$Abbreviations $$ \sim X_1 = HMAC_SHA256(\sim M_5, concat(concat(concat(concat(concat(concat(concat(a_2, \sim M_7), zero), iocap_A), addr_A), addr_B)) $$ = HMAC_SHA256($$ p256(gen, exp_P_1), concat(concat(concat(concat(concat(concat(a_2, nb_6), zero), iocap_A), addr_A), addr_B)) $$$

Attacker

			Honest Process		Atta
			$\begin{array}{c} \{1\} \\ \text{new } \exp_C_1 \\ \{2\} \\ \text{new } \exp_P_1 \end{array}$		
Beginning of process BC_stack_central Beginning of process BC_stack_peripheral Beginning of process BCapp_central Beginning Of BCapp_central Beginning Of BCapp_central Beginning Of BCapp_central BCapp_central BCapp_central BCapp_central BCapp_central BCapp_central BCapp_central BCapp_central BCa	Beginning of process BLE_stack_central p_peripheral \[\{56\}\text{new skdm}_2 \] \[\{57\}\text{new ivm}_2 \] \[\{70\}\text{new ivs}_\]	stack_peripheral s_2 Beginning of process BLEapp_central Beginning of process _2	BLEapp_peripheral Beginning of process step1c Beginning of process step1p Beginning of process	ss step2cjw Beginning of process step2pjw Beginning of	process step3c Beginning of process step3p Beginning of process step4c Beginning of process step4p
				$\sim M = p256(g$	en,exp_C_1)
			$(\sim M_1, \sim M_2) = (skdm_2, ivm_2)$		
			(a,a_1) $(\sim M_3, \sim M_4) = (skds_2, ivs_2)$		
					gen
					$\sim M_5 = p256(gen, exp_P_1)$
			{96}insert p1p(addr_A,gen,p256(gen,exp_P_1),p256(
			gen,exp_r_1))	{117}get p1p(addr_A,gen,p256(gen,exp_P_1),p256(gen,exp_P_1))	
					$\sim M_6 = HMAC_SHA256(nb_6,concat(concat(p256(gen, exp_P_1),gen),zero))$
					a_2
					$\sim M_{-}7 = nb_{-}6$
				{116}insert p2p(addr_A,a_2,nb_6,zero,zero,p256(gen,exp_P_1))	
					{145}get p2p(addr_A,a_2,nb_6,zero,zero,p256(gen, exp_P_1))
					~X_1
					{144}insert p3p(addr_A,a_2,nb_6,p256(gen,exp_P_1))
					{167}get p3p(addr_A,a_2,nb_6,p256(gen,exp_P_1)) {161}insert bc_key_p(addr_A,HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(a_2,nb_6),btlk),addr_A),addr_B))) {166}insert le_key_p(addr_A,AES_CMAC(AES_CMAC(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a_2,nb_6),btlk),addr_A),addr_B)),SALT),brle))
	{81} get le_key_p(addr_A,AES_CMAC(A p256(gen,exp_P_1),concat(con- a_2,nb_6),btlk),addr_A),addr_	AES_CMAC(HMAC_SHA256(ncat(concat(r_B)),SALT),brle))			brle))
				7	
		a 3	\sim $X_{_2}$		
		a_3 PI Fren			
		BLErsp			
			\sim M_{-}°	9	