Abbreviations	
~X_1 = (derive_encryption_key(Curve25519(Curve25519(gen, derive_prikey_from_sn(serial_number)),pri_c_1), rand_3),Curve25519(gen,pri_c_1))	
~M_3 = AES_enc(smartthings,derive_key(derive_encryption_key( Curve25519(Curve25519(gen,derive_prikey_from_sn( serial_number)),pri_c_1),rand_3),bleAuthentication), n1 2)	
~X_2 = AES_enc(serial_number,derive_key(derive_encryption_key( Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2) = AES_enc(serial_number,derive_key(	
derive_encryption_key(Curve25519(Curve25519(gen, pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n1_2),n1_2)	
~X_3 = (AES_dec(AES_enc(serial_number,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),n1_2),n1_2),derive_key(derive_prikey(curve25519(curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1), rand_3),n1_2),n1_2),derive_encryption_key(curve25519(curve25519(gen,derive_prikey_from_sn(serial_number)),	
pri_c_1),rand_3))  ~M_4 = AES_enc(privacy_iv_5,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(	
curve25519(Curve25519(gen,derive_prikey_from_sn( serial_number)),pri_c_1),rand_3),n1_2),n1_2)  ~M_5 = AES_enc(privacy_seed_5,derive_key(derive_encryption_key( Curve25519(Curve25519(gen,derive_prikey_from_sn(	
serial_number)),pri_c_1),rand_3),n1_2),n1_2)  ~M_6 = AES_enc(poolsize,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(	
serial_number)),pri_c_1),rand_3),n1_2),n1_2)  ~M_7 = AES_enc(time_sync_3,derive_key(derive_encryption_key(Curve25519(Curve25519(gen,derive_prikey_from_sn(serial_number)),pri_c_1),rand_3),n1_2),n1_2)	
~X_4 = AES_enc(smartthings,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),bleAuthentication),~M_9) = AES_enc(smartthings,	
derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),bleAuthentication),n2_2)	
~M_10 = AES_enc(smartthings,derive_key(derive_encryption_key( Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn( serial_number)),rand_3),bleAuthentication),a)	
~M_11 = AES_enc(serial_number,derive_key(derive_encryption_key( Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn( serial_number)),rand_3),n2_2),n2_2)	A trace
~X_5 = (AES_enc(AES_dec(~M_4,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)),	
derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)),~M),~M_2),~M_2),derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)),~M_9),~M_9),AES_enc(poolsize,derive_key(derive_encryption_key(	
Curve25519(~M_1,derive_prikey_from_sn(serial_number)),	
pri_c_1),derive_prikey_from_sn(serial_number)), rand_3),n2_2),n2_2),AES_enc(privacy_seed_5,derive_key( derive_encryption_key(Curve25519(Curve25519(gen,	
~X_6 = get_id(derive_key(derive_encryption_key(Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn(serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize)	
~X_7 = get_id(derive_key(derive_encryption_key(Curve25519( Curve25519(gen,pri_c_1),derive_prikey_from_sn( serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize)	
~M_12 = SHA256(concat(get_id(derive_key(derive_encryption_key( Curve25519(Curve25519(gen,pri_c_1),derive_prikey_from_sn( serial_number)),rand_3),privacy),privacy_iv_5, privacy_seed_5,poolsize),a_2))	
~X_8 = SHA256(concat(get_id(derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),privacy),AES_dec(~M_4,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2),AES_dec(~M_5,derive_key(derive_encryption_key(Curve25519(~M_1,derive_prikey_from_sn(serial_number)), ~M),~M_2),~M_2),poolsize),~M_13)) = SHA256(concat(	
= SHA256(concat( get_id(derive_key(derive_encryption_key(Curve25519(	

Attacker

**Honest Process** 

Beginning of process skepts   Beginn	Process step3c  Beginning of process step3c
[8] insert physicarial number, derive pirkey from susand number), derive pirkey from susand number), derive pirkey from susand number))  [27] get.physicarial number, derive pirkey from suserial number))  [27] get.physicarial number, derive pirkey from suserial number))  [27] get.physicarial number, derive hashed suserial number), curve25519(gen,derive pirkey from suserial number))  [27] get.physicarial number, derive hashed suserial number), curve25519(gen,derive pirkey from suserial number))  [27] get.physicarial number, derive hashed suserial number)	
Sert p0s(serial_number,derive_hashed_sn(serial_number), urve25519(gen,derive_prikey_from_sn(Serial_number)))	
nsert pos(serial number, derive_hashed_sn(serial_number), urve25519(gen,derive_prikey_from_sn(Serial_number)))  {27}get pos(serial_number, derive_hashed_sn(serial_number)), Curve25519(gen,derive_prikey_from_sn(serial_number)))  derive_hashed_sn(serial_number)  [29]new_rand 3  (derive_hashed_sn(serial_number), rand_3)	
{27} get p0s(serial_number, derive_prikey_from_sn(serial_number), Curve25519(gen, derive_prikey_from_sn(serial_number)))  derive_hashed_sn(serial_number)  {29} new rand 3  (derive_hashed_sn(serial_number), rand_3)	
derive hashed sn(serial number)  {29}new rand_3  (derive_hashed_sn(serial_number),rand_3)	
[29] new rand_3  (derive_hashed_sn(serial_number), rand_3)	
(derive_hashed_sn(serial_number),rand_3)	
$[11]$ new pri_c_1	
~X_1	
$(\sim M, \sim M\_1) = (rand\_3, Curve25519(gen, pri\_c\_1))$	
{34}new n1_2	
$\sim M_2 = n1_2$	
$\sim M_2 = n1_2$	
~M_3	
~M_3	
~X_2	
~X_3	
{20} new privacy_iv_5 {21} new privacy_seed_5	
{23}new time_sync_3	
(privacy_iv_5,privacy_seed_5,poolsize,time_sync_3)	
(~M_4,~M_5,~M_6,~M_7)	
{53} insert p1c(addrB,derive_key(derive_encryption_key(	
{76} get p0p(serial_number,derive_hashed_sn(serial_number), derive_prikey_from_sn(serial_number),Curve25519( gen,derive_prikey_from_sn(serial_number)))	
~M_8 = derive_hashed_sn(serial_number)	
$(\sim M, \sim M_1) = (rand_3, Curve25519(gen, pri_c_1))$	
$\{59\}$ new n2_2	
a	
$\sim$ M_9 = n2_2	