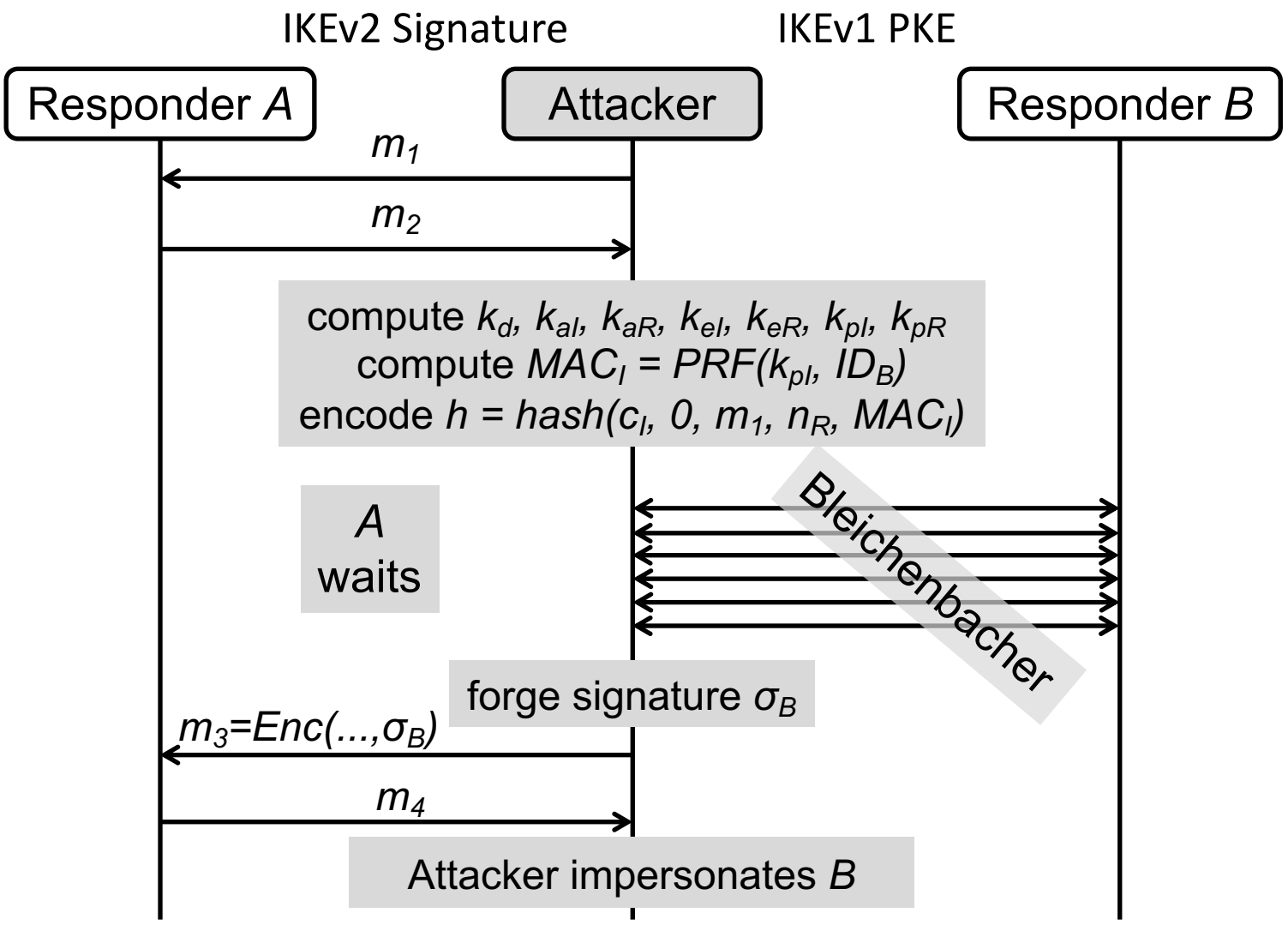
IKEv2 Signature
IKEv1 PKE
Responder A
Attacker
Responder B
m1
m2
compute kd, kaI, kaR, keI, keR, kpI, kpR
compute MACI = PRF(kpI, IDB)
encode h = hash(cI, 0, m1, nR, MACI)
A
waits
Bleichenbacher
forge signature σB
m3=Enc(...,σB)
m4
Attacker impersonates B