Abbreviations

~M_4 = AES_CCM(BCreq,HMAC_SHA256(lk_1,concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2)))),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))

Attacker **Honest Process** Beginning of process BC_secure_pairing {2}new lk_1 {3}insert bc_key_c(addr_B,lk_1) {4}insert bc_key_p(addr_A,lk_1) Beginning of process BC_stack_central Beginning of process BC_stack_peripheral_compromised Beginning of process BCapp_central {9}insert le_key_c(addr_B,AES_CMAC(AES_CMAC(lk_1, SALT),brle)) {14}insert le_key_p(addr_A,AES_CMAC(AES_CMAC(lk_1, SALT),brle)) {38}get bc_key_c(addr_B,lk_1) {16} new rand_m_2 $\sim M = rand_m_2$ [79] get bc_key_p(addr_A,lk_1) {54} new rand_s_2 \sim M = rand_m_2 \sim M 1 = rand s 2 \sim M 1 = rand s 2 \sim M_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2))) ~M_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2))) \sim M_3 = next32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2))) \sim M_3 = next32bit(HMAC_SHA256(HMAC_SHA256(lk_1, concat(concat(btak,addr_A),addr_B)),concat(rand_m_2, rand_s_2))) BCreq ~M 4 ~M 4 \sim M 5 = BCreq