simplified and one-way authentication
TLS 1.2 (2008)

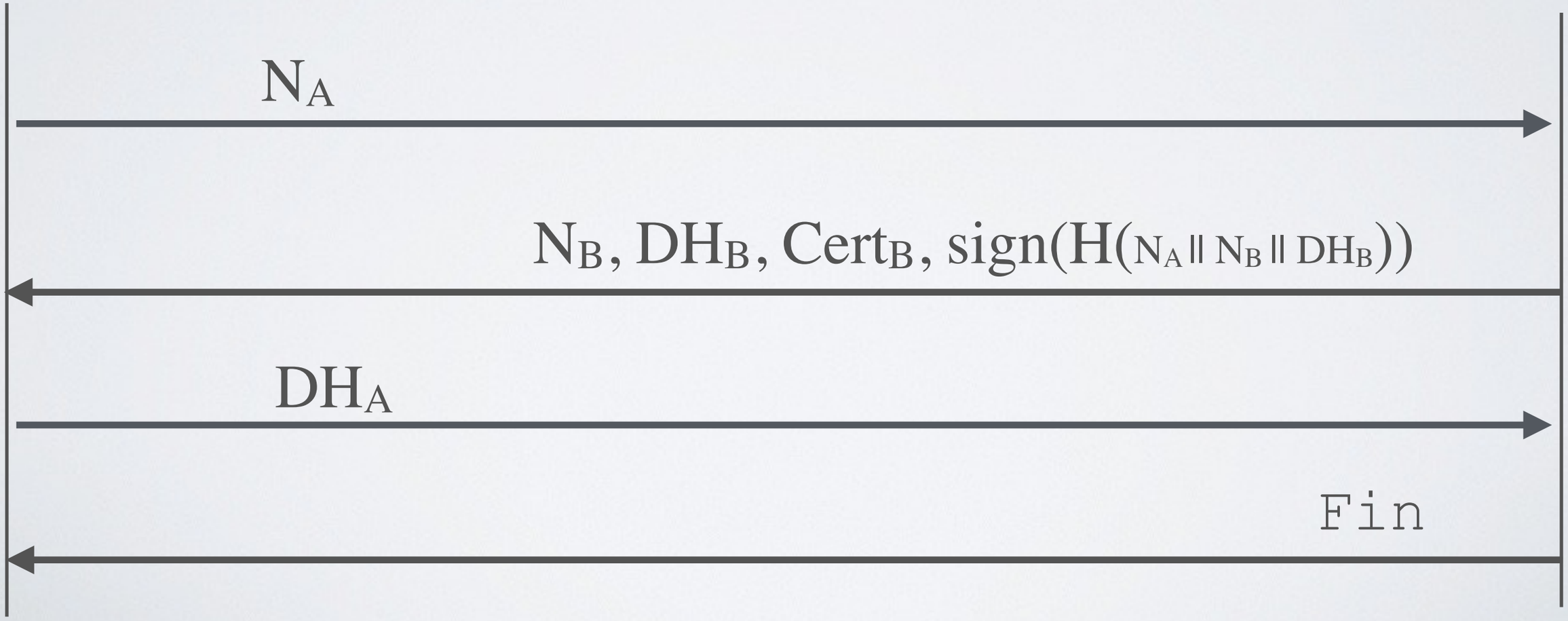

N_A

$N_B, DH_B, Cert_B, sign(H(N_A \| N_B \| DH_B))$


DH_A

Fin

simplified and one-way authentication
TLS 1.2 (2008)



simplified and one-way authentication
TLS 1.3 (2018)