Abbreviations

~X\_1 = FIN(tls12\_prf(tls12\_prf(zero,master\_secret,(~M\_56675, a\_56472)),server\_finished,((((CH(~M\_56675,a\_56478), SH(a\_56472,nego(TLS12,RSA(a\_56479),a\_56480,a\_56475, a\_56481))),CRT(~M\_56780)),CCS(change\_cipher\_spec)), CKE(rsa\_enc(~M\_56780,zero))),FIN(tls12\_prf(tls12\_prf(zero,master\_secret,(~M\_56675,a\_56472)),client\_finished, (~M\_56675,a\_56472)))))

= FIN(tls12\_prf(tls12\_prf( zero,master\_secret,(cr\_56483,a\_56472)),server\_finished, ((((CH(cr\_56483,a\_56478),SH(a\_56472,nego(TLS12, RSA(a\_56479),a\_56480,a\_56475,a\_56481))),CRT(pk( k\_56484))),CCS(change\_cipher\_spec)),CKE(rsa\_enc( pk(k\_56484),zero))),FIN(tls12\_prf(tls12\_prf(zero, master\_secret,(cr\_56483,a\_56472)),client\_finished, (cr\_56483,a\_56472))))))

A trace has been found.

~M\_56963 = aead\_enc(a\_56475,b2ae(tls12\_prf(tls12\_prf(zero,master\_secret,(cr\_56483,a\_56472)),client\_key\_expansion, (a\_56472,cr\_56483))),a\_56476,a\_56477,m\_c(TLS12, cr\_56483,a\_56472,pk(k\_56484),NoPSK))

a\_56472,pk(k\_56484),NoPSK) in phase 1

Honest Process Attacker Beginning of process Client12 Beginning of process appData Beginning of process longTermKeys {2}new cr\_56483 [75] event WeakOrCompromisedKey(NoPubKey) a\_56478  $CH(\sim M_56675,\sim M_56676) = CH(cr_56483,a_56478)$ SH(a\_56472,nego(TLS12,RSA(a\_56479),a\_56480,a\_56475, a\_56481)) a\_56473 {77}new k\_56484 {78}insert longTermKeys\_tbl(a\_56473,k\_56484,pk(k\_56484))  $\sim$ M\_56780 = pk(k\_56484)  $CRT(\sim M_56780) = CRT(pk(k_56484))$ {30} get longTermKeys\_tbl(a\_56473,k\_56484,pk(k\_56484))  $CCS(\sim M_56831) = CCS(change\_cipher\_spec)$  $CKE(\sim M_56877) = CKE(rsa\_enc(pk(k_56484),zero))$  $FIN(\sim M_56895) = FIN(tls12\_prf(tls12\_prf(zero,master\_secret,$ (cr\_56483,a\_56472)),client\_finished,(cr\_56483, a\_56472))) ~X\_1 {25}insert clientSession(cr\_56483,a\_56472,NoPSK, pk(k\_56484),a\_56478,nego(TLS12,RSA(a\_56479),a\_56480, a\_56475,a\_56481),b2ae(tls12\_prf(tls12\_prf(zero, master\_secret,(cr\_56483,a\_56472)),client\_key\_expansion, (a\_56472,cr\_56483))),b2ae(tls12\_prf(tls12\_prf( zero,master\_secret,(cr\_56483,a\_56472)),server\_key\_expansion, (a\_56472,cr\_56483))),tls12\_prf(tls12\_prf(zero, master\_secret,(cr\_56483,a\_56472)),client\_finished, (cr\_56483,a\_56472)),tls12\_prf(zero,master\_secret, (cr\_56483,a\_56472))) CCS(~M\_56922) = CCS(change\_cipher\_spec) {99}get clientSession(cr\_56483,a\_56472,NoPSK,pk( k\_56484),a\_56478,nego(TLS12,RSA(a\_56479),a\_56480, a\_56475,a\_56481),b2ae(tls12\_prf(tls12\_prf(zero, master\_secret,(cr\_56483,a\_56472)),client\_key\_expansion, (a\_56472,cr\_56483))),b2ae(tls12\_prf(tls12\_prf( zero,master\_secret,(cr\_56483,a\_56472)),server\_key\_expansion, (a\_56472,cr\_56483))),tls12\_prf(tls12\_prf(zero, master\_secret,(cr\_56483,a\_56472)),client\_finished, (cr\_56483,a\_56472)),tls12\_prf(zero,master\_secret, (cr\_56483,a\_56472))) (a\_56476,a\_56477) {97}event ClientSends(TLS12,cr\_56483,a\_56472,NoPSK, pk(k\_56484),a\_56476,a\_56477,m\_c(TLS12,cr\_56483, a\_56472,pk(k\_56484),NoPSK)) ~M\_56963 The attacker has the message aead\_dec(a\_56475, b2ae(tls12\_prf(tls12\_prf(zero,master\_secret,(~M\_56675, a\_56472)),client\_key\_expansion,(a\_56472,~M\_56675))),  $a_56476, a_56477, \sim M_56963) = m_c(TLS12, cr_56483,$