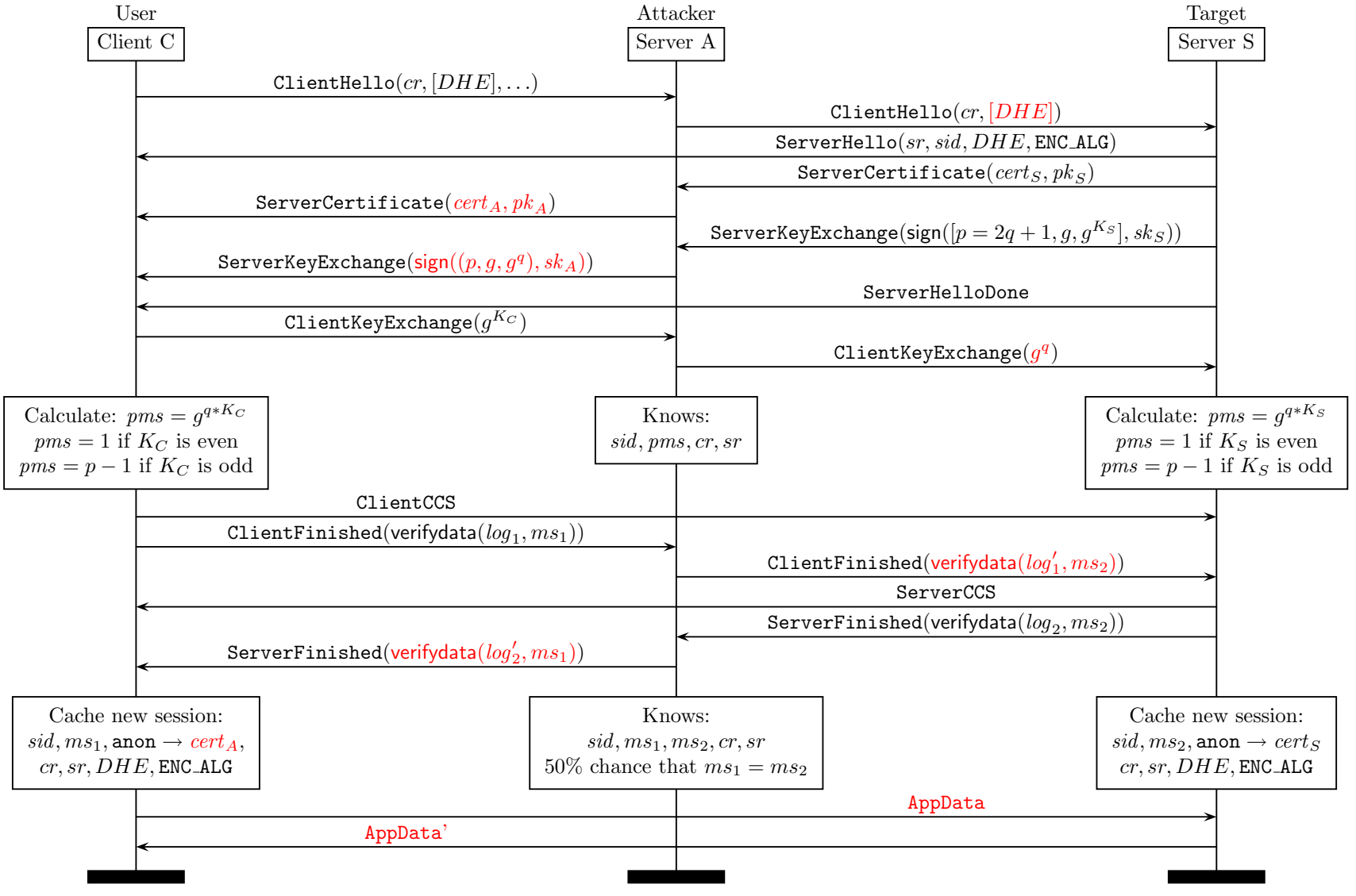
User
Client C
Attacker
Server A
Target
Server S
ClientHello(cr, [DHE], ...)
ClientHello(cr, [DHE])
ServerHello(sr, sid, DHE, ENC_ALG)
ServerCertificate($cert_S$, pk_S)
ServerCertificate($cert_A$, pk_A)
ServerKeyExchange(sign([$p = 2q + 1, g, g^{K_S}$], sk_S))
ServerKeyExchange(sign((p, g, g^q), sk_A))
ServerHelloDone
ClientKeyExchange(g^{K_C})
ClientKeyExchange(g^q)
Calculate: $pms = g^{q*K_C}$
$pms = 1$ if K_C is even
$pms = p - 1$ if K_C is odd
Knows:
sid, pms, cr, sr
Calculate: $pms = g^{q*K_S}$
$pms = 1$ if K_S is even
$pms = p - 1$ if K_S is odd
ClientCCS
ClientFinished(verifydata(log_1, ms_1))
ClientFinished(verifydata(log'_1, ms_2))
ServerCCS
ServerFinished(verifydata(log_2, ms_2))
ServerFinished(verifydata(log'_2, ms_1))
Cache new session:
sid, ms_1, anon $\rightarrow cert_A$,
cr, sr, DHE, ENC_ALG
Knows:
sid, ms_1, ms_2, cr, sr
50% chance that $ms_1 = ms_2$
Cache new session:
sid, ms_2, anon $\rightarrow cert_S$
cr, sr, DHE, ENC_ALG
AppData
AppData'