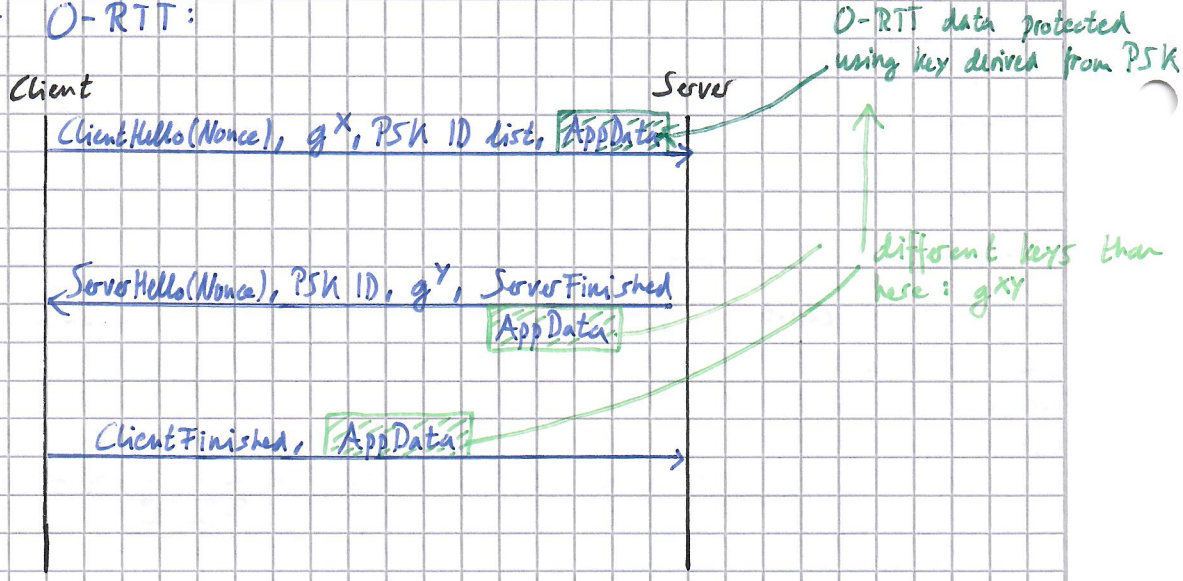
- Handshake – 0-RTT:



⇒ 0-RTT data does not enjoy forward security since protection is based on long-lived symmetric keys.

⇒ 0-RTT is hard to protect against replay attacks (especially in distributed server environments) ⇒ only send idempotent data (doesn't change state of server) in first message of 0-RTT handshake