DevNonce 3, four), NwkKey 3)) A trace has been found. \sim M_7 = mac((DevAddr_3,FCntUp_2,m),KgenSenc((JoinNonce_2, JoinEUI_3,DevNonce_3,four),NwkKey_3)) Attacker Honest Process {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 | $(\sim M_1, \sim M_2, \sim M_3, \sim M_4) = (JoinEUI_3, DevEUI_3, DevNonce_3, \sim M_4, \sim M_4) = (JoinEUI_3, DevEUI_3, DevNonce_3, \sim M_4, \sim M_$ mac((JoinEUI 3,DevEUI 3,DevNqnce 3),NwkKey 3)) $(\sim M, \sim M | 2, \sim M | 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 2, \sim M | 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, DevNonce 3, 3, \sim M | 4) = (JoinEUI 3, M | 4) = (Joi$ mac((JoinEUI 3, DevEUI 3, DevNonce 3), NwkKey 3)) {34} new JoinNonce 2 {35} new Home NetID 2 \sim M = senc((JoinNonce 2, Home NetID 2, DevAddr 3, mac((JoinNonce_2, Home_NetID_2, DevAddr_3), Nwkkey_3)), NwkKey 3) \sim M 5 = senc((JoinNonce 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 Phase 1 \sim M 8 = Appkey 1 \sim M 9 = NwkKey_3 The attacker has the message 1-proj-2-tuple(sdec(~M 6,KgenSenc((1-proj-4-tuple($sdec(\sim M_5,\sim M_9)$), \sim M, \sim M 3,four), \sim M 9))) = m in phase 1

Abbreviations

 \sim M_6 = senc((m,FCntUp_2),KgenSenc((JoinNonce_2,JoinEUI_3,