Abbreviations
~M_40771 = sr_40422
~M_40773 = TLS12
~M_40778 = StrongRSADecryption
~M_40775 = a_40404
~M_40776 = a_40405
~M_40777 = a_40406
~X_1 = SH(~M_40771,nego(TLS12,RSA(a_40416),a_40417,a_40418,a_40419)) = SH(sr_40422,nego(TLS12,RSA(a_40416),a_40417,a_40418,a_40419))
~X_2 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_40630,~M_40771)),client_finished,(~M_40630,~M_40771))) = FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_40421,sr_40422)),client_finished,(cr_40421,sr_40422)))
~X_3 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_40630,~M_40771)),server_finished,((((((CH(~M_40630,a_40415),SH(~M_40771,nego(TLS12,RSA(a_40416),a_40417,a_40418,a_40419))),CRT(~M_41088)),CCS(change_cipher_spec)),CKE(rsa_enc(~M_41088,zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_40630,~M_40771)),client_finished,(~M_40630,~M_40771)))))) = FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_40421,sr_40422)),server_finished,((((((CH(cr_40421,a_40415),SH(sr_40422,nego(TLS12,RSA(a_40416),a_40417,a_40418,a_40419))),CRT(pk(k_40423))),CCS(change_cipher_spec)),CKE(rsa_enc(pk(k_40423),zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_40421,sr_40422)),client_finished,(cr_40421,sr_40422))))))

A trace has been found.