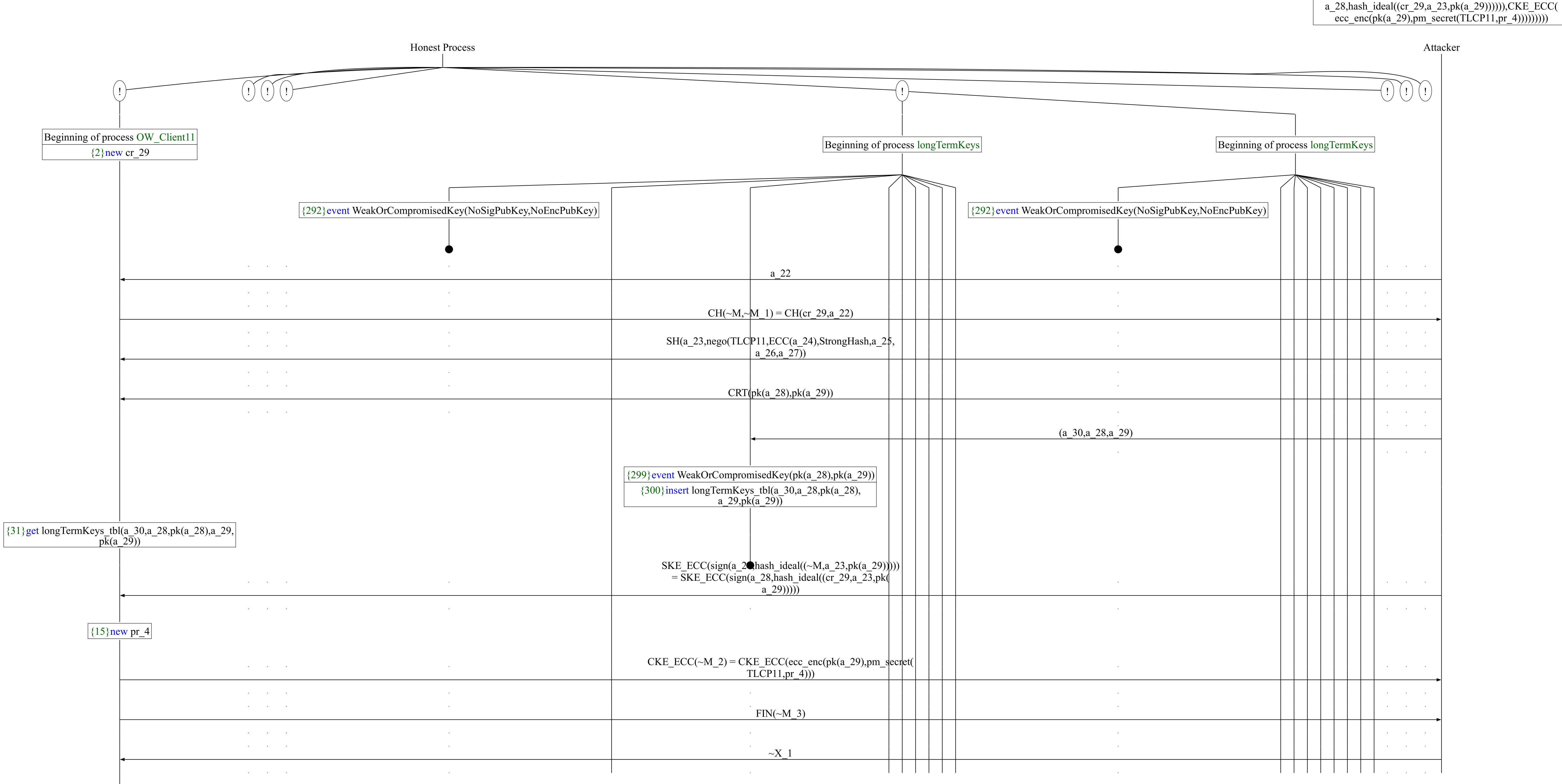
A trace has been found.



{29}event OWClientFinished(TLCP11,cr_29,a_23,NoSID, pk(a_28),pk(a_29),a_22,nego(TLCP11,ECC(a_24),StrongHash, a_25,a_26,a_27),b2ae(prf(prf(pm_secret(TLCP11, pr_4),master_secret,(cr_29,a_23)),client_key_expansion, (a_23,cr_29))),b2ae(prf(prf(pm_secret(TLCP11,pr_4), master_secret,(cr_29,a_23)),server_key_expansion, (a_23,cr_29))),prf(prf(pm_secret(TLCP11,pr_4), master_secret,(cr_29,a_23)),client_finished,(((CH(cr_29,a_22),SH(a_23,nego(TLCP11,ECC(a_24), StrongHash,a_25,a_26,a_27))),CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(a_28,hash_ideal((cr_29,a_23,pk(a_29))))),CKE_ECC(ecc_enc(pk(a_29),pm_secret(TLCP11,pr_4)))),prf(pm_secret(TLCP11,pr_4),master_secret,(cr_29,a_23)))

Abbreviations

~M_3 = prf(prf(pm_secret(TLCP11,pr_4),master_secret, (cr_29,a_23)),client_finished,(((CH(cr_29,a_22), SH(a_23,nego(TLCP11,ECC(a_24),StrongHash,a_25, a_26,a_27))),CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(a_28,hash_ideal((cr_29,a_23,pk(a_29)))))),CKE_ECC(ecc_enc(pk(a_29),pm_secret(TLCP11,pr_4)))))

~X_1 = FIN(prf(prf(ecc_dec(a_29,~M_2),master_secret,(~M,a_23)),server_finished,((((CH(~M,a_22),SH(a_23,nego(TLCP11,ECC(a_24),StrongHash,a_25,a_26, a_27))),CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(a_28, hash_ideal((~M,a_23,pk(a_29))))),CKE_ECC(~M_2)), FIN(prf(prf(ecc_dec(a_29,~M_2),master_secret,(~M,a_23)),client_finished,((((CH(~M,a_22),SH(a_23, nego(TLCP11,ECC(a_24),StrongHash,a_25,a_26,a_27))), CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(a_28,hash_ideal(

(~M,a_23,pk(a_29)))))),CKE_ECC(~M_2)))))))

prf(prf(pm_secret(TLCP11,pr_4),master_secret,(cr_29,a_23)),server_finished,((((CH(cr_29,a_22), SH(a_23,nego(TLCP11,ECC(a_24),StrongHash,a_25, a_26,a_27))),CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(a_28,hash_ideal((cr_29,a_23,pk(a_29)))))),CKE_ECC(ecc_enc(pk(a_29),pm_secret(TLCP11,pr_4)))),FIN(prf(prf(pm_secret(TLCP11,pr_4),master_secret,(cr_29,a_23)),client_finished,(((CH(cr_29,a_22),SH(a_23,nego(TLCP11,ECC(a_24),StrongHash,a_25,a_26,a_27))),CRT(pk(a_28),pk(a_29))),SKE_ECC(sign(