A trace has been found.

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), ~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\_encryption\_key(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( 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) 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) ~X\_5 = (AES\_enc(AES\_dec(~M\_4,derive\_key(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),~M\_9),~M\_9),AES\_enc(AES\_dec(~M\_5,derive\_key(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),~M\_9),~M\_9),AES\_enc(peolsize\_derive\_key(derive\_encryption\_key( 

~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)

~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\_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),salt1\_2))

	Honest Process						Attacker 
		Beginning of process step1c	Beginning of process step1p	Beginning of process step2c	Beginning of process step2p	Beginning of process user Beginning of process step3c Beginning of process step3p	
(serial_number,derive_hashed_sn(serial_number), Curve25519(gen,derive_prikey_from_sn(serial_number)	, er)))						
{8}insert p0p(serial number	er,derive hashed sn(serial number),						
derive_prikey_from_s: gen,derive_prikey	er,derive_hashed_sn(serial_number), sn(serial_number),Curve25519( y_from_sn(serial_number)))						
{2}insert p0s(serial_number,derive_hashed_sn(serial_number), Curve25519(gen,derive_prikey_from_sn(serial_number)))							
	{27} get p0s(serial_number,derive_hashed_sn(serial_number), Curve25519(gen,derive_prikey_from_sn(serial_number)))						
	Curve25515(gen,derive_prikey_nom_sn(serial_number))						
		4			derive_hashed_sn(s	serial_number)	
		{29} new rand_3					
	(derive_hashed_sn(serial_numbe	er),rand_3)					
	{11}new pri_c_1						
	~X_1						
					$(\sim M, \sim M_1) = (rand_3, Cur$	rve25519(gen,pri_c_1))	-
		{34} new n1_2					
					$\sim M_2 = 1$	n1 2	
					$\sim M_2 = 1$	n1_2	
					~M_3	3	
		4			~M_3	3	
					~X_2	2	
	~X 3						
	{20} new privacy_iv_5 {21} new privacy_seed_5 {23} new time_sync_3						
	{23} new time_sync_3						
	(privacy_iv_5,privacy_seed_5,poolsize	e,time_sync_3)					
					(~M_4,~M_5,~]	$\sim M_6, \sim M_7)$	
	Curve25519 serial_numb	c(addrB,derive_key(derive_end (Curve25519(gen,derive_prike er)),pri_c_1),rand_3),privacy),p privacy seed 5,poolsize)	ey_from_key( ey_from_sn( orivacy_iv_5,				
				n(serial number).			
		derive_p gen,	serial_number,derive_hashed_s: orikey_from_sn(serial_number), derive_prikey_from_sn(serial_n	Curve25519( amber)))			
					T.M. Q.	- derive hashed sp(serial number)	
						= derive_hashed_sn(serial_number)	
					(~M,~M_1	_1) = (rand_3,Curve25519(gen,pri_c_1))	
			{59}new n2_2				
						a	
						$\sim$ M 9 = n2 2	
						~X_4	
						~M_10	
						~M_11	