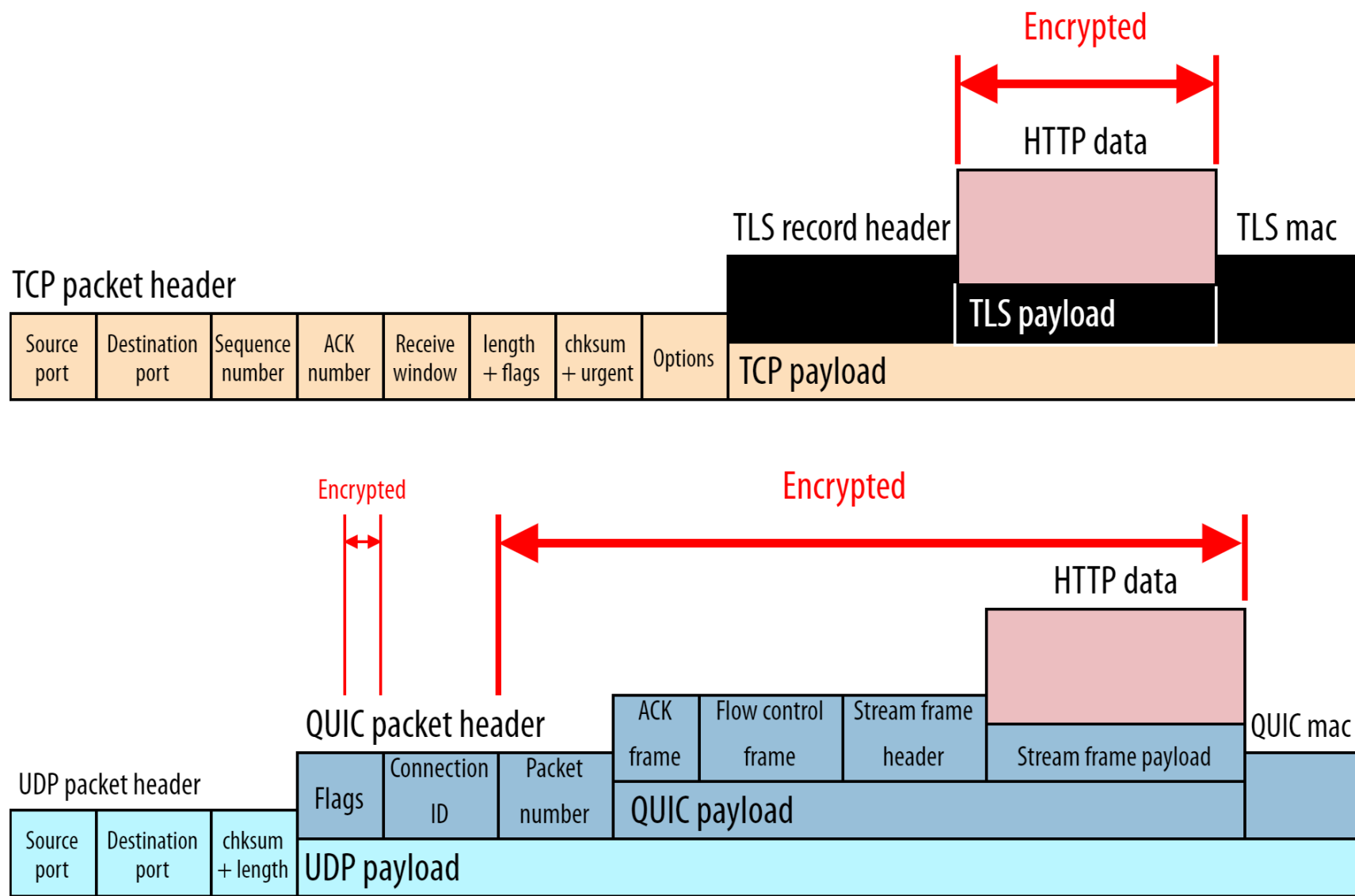
robin.marx@kuleuven.be



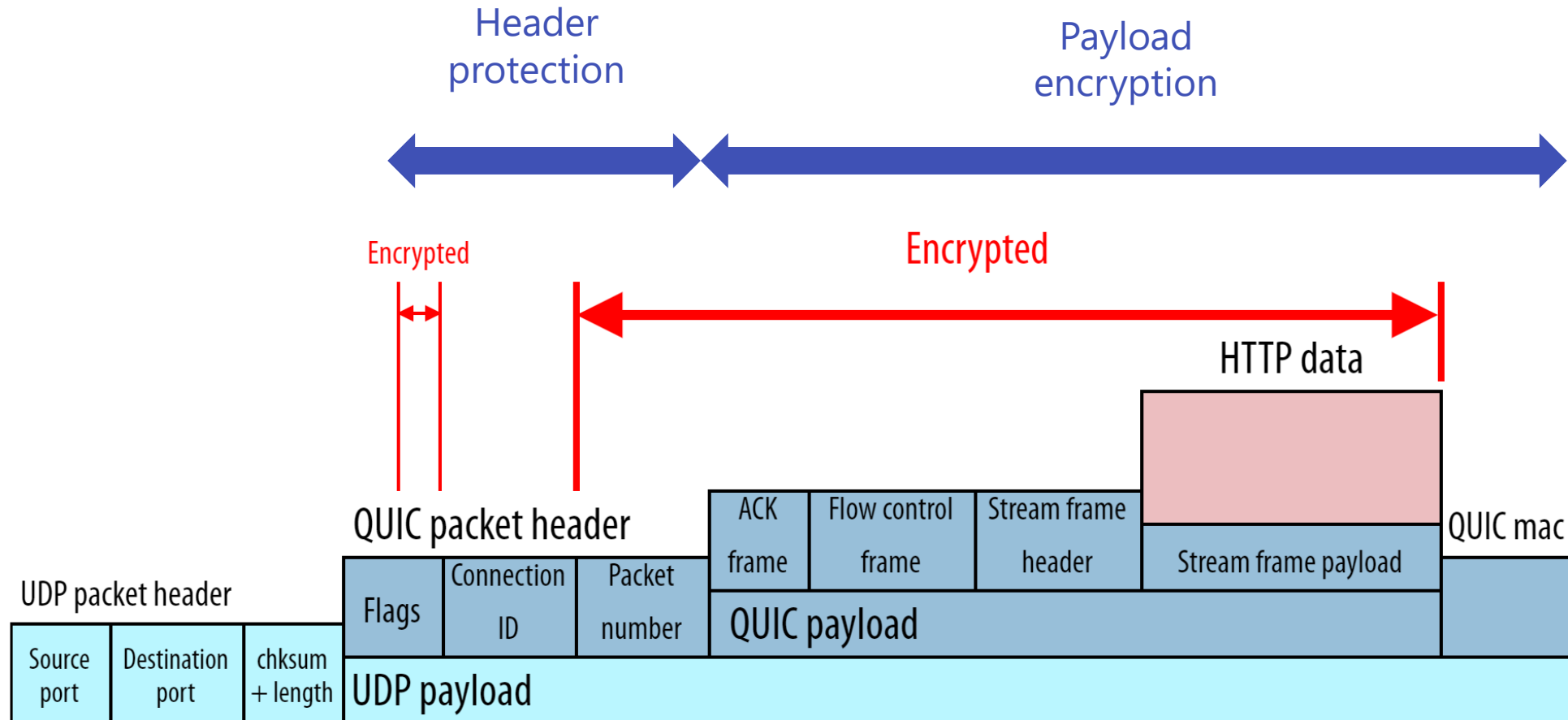
TCP+TLS vs QUIC



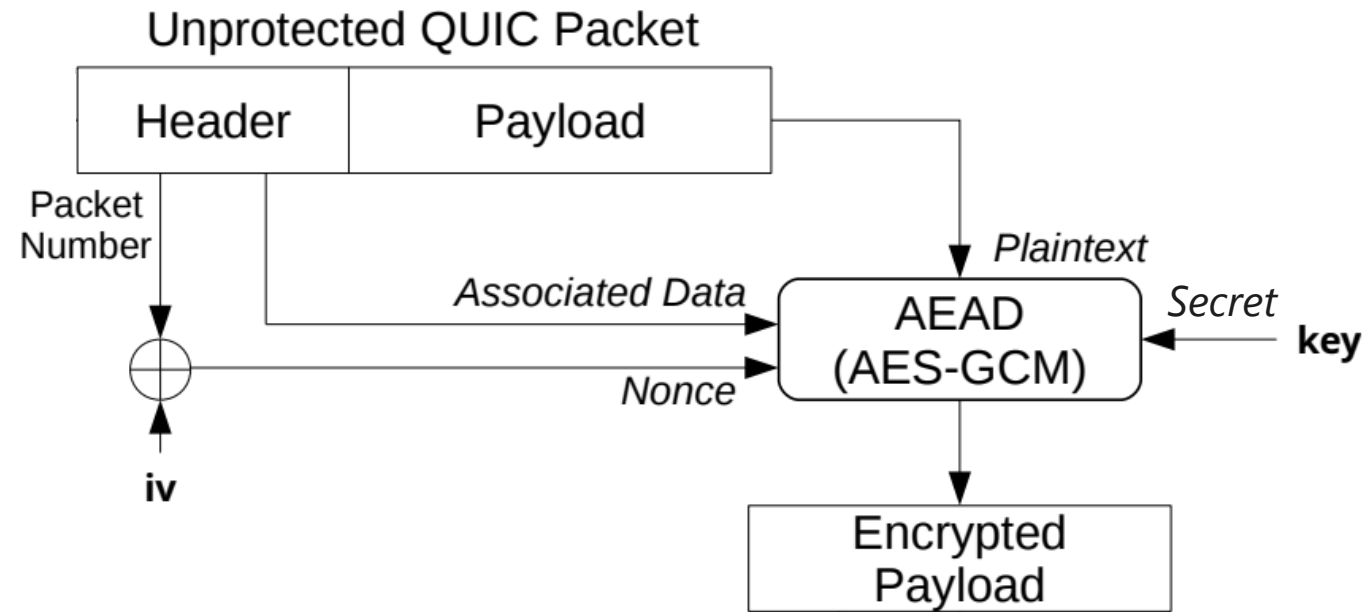
TCP+TLS vs QUIC



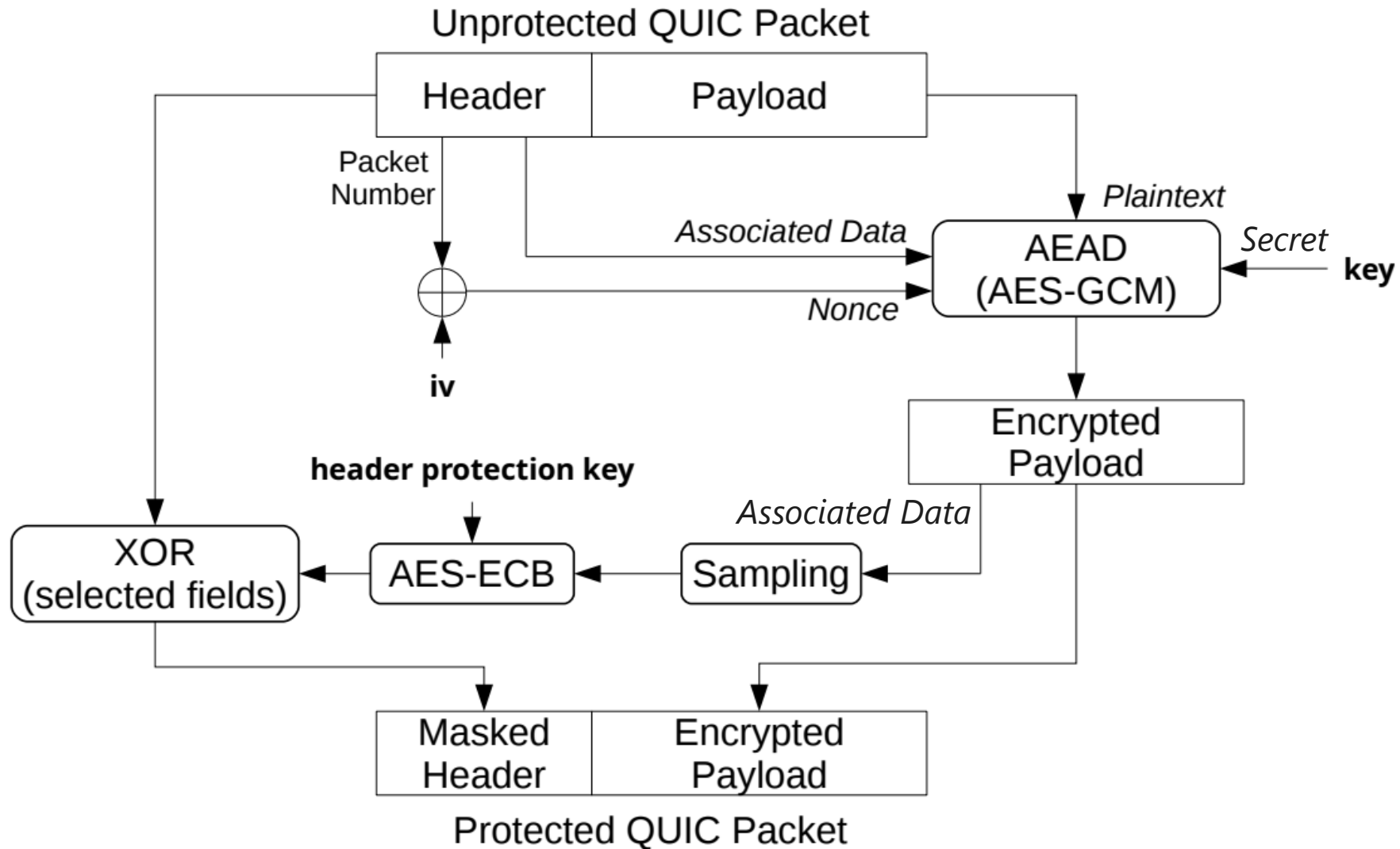
QUIC packets are “encrypted twice”



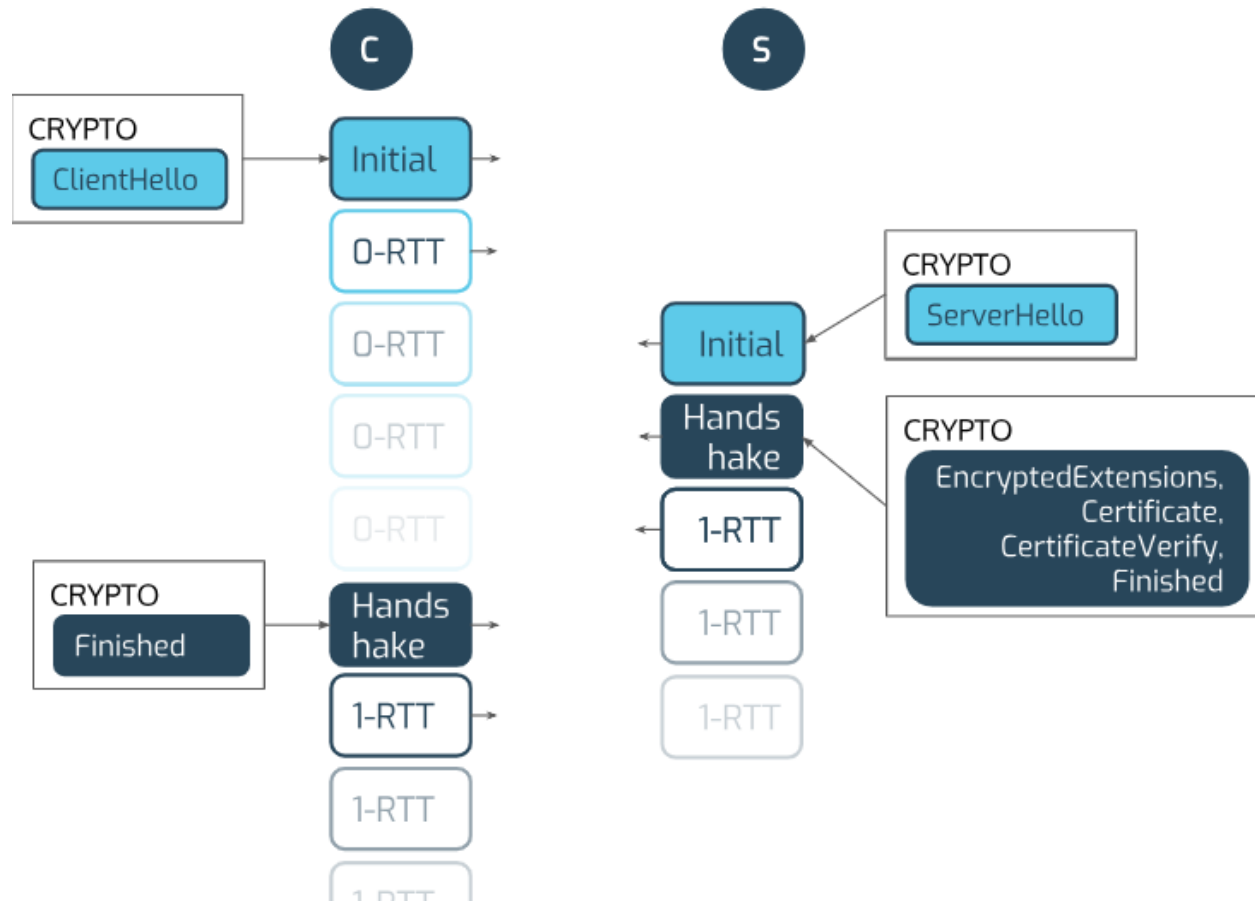
Payload encryption



Header protection and Payload encryption



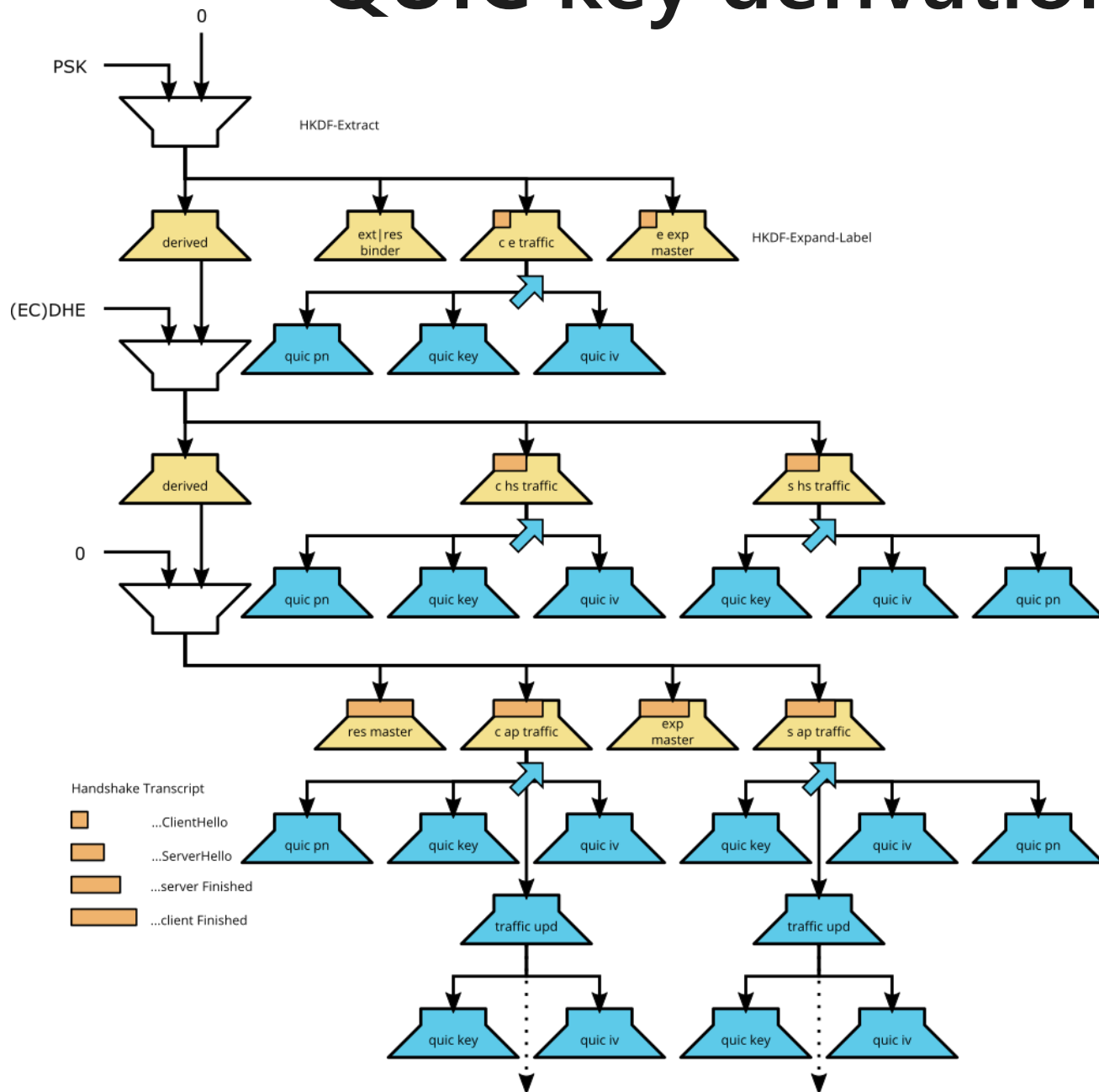
Combined Transport and Crypto handshake



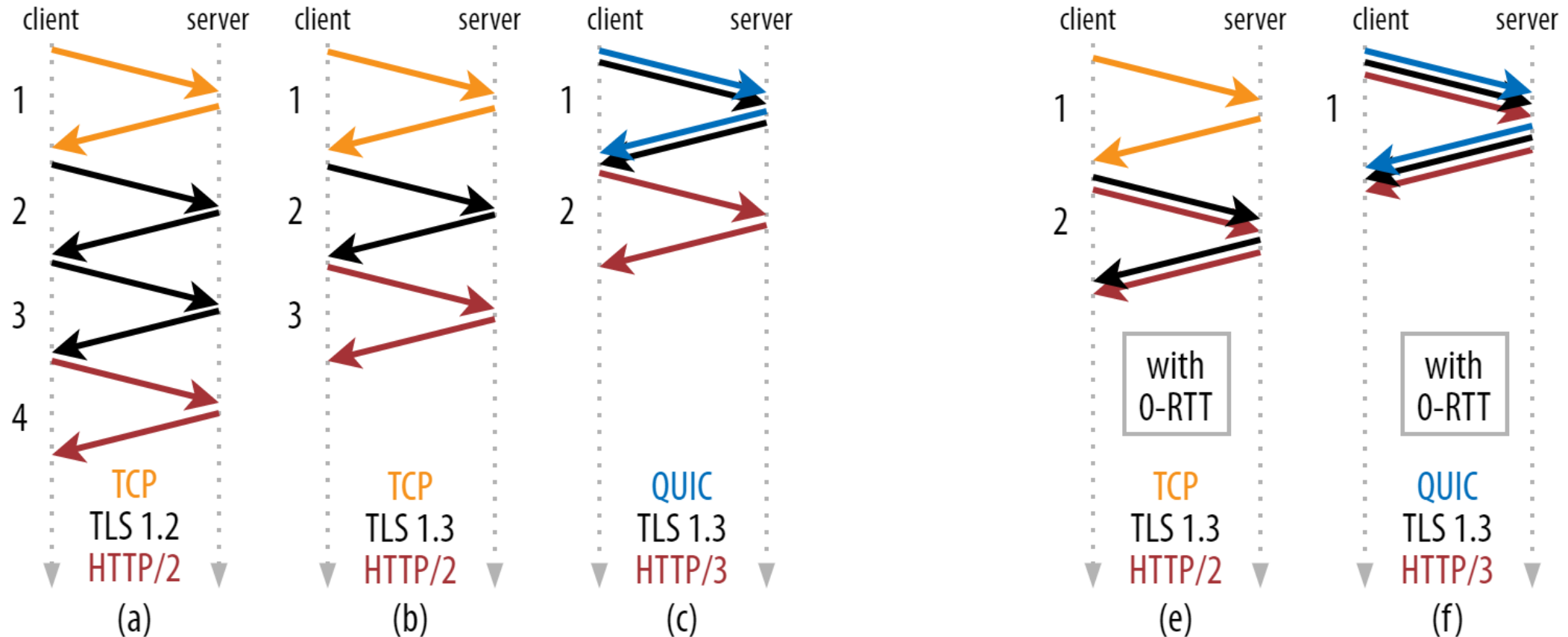
Main differences from TLS 1.3

- Hello's are "encrypted" (obfuscated)
- No EndOfEarlyData message
- **No records!**
 - Replaced by QUIC CRYPTO and STREAM frames
- Separate key derivations

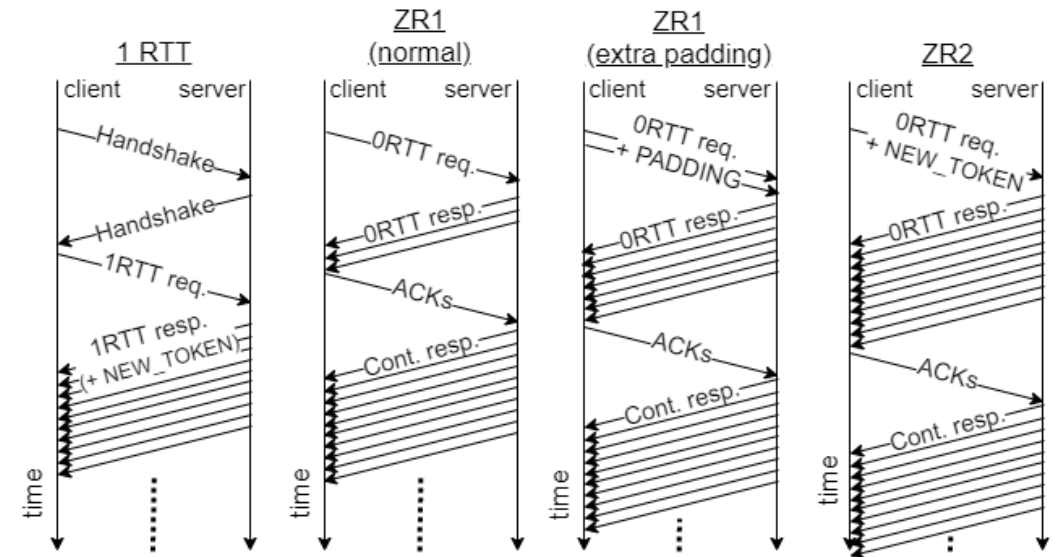
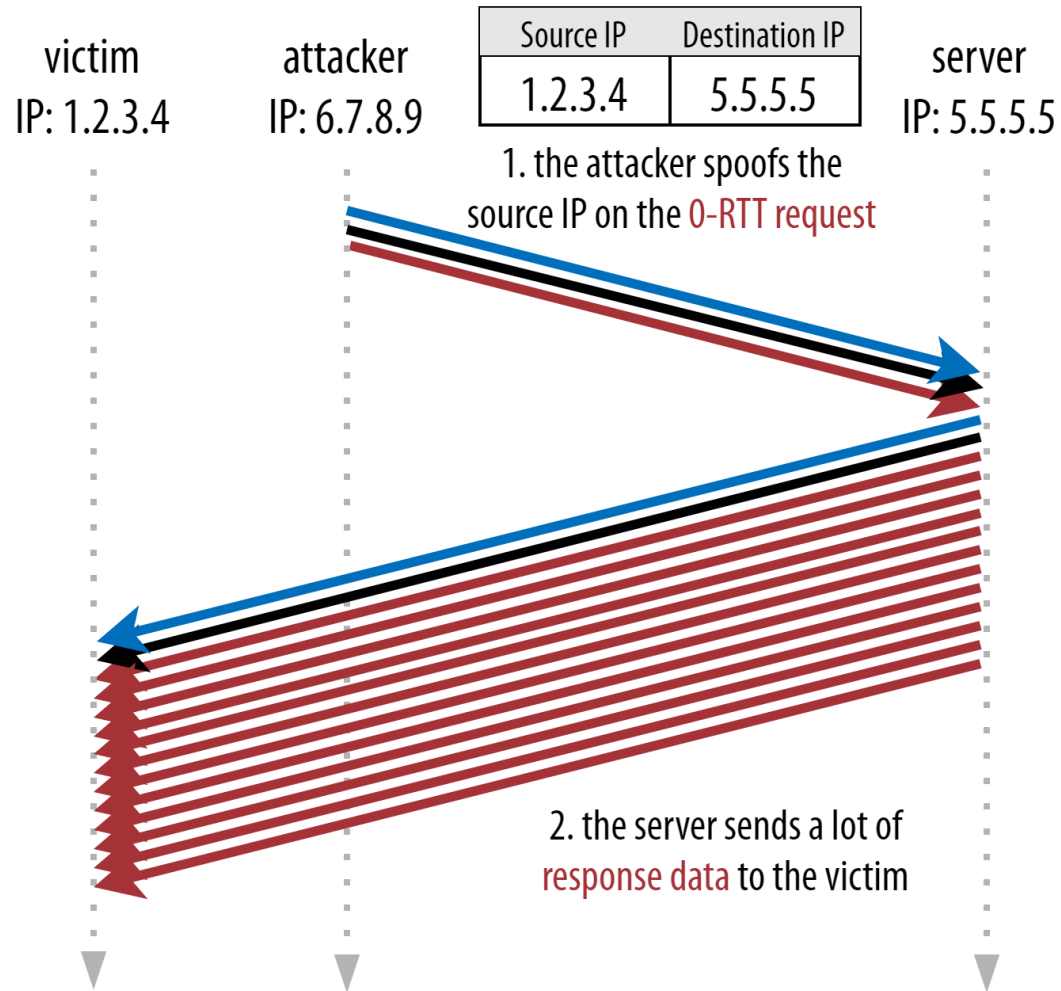
QUIC key derivation schedule



Combined Transport and Crypto handshake



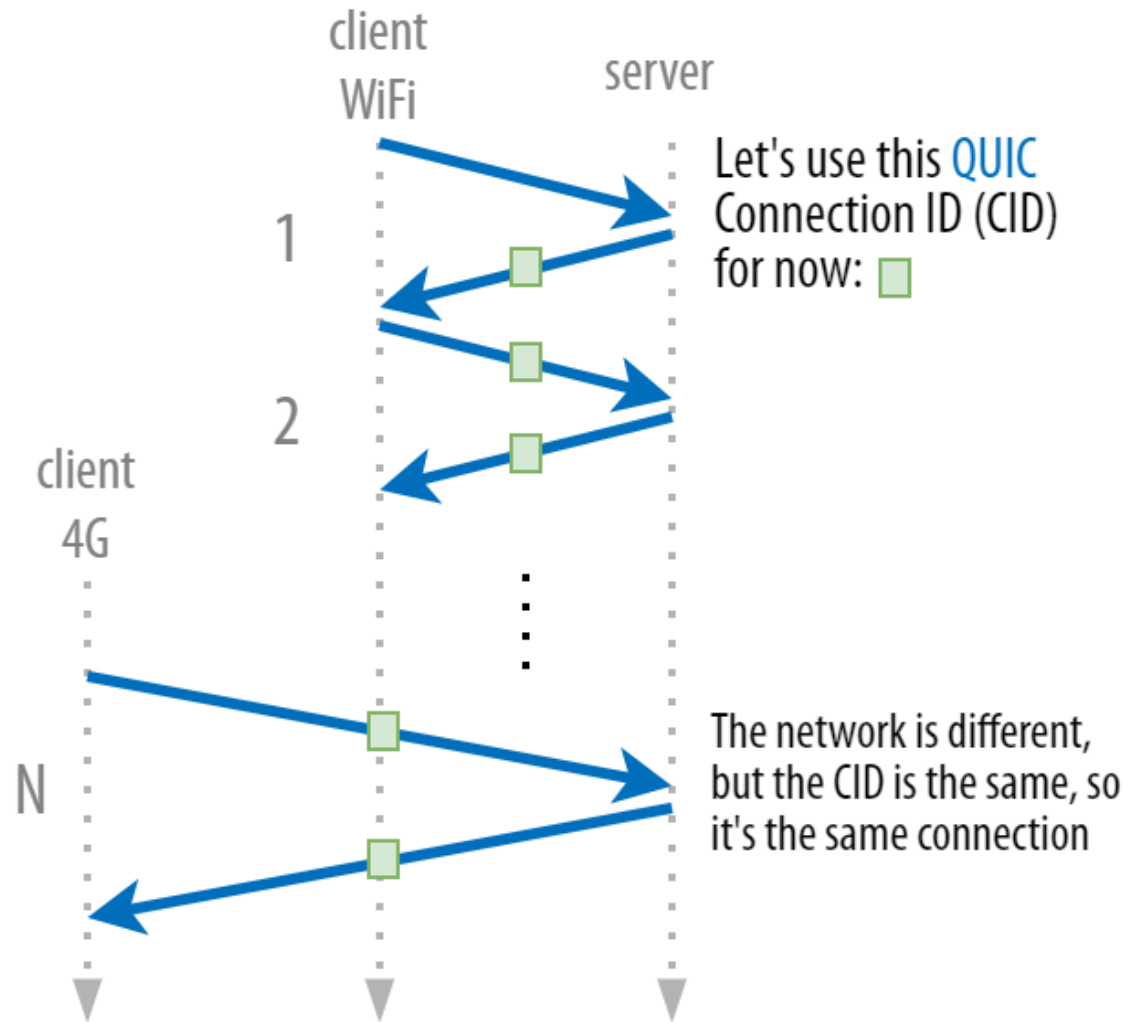
Amplification prevention/mitigation



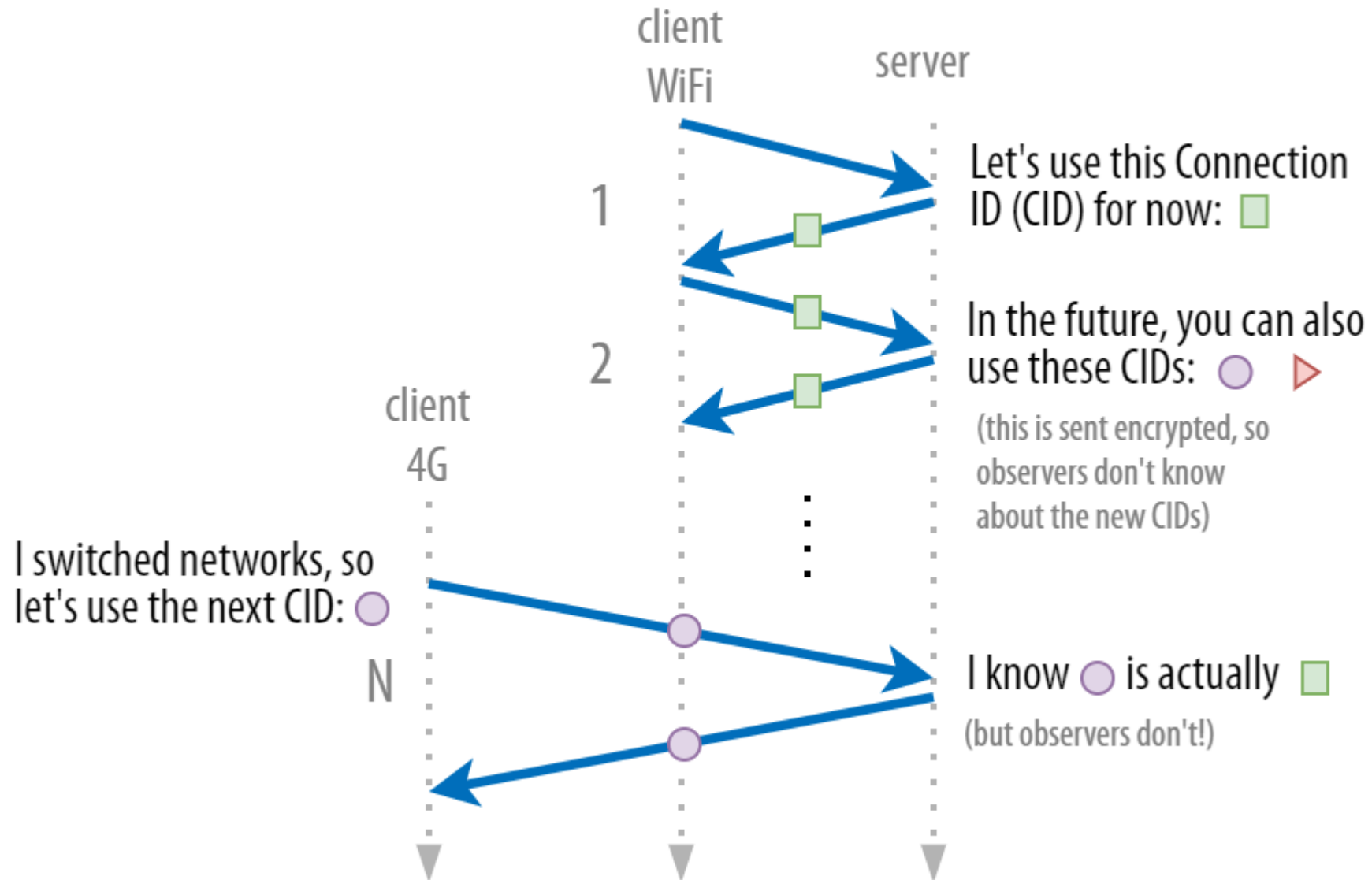
Other issues

- Replay attacks
- STEK rotation
- → not QUIC specific, also for TCP+TLS resumption/0-RTT

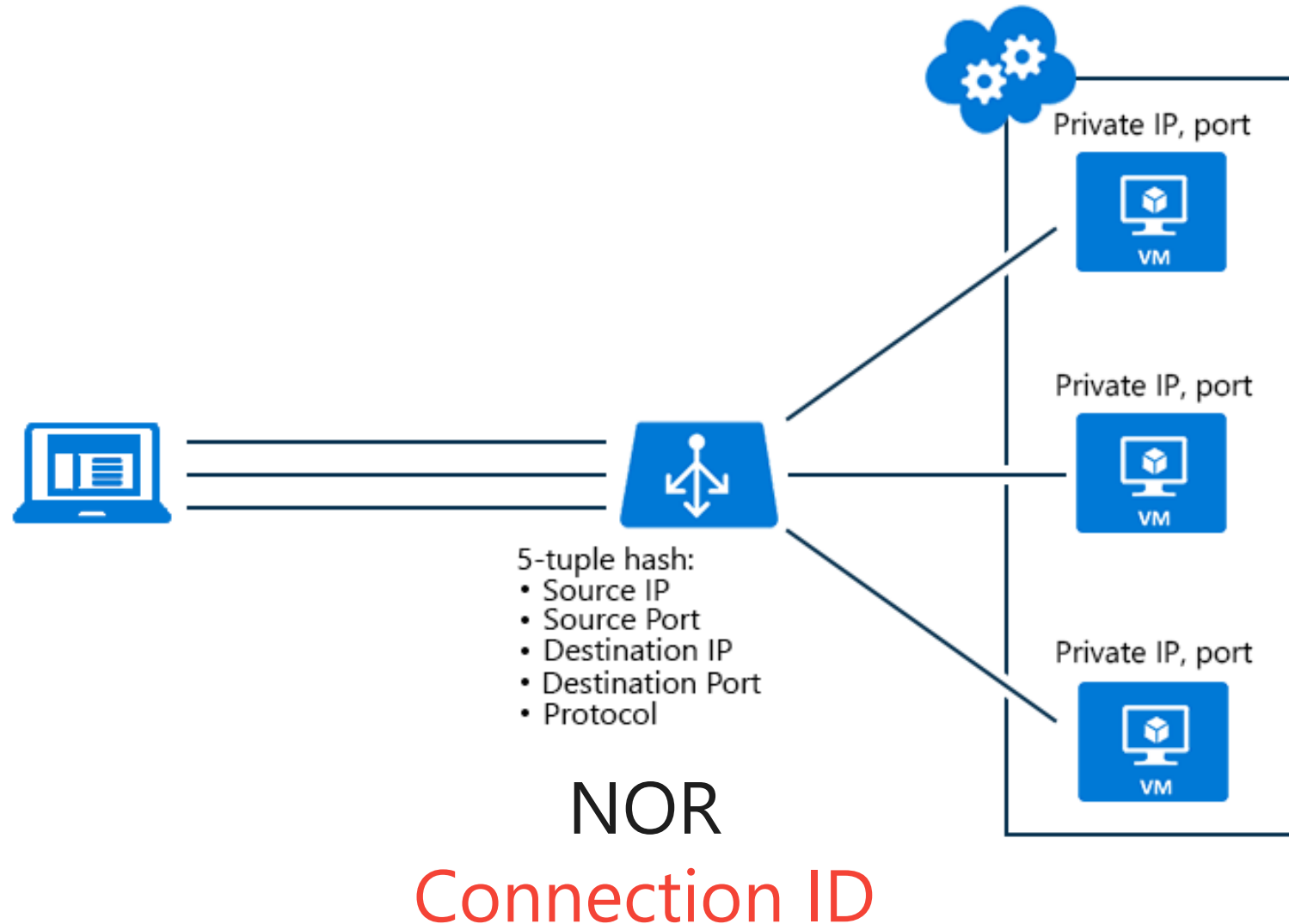
Connection migration is a privacy nightmare



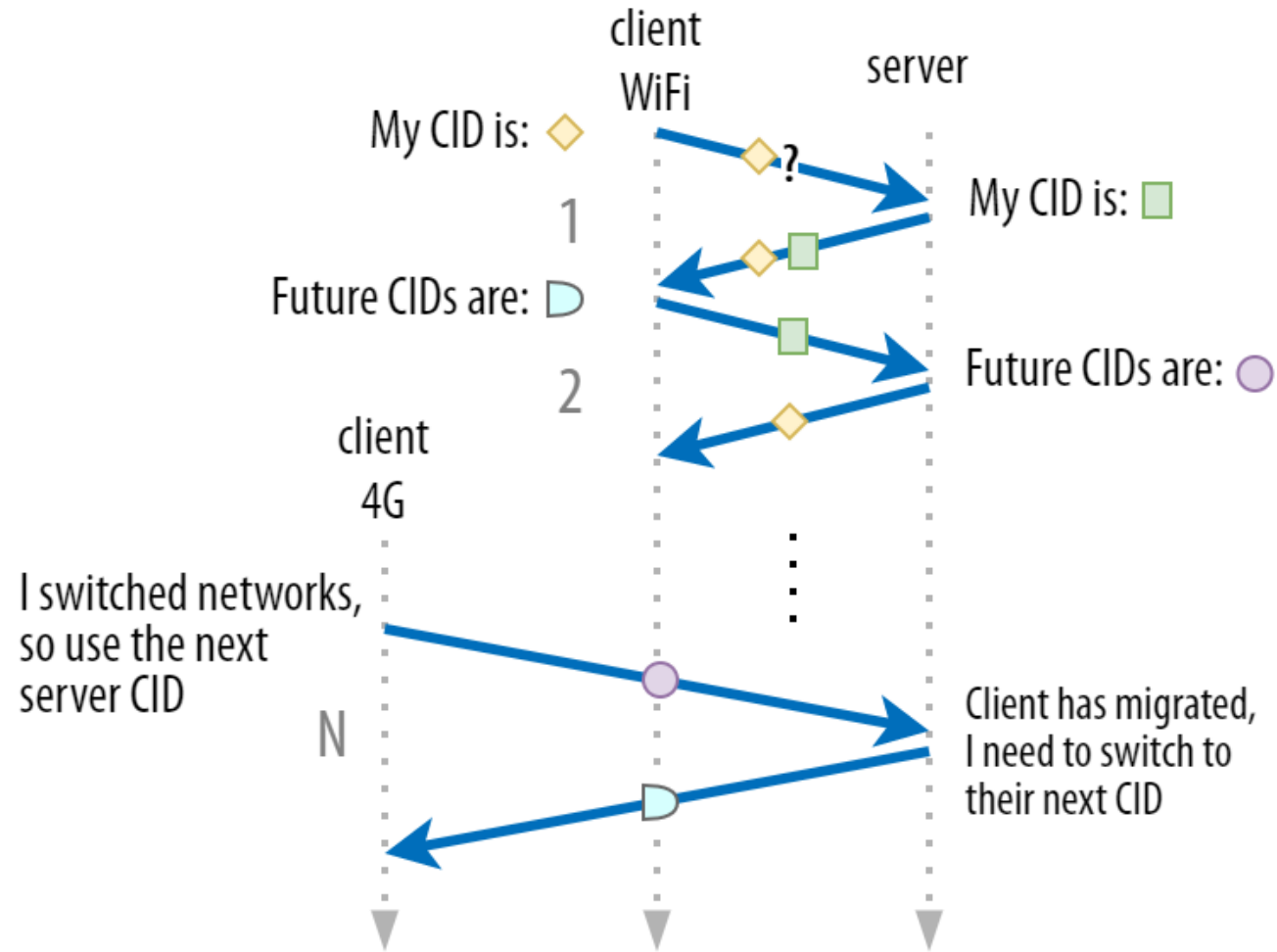
Linkability prevention with migration



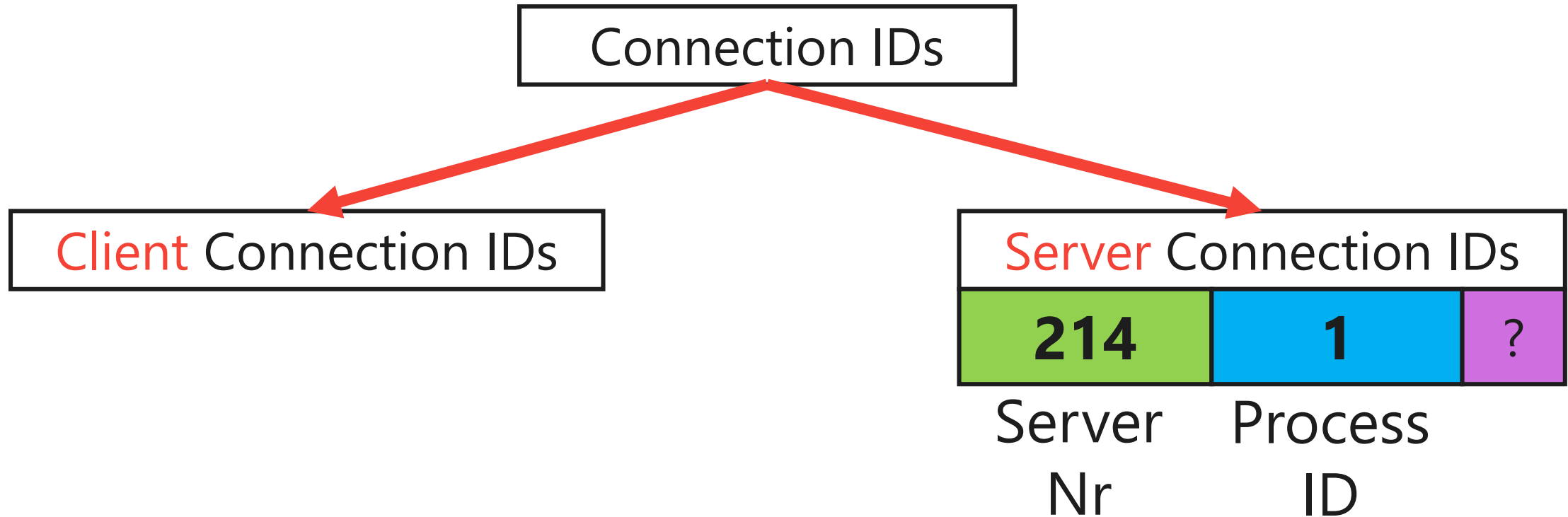
Linkability prevention is deployment nightmare



Splitting CIDs for routability



Splitting CIDs for routability



Need to use standard/configured/negotiated format for:

- Load balancers
- Potentially also firewalls!

Open that UDP:443

× Headers Preview Response Initiator Timing Cookies

▼ General

Request URL: `https://www.facebook.com/`

Request Method: `GET`

Status Code: 🟢 `200`

Remote Address: `[2a03:2880:f121:83:face:b00c:0:25de]:443`

Referrer Policy: `strict-origin-when-cross-origin`

▼ Response Headers

alt-svc: `h3-29=":443"; ma=3600,h3-27=":443"; ma=3600`

cache-control: `private, no-cache, no-store, must-revalidate`

content-encoding: `br`

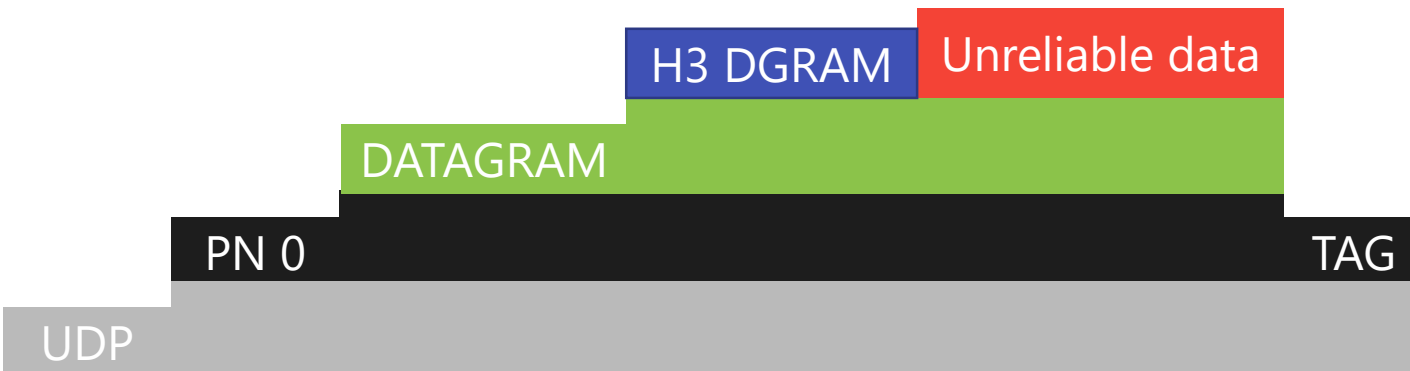
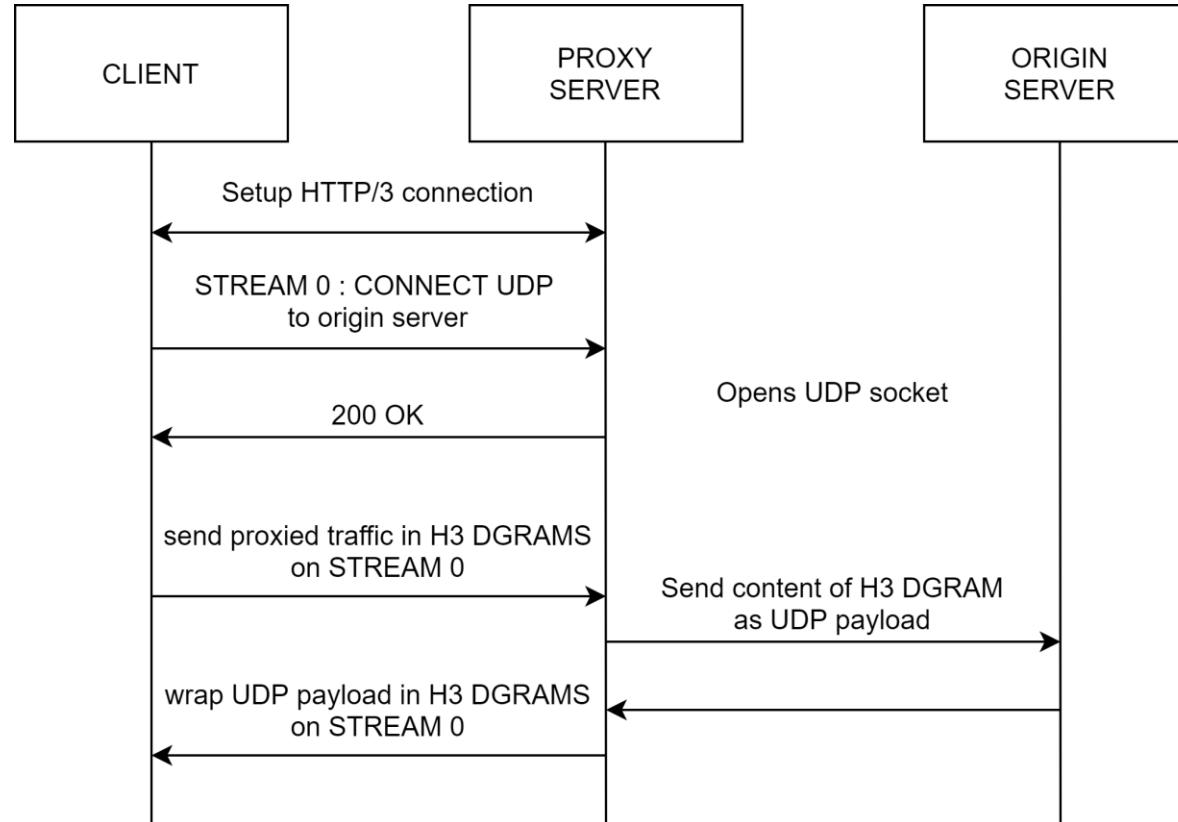
Tunneling/Proxying stuff over QUIC

Lots of stuff proposed:

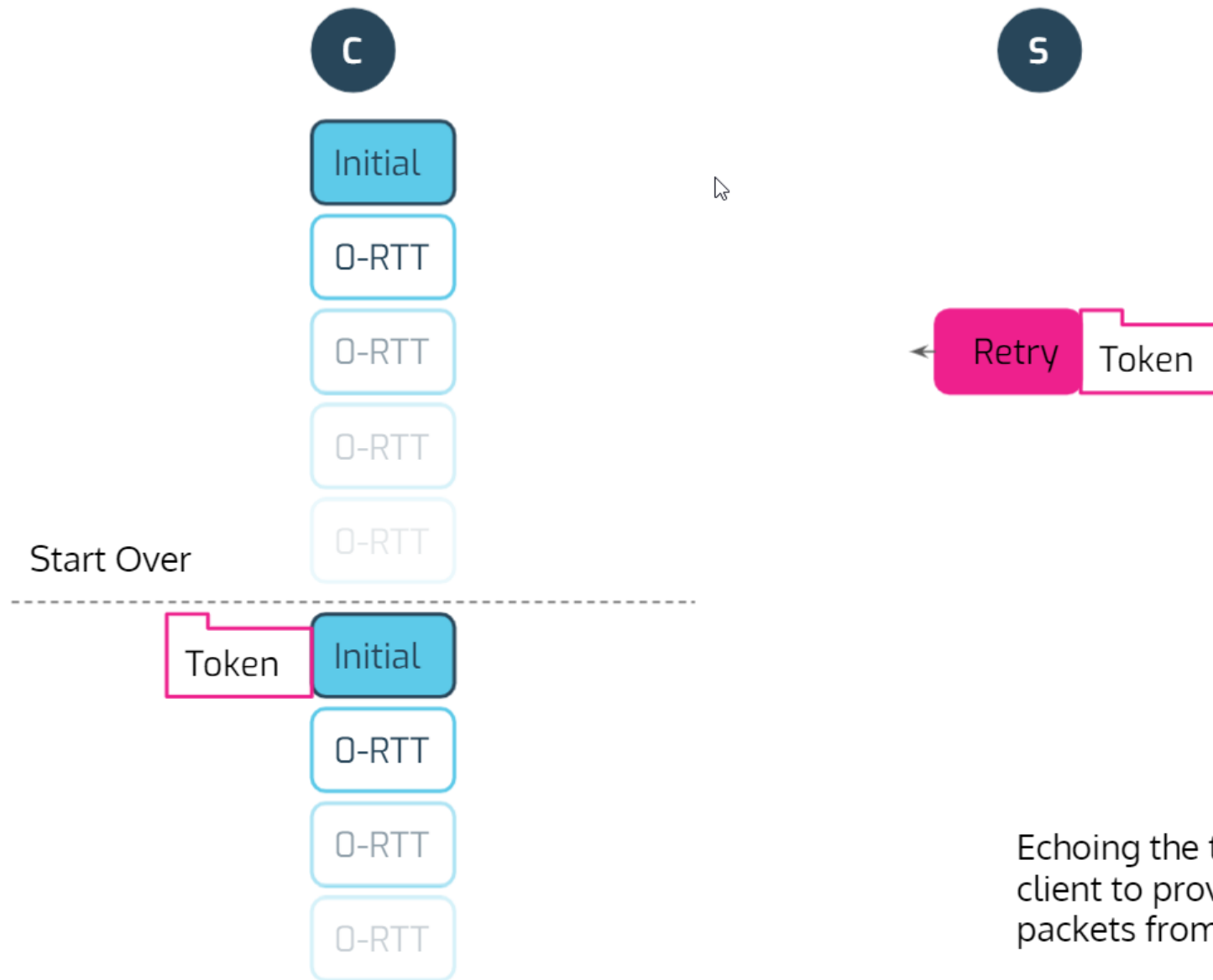
- DNS over QUIC / H3
- WebTransport
- SSH over QUIC
- ...

Block all or nothing

- H3 falls back to H2 over TCP
- Other things might not be so lucky...



TCP SYN Cookies ~ = QUIC RETRY token



Echoing the token forces the client to prove that it can receive packets from the server.

Prevent TLS interceptors from messing with QUIC



dschinazi 9:17 PM

QUIC uses the local store but it fails the handshake if the root CA is not in the default set. This was done by policy to prevent antivirus software from MITM QUIC so we can keep evolving QUIC.

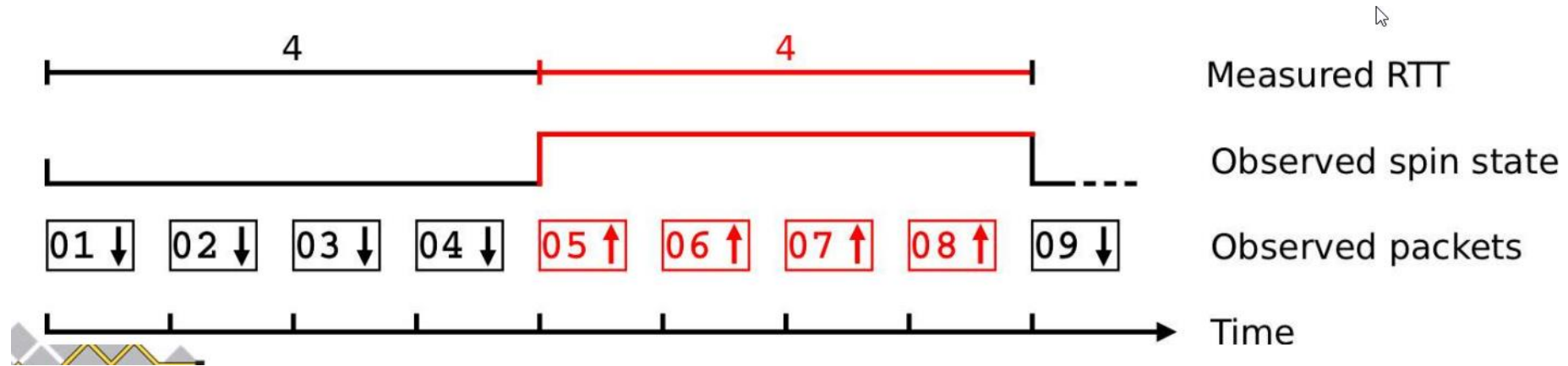
```
35 options = webdriver.ChromeOptions()
36 options.gpu = False
37 options.headless = True
38 options.binary_location = "/usr/bin/google-chrome-beta"
39 options.add_argument("--no-sandbox")
40 options.add_argument("--enable-quic")
41 options.add_argument("--quic-version=h3-29")
42 options.add_argument("--origin-to-force-quic-on=" + server)
43 options.add_argument("--log-net-log=/logs/chrome.json")
44 options.add_argument("--net-log-capture-mode=IncludeSensitive")
45 options.add_argument("--ignore-certificate-errors-spki-list=" + get_args().certhash)
```

Prevent TLS interceptors from messing with QUIC

```

> User Datagram Protocol, Src Port: 55844, Dst Port: 443
▼ QUIC IETF
  > QUIC Connection information
    [Packet Length: 1350]
    1... .... = Header Form: Long Header (1)
    .1... .... = Fixed Bit: True
    ..00 .... = Packet Type: Initial (0)
    .... 00... = Reserved: 0
    .... ..00 = Packet Number Length: 1 bytes (0)
    Version: draft-29 (0xff00001d)
    Destination Connection ID Length: 8
    Destination Connection ID: 30ae1bcdddf6810d
    Source Connection ID Length: 0
    Token Length: 0
    Length: 1332
    Packet Number: 1
    Payload: 56b3067494565dc75f836f06935566a1636ff3ce0a5999f74c838481f7b1a5d5e03f2121...
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > PADDING Length: 8
  > PING
  > PADDING Length: 865
  > TLSv1.3 Record Layer: Handshake Protocol: Hello Request (fragment)
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > PING
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > PING
  > PING
  > PADDING Length: 51
  > PING
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > TLSv1.3 Record Layer: Handshake Protocol: Multiple Handshake Messages
  > PING
  > PING
  ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Frame Type: CRYPTO (0x0000000000000006)
    Offset: 17
    Length: 51
    Crypto Data
    Handshake Protocol: Client Hello (last fragment)
  > [9 Reassembled Handshake Fragments (349 bytes): #1(17), #1(51), #1(4), #1(215), #1(3), #1(11), #1(30), #1(4), #1(14)]
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 345
    Version: TLS 1.2 (0x0303)
    Random: 313bde25ed22c84b3d9efc64ec3e1afb15ad272a02728ea48a837307c1e02338
    Session ID Length: 0
    Cipher Suites Length: 6
    > Cipher Suites (3 suites)
    Compression Methods Length: 1
    > Compression Methods (1 method)
    Extensions Length: 298
    > Extension: server_name (len=31)
    > Extension: supported_groups (len=8)
    > Extension: application_layer_protocol_negotiation (len=8)
    > Extension: signature_algorithms (len=20)
    > Extension: key_share (len=38)
    > Extension: psk_key_exchange_modes (len=2)
```

QUIC observability / debuggability



QUIC observability / debuggability

| quic-microsoft.pcap | | | | | | |
|--|----------|----------------|----------------|----------|--------|--|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | | |
| Apply a display filter ... <Ctrl-/> | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1 | 0.000000 | 10.168.234.1 | 138.91.188.147 | QUIC | 1294 | Initial, DCID=9b4dccfc42f8ab9c, SCID=cf4d6e8c2c7b43a2, PKN: 0, CRYPTO, PADDING |
| 2 | 0.170410 | 138.91.188.147 | 10.168.234.1 | QUIC | 1294 | Handshake, DCID=cf4d6e8c2c7b43a2, SCID=09fa3e7edeb3b621ae |
| 3 | 0.170550 | 138.91.188.147 | 10.168.234.1 | QUIC | 1294 | Handshake, DCID=cf4d6e8c2c7b43a2, SCID=09fa3e7edeb3b621ae |
| 4 | 0.170558 | 138.91.188.147 | 10.168.234.1 | QUIC | 1108 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |
| 5 | 0.171689 | 10.168.234.1 | 138.91.188.147 | QUIC | 331 | Protected Payload (KP0), DCID=09fa3e7edeb3b621ae |
| 6 | 0.171765 | 10.168.234.1 | 138.91.188.147 | QUIC | 1514 | Protected Payload (KP0), DCID=09fa3e7edeb3b621ae |
| 7 | 0.172241 | 10.168.234.1 | 138.91.188.147 | QUIC | 225 | Protected Payload (KP0), DCID=09fa3e7edeb3b621ae |
| 8 | 0.336168 | 138.91.188.147 | 10.168.234.1 | QUIC | 1294 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |
| 9 | 0.336473 | 138.91.188.147 | 10.168.234.1 | QUIC | 1482 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |
| 10 | 0.336480 | 138.91.188.147 | 10.168.234.1 | QUIC | 1294 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |
| 11 | 0.336483 | 138.91.188.147 | 10.168.234.1 | QUIC | 172 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |
| 12 | 0.336737 | 10.168.234.1 | 138.91.188.147 | QUIC | 77 | Protected Payload (KP0), DCID=09fa3e7edeb3b621ae |
| 13 | 0.496553 | 138.91.188.147 | 10.168.234.1 | QUIC | 80 | Protected Payload (KP0), DCID=cf4d6e8c2c7b43a2 |

SSLKEYLOGFILE

| | |
|--|--|
| User Datagram Protocol, Src Port: 443, Dst Port: 44873 | |
| QUIC IETF | |
| QUIC Connection information | |
| [Packet Length: 179] | |
| 1... .. = Header Form: Long Header (1) | |
| .1.. .. = Fixed Bit: True | |
| ..00 .. = Packet Type: Initial (0) | |
| 00.. = Reserved: 0 | |
|11 = Packet Number Length: 4 bytes (3) | |
| Version: 1 (0x00000001) | |
| Destination Connection ID Length: 8 | |
| Destination Connection ID: cf4d6e8c2c7b43a2 | |
| Source Connection ID Length: 9 | |
| Source Connection ID: 09fa3e7edeb3b621ae | |
| Token Length: 0 | |
| Length: 152 | |
| Packet Number: 0 | |
| Payload: e4f7d2fe84cfcfc658a0a82fed735babbf4cf18d8190b7091bef03f71ef8e9e6714e128a... | |
| ACK | |
| TLSv1.3 Record Layer: Handshake Protocol: Server Hello | |
| QUIC IETF | |
| [Packet Length: 1073] | |
| 1... .. = Header Form: Long Header (1) | |
| .1.. .. = Fixed Bit: True | |
| ..10 .. = Packet Type: Handshake (2) | |
| Version: 1 (0x00000001) | |
| Destination Connection ID Length: 8 | |
| Destination Connection ID: cf4d6e8c2c7b43a2 | |
| Source Connection ID Length: 9 | |
| Source Connection ID: 09fa3e7edeb3b621ae | |
| Length: 1047 | |
| [Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available] | |
| Remaining Payload: c8f603b80e21bb56c7dc939bccc3f43faa6d40e40afr42b06664f247e7h9552a7352fh378 | |
| 00d8 01111000 00101111 10010101 01110001 00000110 11100010 00000000 00000000 x/ | |
| Frame (1294 bytes) Decrypted QUIC (132 bytes) | |
| QUIC IETF (quic), 1073 byte(s) | |
| Packets: 13 · Displayed: 13 (100.0%) | |

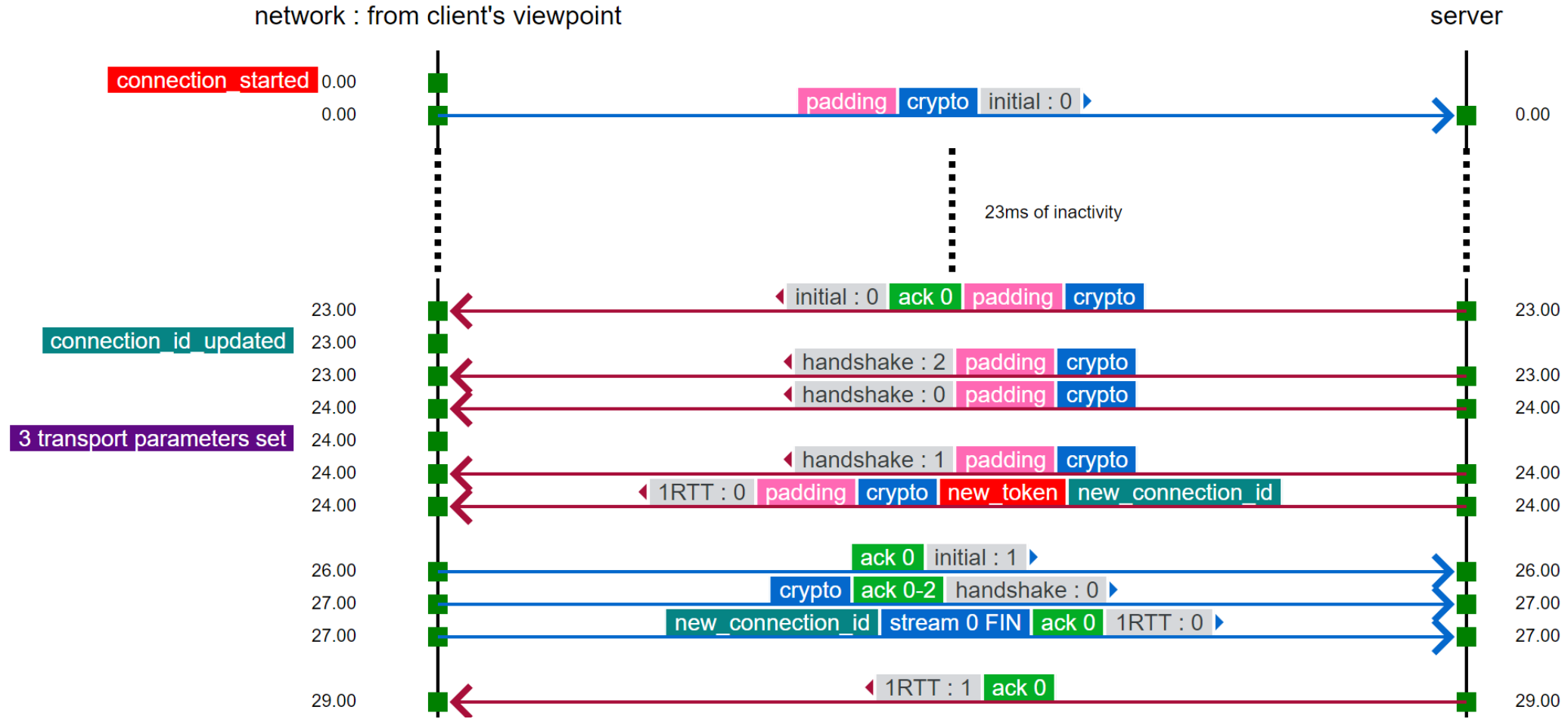
[qlog] structured endpoint logging

```
{
  "event_fields": [
    "time", "group_id", "category", "event", "data"
  ],
  "events": [
    [1553986553579, 0, "transport", "packet_received", {"header": {} }],
    [1553986553580, 0, "recovery", "metrics_updated", {"smoothed_rtt": 85}],
    [1553986553588, 1, "http", "frame_parsed", {"frame_type": "DATA"}],
    [1553986553598, 0, "transport", "packet_sent", {"header": {} }]
  ]
}
```

get data from implementations directly



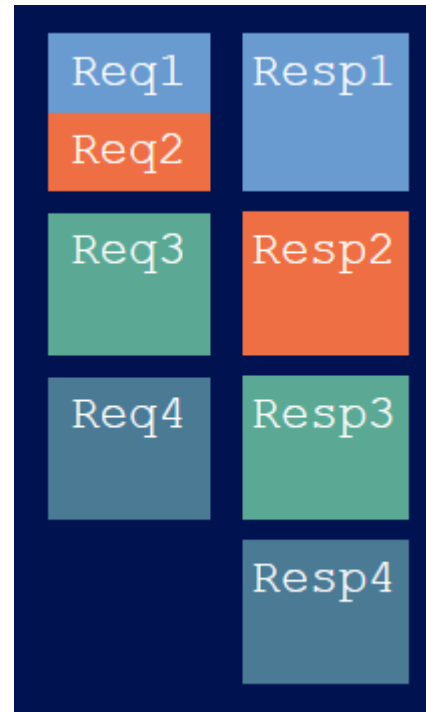
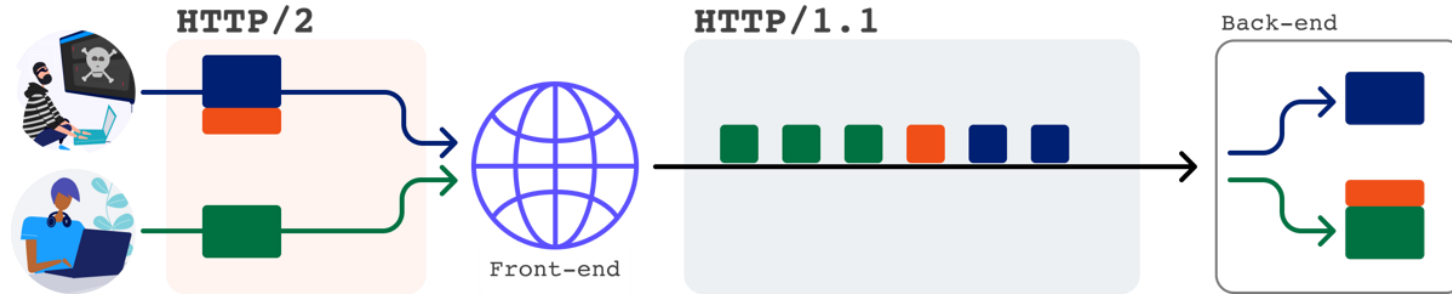
QUIC and HTTP/3 tools



<https://qvis.quictools.info>

<https://github.com/quiclog/qvis>

HTTP/2 request smuggling



```
POST /n HTTP/1.1
Host: www.netflix.com
Content-Length: 4
```

```
abcdGET /n HTTP/1.1
Host: 02.rs?x.netflix.com
Foo: bar
```

Image sources

1. See bottom right of most slides
2. <https://github.com/rmarx/http3-for-webdevs> = collection of free to re-use diagrams