Abbreviations
~M_17 = AES_enc(smartthings_const,kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),bleAuthentication_const),a_20)
~M_18 = open_ch
~X_1 = (AES_enc(smartthings_const,kdf2(~M_12,bleAuthentication_const),~M_15),open_ch) = (AES_enc(smartthings_const,kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),bleAuthentication_const),n2_2),open_ch)
~M_19 = AES_enc(serial_number_const,kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),n2_2),n2_2)
~M_20 = open_ch
~M_21 = AES_enc(serial_number_const,kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),n2_2),n2_2)
~M_22 = open_ch
~X_2 = (serial_number_const,(~M_12,pre_app1)) = (serial_number_const,(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),pre_app1))
~X_3 = (AES_enc(~M_25,kdf2(~M_12,~M_15),~M_15),open_ch) = (AES_enc(secure_param_4,kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),n2_2),n2_2),open_ch)
~X_4 = (get_id(kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),privacy_const),secure_param_4,secure_param_4,secure_param_4),id_s)
~X_5 = (get_id(kdf2(derive_encryption_key(exp(exp(g,pri_c),kdf1(serial_number_const)),a_19),privacy_const),secure_param_4,secure_param_4,secure_param_4),(serial_number_const,id_p))

A trace has been found.