First we introduce the basic type we will use:

$$
\begin{aligned}
MESSAGE ::= \; & ClientHello \\
| \; & ServerHello \\
| \; & ServerKeyExchange \\
| \; & ServerCertificate \\
| \; & ServerCertificateVerify \\
| \; & HelloRetryRequest \\
| \; & CertificateRequest \\
| \; & ClientCertificate \\
| \; & ClientFinished \\
| \; & ServerFinished
\end{aligned}
$$

And then our schema:

$$
\begin{array}{|l}
\hline
CLIENT \\
in? : MESSAGE \\
out! : MESSAGE \\
\hline
(out! = ClientHello) \\
\lor (in? == ServerFinished \land out! = ClientFinished) \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
SERVER \\
in? : MESSAGE \\
out! : MESSAGE \\
\hline
(in? == ClientHello \land out! = \mathrm{seq}\, ServerHello, SerevreKeyExchange, \\
\qquad\qquad\qquad\qquad\qquad\qquad EncryptedExtensions, ServerCertificate, \\
\qquad\qquad\qquad\qquad\qquad\qquad ServerCertificateVerify, ServerFinished) \\
\lor \quad (in? == ClientFinished \land out! = ApplicationData) \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
0 - RTT - SERVER \\
in? : MESSAGE \\
out! : MESSAGE \\
\hline
in? == ClientHello \land out! = \mathrm{seq}\, ServerHello, KeyShare, \\
\qquad\qquad\qquad\qquad\qquad\qquad ServerFinished, ApplicationData \\
\hline
\end{array}
$$

$0 - RTT - CLIENT$

$in? : MESSAGE$

$out! : MESSAGE$

$out! = \text{seq}\ ClientHello, SessionTicket, KeyShare$