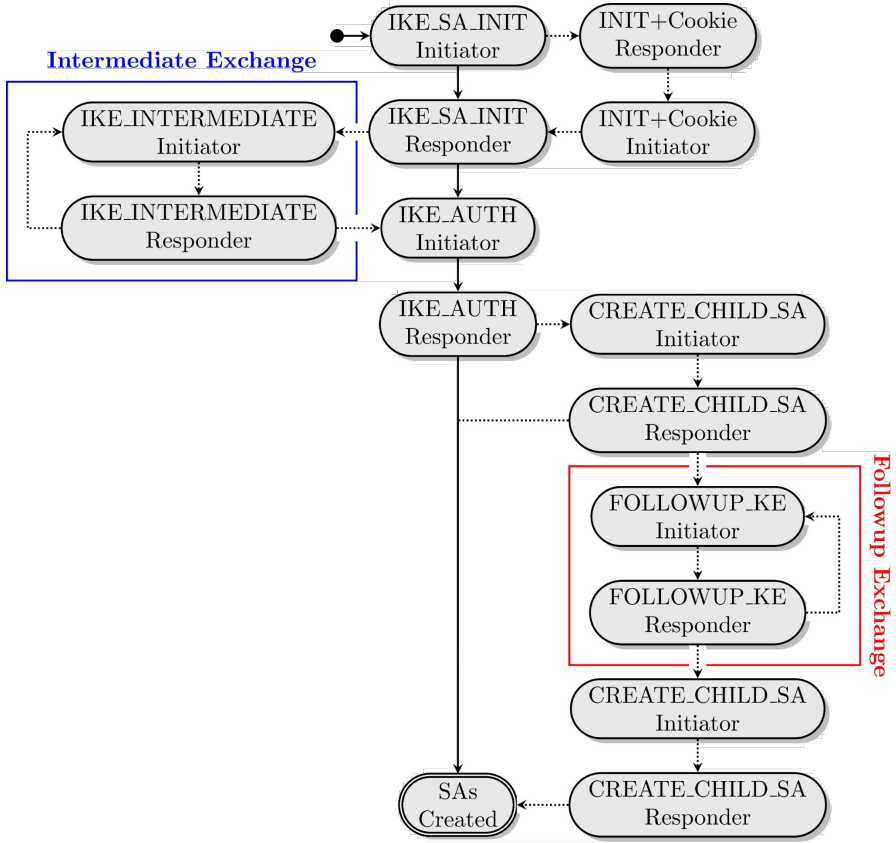
Improvements for Post-Quantum IKEv2

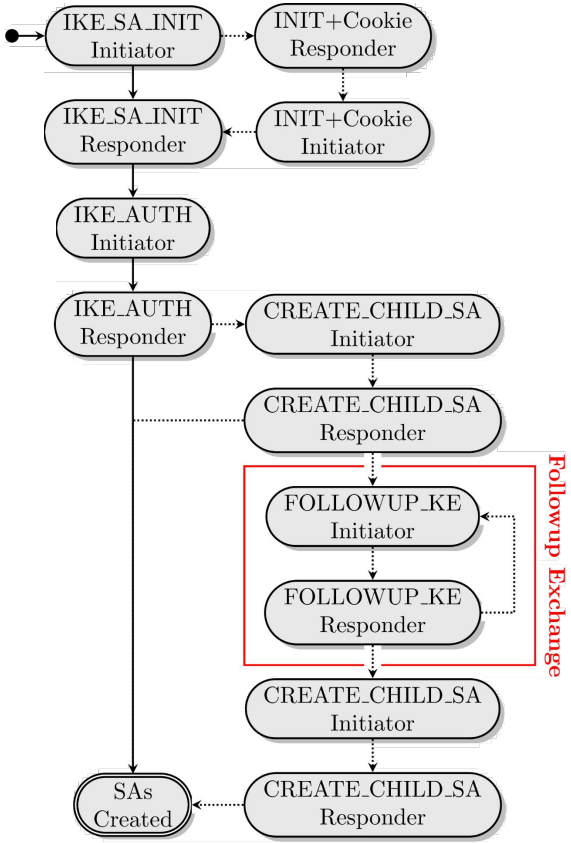
Intermediate Exchanges

- Often fragmented, especially when used for PQKEs
- Signing fragmented intermediate messages is complex
- Large PQKEs in intermediate messages lead to vulnerabilities againts DOS attacks ⇒ Move them to FOLLOWUP_KE

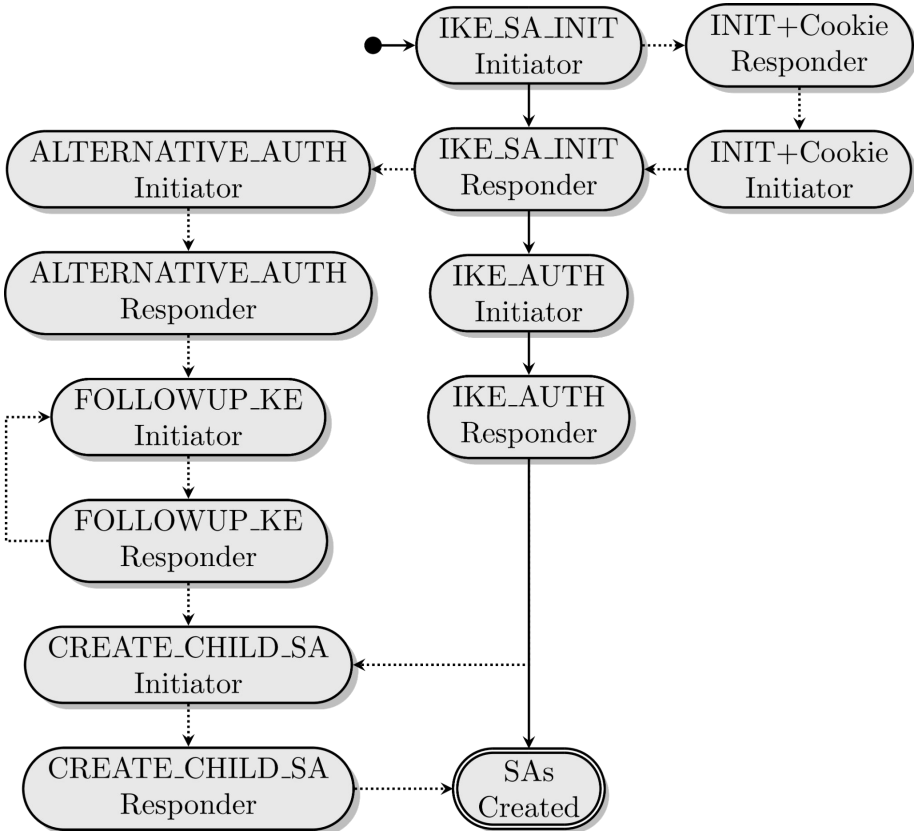
Status Quo


IKE_SA_INIT
Initiator
INIT+Cookie
Responder
Intermediate Exchange
IKE_INTERMEDIATE
Initiator
IKE_SA_INIT
Responder
INIT+Cookie
Initiator
IKE_INTERMEDIATE
Responder
IKE_AUTH
Initiator
IKE_AUTH
Responder
CREATE_CHILD_SA
Initiator
CREATE_CHILD_SA
Responder
FOLLOWUP_KE
Initiator
FOLLOWUP_KE
Responder
Followup Exchange
CREATE_CHILD_SA
Initiator
SAs
Created
CREATE_CHILD_SA
Responder

First Step: No IKE_INTERMEDIATE



Second Step: New Authentication Exchange



Benefits

- Independent of complex IKE_INTERMEDIATE exchanges
- DoS protected introduction of large PQKEs
- Clean state machine
- New place for exchanging handshake data after establishing an authenticated channel