Abbreviations	
$\sim M_8518 = sr_8318$	
$\sim M_8520 = TLS12$	
~M_8525 = StrongRSADecryption	
\sim M_8522 = a_8307	
$\sim M_8523 = a_8304$	
\sim M_8524 = a_8308	

A trace has been found.

~X_1 = FIN(tls12_prf(tls12_prf(a_8305,master_secret,(a_8306,~M_8518)),client_finished,(a_8306,~M_8518)))

FIN(tls12_prf(tls12_prf(a_8305,master_secret, (a_8306,sr_8318)),client_finished,(a_8306,sr_8318))) ~M_8759 = aead_enc(a_8304,b2ae(tls12_prf(tls12_prf(

a_8305,master_secret,(a_8306,sr_8318)),server_key_expansion,

(sr_8318,a_8306))),a_8312,a_8313,secretS2C)

Honest Process Attacker Beginning of process longTermKeys Beginning of process Server12 {75}event WeakOrCompromisedKey(NoPubKey) CH(a_8306,a_8310) SH(a_8309,nego(TLS12,RSA(StrongRSADecryption), a_8307,a_8304,a_8308)) {36}new sr_8318 SH(~M_8518,nego(~M_8520,RSA(~M_8525),~M_8522,~M\\$523, ~M_8524)) a_8315 {77}new k_8343 [78] insert longTermKeys_tbl(a_8315,k_8343,pk(k_8343)) \sim M_8552 = pk(k_8343) {64}get longTermKeys_tbl(a_8315,k_8343,pk(k_8343)) $CRT(\sim M_8576) = CRT(pk(k_8343))$ CCS(a_8317) $CKE(rsa_enc(\sim M_8552,a_8305)) = CKE(rsa_enc(pk($ k_8343),a_8305)) \sim M_8679 = zero ~X_1 $FIN(\sim M_8728) = FIN(tls12_prf(tls12_prf(a_8305,$ master_secret,(a_8306,sr_8318)),server_finished, (a_8306,sr_8318))) $FIN(\sim M_8740) = FIN(tls12_prf(tls12_prf(a_8305,$ master_secret,(a_8306,sr_8318)),server_finished, (a_8306,sr_8318))) {57}insert serverSession(a_8306,sr_8318,NoPSK, pk(k_8343),a_8310,nego(TLS12,RSA(StrongRSADecryption), a_8307,a_8304,a_8308),b2ae(tls12_prf(tls12_prf(a_8305,master_secret,(a_8306,sr_8318)),client_key_expansion, (sr_8318,a_8306))),b2ae(tls12_prf(tls12_prf(a_8305, master_secret,(a_8306,sr_8318)),server_key_expansion, (sr_8318,a_8306))),tls12_prf(tls12_prf(a_8305, master_secret,(a_8306,sr_8318)),client_finished, (a_8306,sr_8318)),tls12_prf(a_8305,master_secret, (a_8306,sr_8318))) CCS(a_8314) (a_8312,a_8313) ~M_8759