First Octet

QUIC, IETF 103, November 2018
Martin Thomson
Discussed in NYC

Initial, 0-RTT, Handshake, Retry

1-RTT

0 1 S K P P

1 1 T T P P
Common

One header type bit

1 = long, 0 = short

One “QUIC bit”

Lower bits are encrypted

Last two bits are packet number length

\[
\text{pn\_length} = \left(\left(\text{packet}[0] \oplus \text{e\_mask}\right) \& 3\right) + 1
\]
Long Header

| 1 | 1 | T | T | P | P |

No spin bit or key phase

Two type bits: Initial(0), 0-RTT(1), Handshake(2), Retry(3)

Encrypt the rest

Two spare bits must be zero before encryption

Negotiate the use of other values if you like
Short Header

Spin bit (if accepted, spare and encrypted otherwise)
Spare bits must be zero before encryption
Key phase is before packet number length

Note: packet number encryption key can’t be updated
#1575 - Packet Number Encryption Sampling

Current:

```python
start = min(1 + len(connection_id) + 4, len(packet)-16)
sample = packet[start:start+16]
```

Proposed (but still needed?):

```python
start = min( 1 + len(connection_id) + 4 , len(packet)-16)
```

Pad so that the sample is always 16 bytes, that is:

```python
len(frames) + len(packet number) >= 4
```