Abbreviations \sim 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)) **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 JS| $(\uparrow M_1, \sim M_2, \sim M_3, \sim M_4) = (JoinEUI_3, DevEUI_3, DevNonce \beta,$ mac((JoinEUI_3,DevEUI_3,DevNonce 3),NwkKey 3)) $(\sim M, \sim M_2, \sim M_3, \sim M_4) = (JoinEUI_3, DevEUI_3, DevNonce_3, mac((JoinEUI_3, DevEUI_3, DevNonce_3), NwkKey_3))$ {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((JoinNonce 2, Home NetlD 2, DevAddr 3, mac((JoinNonce_2, Home_NetID_2, DevAddr_3), NwkKey_3)), NwkKey 3) $(\sim M_6, \sim M_7)$ $(\sim M \perp 6, \sim M_{\perp}7)$

Beginning of process ED

{22}new FCntUp_2

{26} event endED

{46} event endJS

A trace has been found.