A trace has been found.

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)

 $\sim$ M\_18 = open\_ch

~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)

 $a_19), pre_app1))$   $\sim X_3 = (AES_enc(\sim M_25, kdf2(\sim M_12, \sim M_15), \sim M_15), open_ch)$  =  $(AES_enc(secure, param_4, kdf2(derive, encryption_key))$ 

**Honest Process** Attacker {1}new sec\_ch (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\sim M, \sim M_1) = (derive\_hashed\_sn(serial\_number\_const), open\_ch)$ (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\sim M_2, \sim M_3) = (derive\_hashed\_sn(serial\_number\_const),$ (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\sim M_4, \sim M_5) = (derive\_hashed\_sn(serial\_number\_const), open\_ch)$ (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\sim M_6, \sim M_7) = | (derive_hashed_sn(serial_number_const), open_ch)$ (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\begin{tabular}{ll} M\_8,\sim M\_9) = (derive\_hashed\_sn(serial\_number\_const), open\_ch) \end{tabular}$ (serial\_number\_const,sn\_owner) {4}event Bounded(serial\_number\_const)  $(\sim M_10, \sim M_11) = (derive_hashed_sn(serial_number_const),$ (derive\_hashed\_sn(serial\_number\_const),(a\_19,pre\_app1)) {10} new pri\_c {14}event SendPubkey(sec\_ch,pri\_c,exp(g,pri\_c))  $(\sim M_12,(\sim M_13,\sim M_14)) = (derive\_encryption\_key(exp(exp(g,kdf1(serial_number_const)),pri_c),a_19),$   $(exp(g,pri_c),pre_app1))$  $(a_19,(\sim M_13,open_ch)) = (a_19,(exp(g,pri_c),open_ch))$  $(\sim M_15, \sim M_16) = (n2_2, open_ch)$ (a\_20,open\_ch)  $(\sim M_17, \sim M_18)$ {92}event SteppEnd1 {96} event SendSn(AES\_enc(serial\_number\_const,kdf2(derive\_encryption\_key(exp(exp(g,pri\_c),kdf1(serial\_number\_const)), a\_19),n2\_2),n2\_2))  $(\sim M_19, \sim M_20)$  $(\sim M_21, \sim M_22)$  $(a_21,pre_app1)$ {17}event StepsEnd1  $(\sim M_23, \sim M_24) = (unbound\_const, pre\_app1)$ ~X\_2 {32}event StepsEnd2 {33}new secure\_param\_4 {34} event SendSecureParam(secure\_param\_4)  $(\sim M_25 \sim M_26) = (secure_param_4, pre_app1)$ ~X\_5