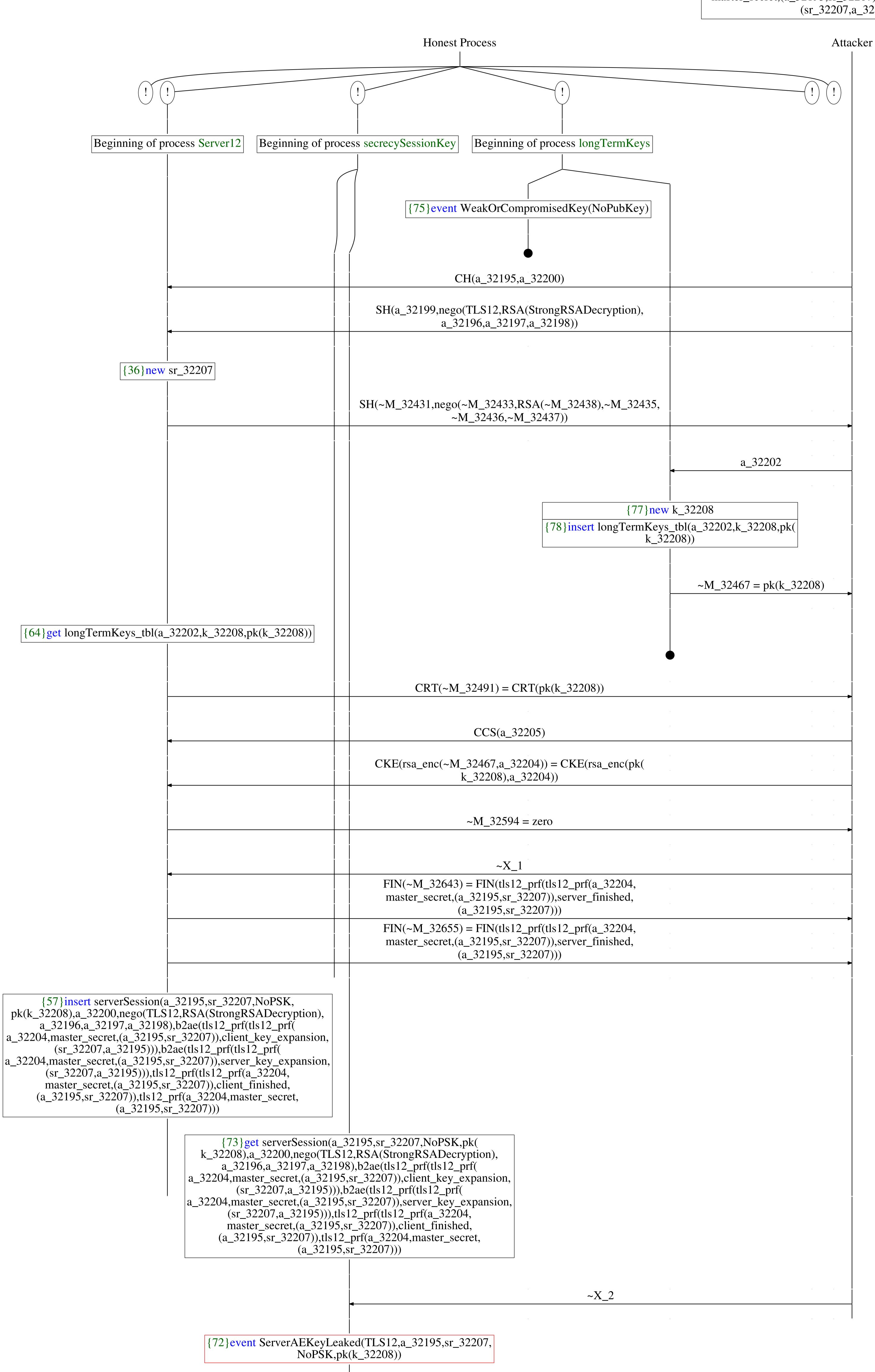
Abbreviations
$\sim$ M_32431 = sr_32207
~M_32433 = TLS12
~M_32438 = StrongRSADecryption
$\sim$ M_32435 = a_32196
$\sim$ M_32436 = a_32197
$\sim$ M_32437 = a_32198
$\sim X_1 = FIN(tls12\_prf(tls12\_prf(a_32204,master\_secret,$

~X\_1 = FIN(tls12\_prf(tls12\_prf(a\_32204,master\_secret, (a\_32195,~M\_32431)),client\_finished,(a\_32195,~M\_32431)))

FIN(tls12\_prf(tls12\_prf(a\_32204,master\_secret, (a\_32195,sr\_32207)),client\_finished,(a\_32195,sr\_32207)))

~X\_2 = b2ae(tls12\_prf(tls12\_prf(a\_32204,master\_secret, (a\_32195,~M\_32431)),server\_key\_expansion,(~M\_32431, a\_32195)))

= b2ae(tls12\_prf(tls12\_prf(a\_32204, master\_secret,(a\_32195,sr\_32207)),server\_key\_expansion, (sr\_32207,a\_32195)))



A trace has been found.