A trace has been found. **Honest Process** Attacker {1}new Appkey 1 {2}new NwkKey 3 {3}new JoinEUI 3 {4}new DevEUI 3 {5}new DevNonce 3 {6}new DevAddr 3 \sim M = JoinEUI 3 Beginning of process ED |Beginning of process JS| $(\sim M \ 1, \sim M \ 2, \sim M \ 3, \sim M \ 4) = (JoinEU[\ 3, DevEUI \ 3, DevNonce \ 3, \ 4])$ mac((JoinEUI 3,DevEUI 3,DevNonce 3),NwkKey 3)) $(\sim M, \sim M_2, \sim M_3, \sim M_4) = (JoinEUI_3, DevEUI_3, DevNonce_3, \sim M_4) = (JoinEUI_3, DevNonce_3, \sim M_4)$ mac((JoinEUI 3, DevEUI 3, DevNonce 3), NwkKey 3)) {34} new JoinNonce 2 {35}new Home NetID 2 \sim M | 5 = senc((JoinNonce 2, Home NetID 2, DevAddr 3, mac((JoinNonce_2,Home_NetID_2,DevAddr_3),NwkKey_3)), NwkKey 3) \sim M 5 = senc((Join Nonce 2, Home NetID 2, DevAddr 3, mac((JoinNonce 2, Home_NetID_2, DevAddr_3), NwkKey_3)), NwkKey 3) {22}new FCntUp_2 $(\sim M_6, \sim M_7)$ {26} event endED

Abbreviations

~M 6 = senc((m,FCntUp 2),KgenSenc((JoinNonce 2,JoinEUI 3, DevNonce 3, four), NwkKey 3))

 \sim M_7 = mac((DevAddr_3,FCntUp_2,m),KgenSenc((JoinNonce_2, JoinEUI 3, DevNonce 3, four), NwkKey 3))