A trace has been found.

~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\_sn(serial\_number,derive\_prikey\_from\_sn(serial\_number)),rand\_3),n1\_2),n1\_2),derive\_key(derive\_encryption\_key(Gurve25519,derive\_key(fence)),rand\_3),n1\_2),n1\_2),derive\_key(fence) ~M\_4 = AES\_enc(privacy\_iv\_3,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\_3,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) ~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)

Abbreviations

~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\_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\_3,privacy\_seed\_3,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\_3,privacy\_seed\_3,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),~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\_3,
privacy\_seed\_3,poolsize),salt1\_2))

Beginning of process step0s   Beginning of process step0p   Beginning of process step1p   Beginning of process step1c   Beginning of process step2p   Beginn											serial_number)),rand_3; privacy_seed_3,p
							Honest Process				Attac
	Beginning of	f process step0s	of process step0p Beginning of process step1s	Beginning of proce	ress step1c	Beginning of process step1p	Beginning of process step2c	Beginning of r	process step2p Bea	sinning of process user   Beginning of process step3c   Beginning of process	s sten3n
		Curve25519(gen,derive_prikey_from_sn(serial_numbe	er)))								
		{8}insert p0p(serial_number derive_prikey_from_singen,derive_prikey	er,derive_hashed_sn(serial_number), n(serial_number),Curve25519( r from sn(serial_number)))								
** Secretary and secretary and a contract of the contract of t	2}insert p0s(serial_number,d										
The content of the	Curve25519(gen,derive_pri		{27} get p0s(serial_number,derive_hashed_sn(serial_number),								
Macro action count action and if  ( There of _   )  ( The of _			Curve25519(gen,derive_prikey_from_sn(serial_number)))								
Classes   Clas				4				deri	rive_hashed_sn(serial_num	aber)	
1-34.4   12.1				{29} new rar	.nd_3						
[23] (23) (23) (23) (23) (23) (23) (23) (23)			(derive_hashed_sn(serial_numbe	er),rand_3)							
[10] eq. 2			{11} new pri_c_1								
(A) the second 2   1-32 = 0.12			~X_1								
[10] eq. 2								(~M,~M 1)	) = (rand 3,Curve25519(α	gen,pri c 1))	
(2) (2) (3) (3) (3) (3) (3) (3) (3) (3) (3) (3					1 2			· · · · · · · · · · · · · · · · · · ·			
(2) (2) (3) (3) (3) (3) (3) (3) (3) (3) (3) (3				{34}new n.	11_2						
200 con freezy by 3  [200 con freezy by 3  [									$\sim M_2 = n1_2$		-
All case prices to the second and th				4					~M_2 = n1_2		
(23) constituency and 3  [23) constituency and 3  [25) constituency and 4  [26) constituency and 4  [27) constituency and 4  [27] constituency and 4  [28] constituency and									~M_3		
(23) new privacy is 23 (23) new privacy and 3, past deviations by in 3)  (privacy is 3, privacy, and 3, past deviations by in 3)  (privacy is 3, privacy, and 3, past deviations by in 3)  (b) Singer's blooded state of the privacy from the privac				4							
(A) see privacy and 3 (2) new privacy and 3				4					~X_2		
(21) new jerney as (3)  - (25) new inter year 3  (privary in 3 privary seed 3 positions, transport (3)  (privary in 3 privary seed 3 positions, transport (3)  (privary in 3 privary seed 3 positions, transport (3)  (privary in 3 privary seed 3 positions)  (privary in 4 privary in 5 privary i			~X_3								
(23) men interpret 3  (23) men interpret 3  (24) men interpret 3  (25) men interpret 3  (26) men interpret 3  (26) men interpret 3  (26) men interpret 3  (26) men interpret 3  (27) men interpret 3  (28) men interpret 3			{20}new privacy iv 3								
(privacy iv 3.privacy seed 3.poolsize time syste 3)  (Schingen pleaddright interive keylderive encryption keyl seeml number) pri of listed 3 privacy privacy iv 3 privacy seed 3 provincy privacy iv 3 privacy seed 3 provincy seed 3 provincy seed 3 privacy seeml numbers of success and numbers of success and success of success and success of s			{21} new privacy_seed_3 {23} new time_sync_3								
(~M 4,~M 5,~M 6,~M 7)  (S4) insert plotably it get is large price; from set sectal number) price; and objective, plane is large price; from set sectal number) price; and objective, plane is large price; and objective, plane is large price; and objective, plane is large price; from set sectal number).  (78) set player player in manufacture, bashed_set(serial_number), curve_255.19  gen, denve_price; from_satserial_number))  -M_8 = derive_hashed_sat(serial_number)  (-M_A M_1) = (rand_3 Curve_25519(gen.pric_1))				e time sync 3)							
(54) insert plotaddrB.get iddorwe key(derive enreption key(			(privacy_iv_3,privacy_seea_3,poorsize	- SyllC_S/							
{78}qet pop(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)  (~M,~M_1) = (rand_3,Curve25519(gen,pri_c_1))									~M_4,~M_5,~M_6,~M_7		
{78}qet pop(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)  (~M,~M_1) = (rand_3,Curve25519(gen,pri_c_1))			{54}insert p1c(a Curve25519	addrB,get_id(derive 9(Curve25519(gen,d	key(derive_encrederive_prikey_from	yption_key( om_sn(					
$\sim M\_8 = derive\_hashed\_sn(serial\_number)$ $(\sim M, \sim M\_1) = (rand\_3, Curve25519(gen, pri\_c\_1))$			Serial_Hullip								
$(\sim M, \sim M\_1) = (rand\_3, Curve 25519(gen, pri\_c\_1))$					{78} <mark>get</mark> p0p(serion derive_prike gen,derive_	al_number,derive_hashed_sn(s ey_from_sn(serial_number),Cur ive_prikey_from_sn(serial_num	erial_number), rve25519( ber)))				
$(\sim M, \sim M\_1) = (rand\_3, Curve 25519(gen, pri\_c\_1))$											
(60) new n2 2   a   -M_9 = n2 2   -X_4   -M_10   -M_11									$(\sim M, \sim M_1) = (rand)$	d_3,Curve25519(gen,pri_c_1))	
**************************************						{60} new n2_2					
$-M 9 = n2 2$ $-X_{4}$ $-M_{10}$										a	
~X_4  ~M_10									~]	$M_9 = n2_2$	
~M_10										~X_4	
~M 11										~M_10	
										~M 11	