Abbreviations
~X_1 = (derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),(exp(g,pri_c),(SendPubkey,pre_app1)))
~M_9 = AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),bleAuthentication_const),n2_2)
~M_10 = open_ch
~M_11 = AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),rand_3),bleAuthentication_const),n1_2)
~M_12 = open_ch
~X_2 = (~M_11,open_ch) = (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),bleAuthentication_const),n1_2),open_ch)
~X_3 = (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(~M_3,derive_prikey_from_sn(serial_number_const)),~M_2),bleAuthentication_const),~M_7),open_ch) = (AES_enc(smartthings_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),bleAuthentication_const),n2_2),open_ch)
~M_13 = AES_enc(serial_number_const,derive_key(derive_encryption_key(exp(exp(g,pri_c),derive_prikey_from_sn(serial_number_const)),rand_3),n2_2),n2_2)
~M_14 = open_ch
~X_4 = (~M_13,open_ch) = (AES_enc(serial_number_const,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),n2_2),n2_2),n2_2),open_ch)
~M_15 = AES_enc(secure_param_4,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),n2_2),n2_2)
~M_16 = open_ch
~X_5 = (~M_15,open_ch) = (AES_enc(secure_param_4,derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),n2_2),n2_2),open_ch)
~X_6 = (get_id(derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),privacy_const),secure_param_4,secure_param_4,secure_param_4),(id_c,central_user_data_out))
~X_7 = (get_id(derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),privacy_const),secure_param_4,secure_param_4,secure_param_4),(id_p,peripheral_user_data_out))
~M_17 = tmp
~M_18 = AES_enc(sv,get_id(derive_key(derive_encryption_key(exp(exp(g,derive_prikey_from_sn(serial_number_const)),pri_c),rand_3),privacy_const),secure_param_4,secure_param_4,secure_param_4),tmp)
~M_19 = open_ch

A trace has been found.