| Abbreviations |
| --- |
| ~M_16834 = sr_16485 |
| ~M_16836 = TLS12 |
| ~M_16841 = StrongRSADecryption |
| ~M_16838 = a_16467 |
| ~M_16839 = a_16468 |
| ~M_16840 = a_16469 |
| ~X_1 = SH(~M_16834,nego(TLS12,RSA(a_16479),a_16480,a_16481, a_16482)) = SH(sr_16485,nego(TLS12,RSA(a_16479), a_16480,a_16481,a_16482)) |
| ~X_2 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_16693, ~M_16834)),client_finished,(~M_16693,~M_16834))) = FIN(tls12_prf(tls12_prf(zero,master_secret,( cr_16484,sr_16485)),client_finished,(cr_16484, sr_16485))) |
| ~X_3 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_16693, ~M_16834)),server_finished,(((((CH(~M_16693,a_16478), SH(~M_16834,nego(TLS12,RSA(a_16479),a_16480,a_16481, a_16482))),CRT(~M_17151)),CCS(change_cipher_spec)), CKE(rsa_enc(~M_17151,zero))),FIN(tls12_prf(tls12_prf( zero,master_secret,(~M_16693,~M_16834)),client_finished, (~M_16693,~M_16834)))))) = FIN(tls12_prf(tls12_prf( zero,master_secret,(cr_16484,sr_16485)),server_finished, (((((CH(cr_16484,a_16478),SH(sr_16485,nego(TLS12, RSA(a_16479),a_16480,a_16481,a_16482))),CRT(pk( k_16486))),CCS(change_cipher_spec)),CKE(rsa_enc( pk(k_16486),zero))),FIN(tls12_prf(tls12_prf(zero, master_secret,(cr_16484,sr_16485)),client_finished, (cr_16484,sr_16485))))) |

A trace has been found.