

A trace has been found.

Honest Process

Attacker

$\{1\}$ new devEUI_3
$\{2\}$ new appEUI_3

Beginning of process ED
$\{5\}$ new privEK_ED_1
$\{7\}$ event EDsendmessage1

Beginning of process JS
$\{54\}$ new privEK_AS_1

$(\sim M, \sim M_1, \sim M_2) = (\exp(g, \text{privEK_ED_1}), \text{devEUI_3}, \text{appEUI_3})$

$(a, \sim M_2, a_1) = (a, \text{appEUI_3}, a_1)$

$\{11\}$ event EDgetmessage2
