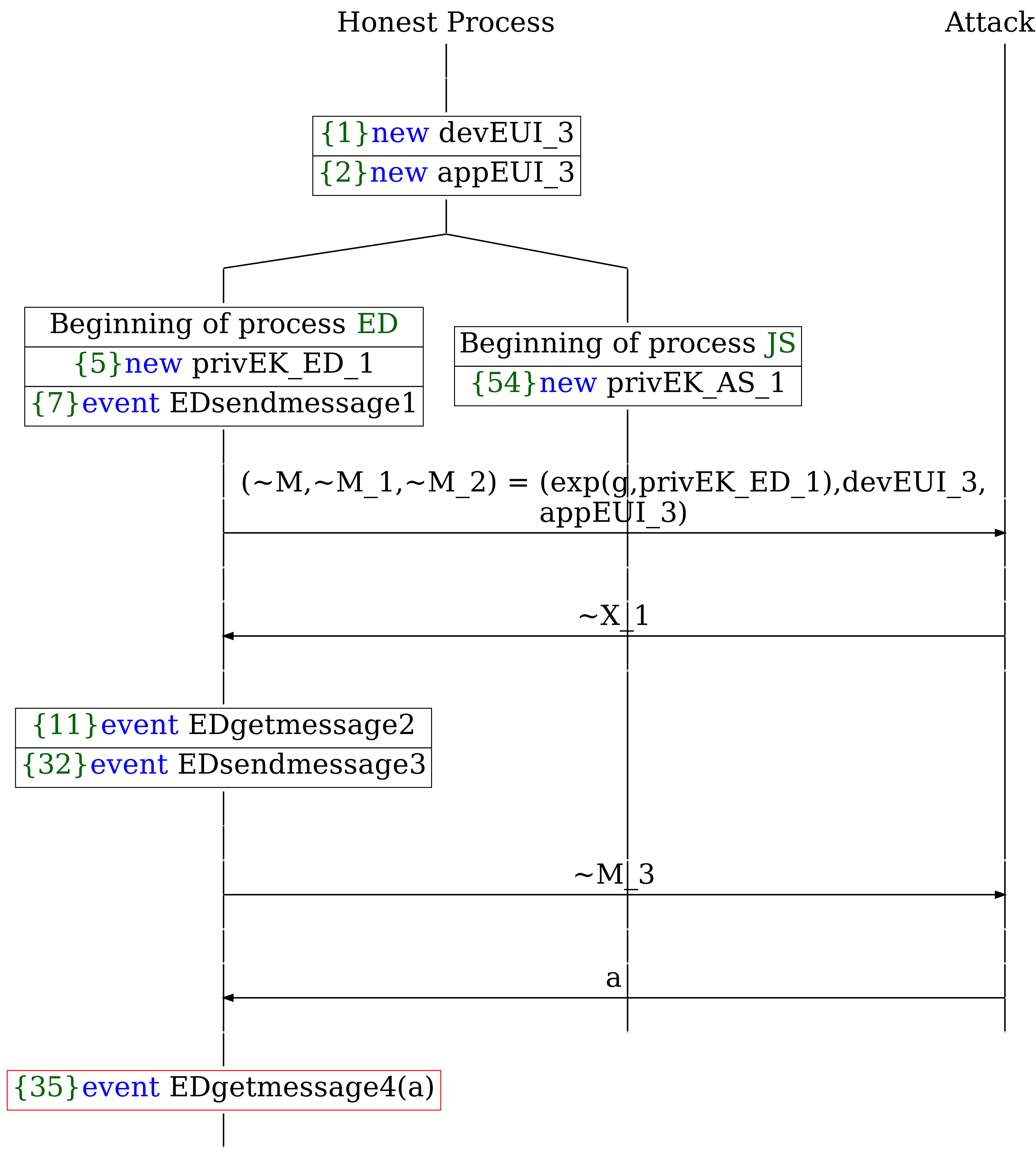
| Abbreviations |
|---|
| ~X_1 = (g,~M_2,xor(HKDFexpand(HKDFextract(emptyextractKey,<br>~M),sha256((sha256((~M,~M_1,~M_2)),g,~M_2)),emptystring),<br>(cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,~M),~M),sha256((sha256((~M,~M_1,<br>~M_2)),g,~M_2)),K_2m_constantstring),HKDFexpand(<br>HKDFextract(HKDFextract(emptyextractKey,~M),~M),<br>sha256((sha256((~M,~M_1,~M_2)),g,~M_2)),IV_2m_constantstring),<br>emptystring,(sha256((sha256((~M,~M_1,~M_2)),g,<br>~M_2)),cred_AS)))))<br>= (g,appEUI_3,xor(HKDFexpand(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),emptystring),(cred_AS,AEAD_enc(HKDFexpand(<br>HKDFextract(HKDFextract(emptyextractKey,exp(g,<br>privEK_ED_1)),exp(g,privEK_ED_1)),sha256((sha256(<br>(exp(g,privEK_ED_1),devEUI_3,appEUI_3)),g,appEUI_3)),<br>K_2m_constantstring),HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),IV_2m_constantstring),emptystring,<br>(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),cred_AS))))) |
| ~M_3 = AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((sha256((exp(g,privEK_ED_1),devEUI_3,<br>appEUI_3)),g,appEUI_3)),xor(HKDFexpand(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),sha256((sha256(<br>(exp(g,privEK_ED_1),devEUI_3,appEUI_3)),g,appEUI_3)),<br>emptystring),(cred_AS,AEAD_enc(HKDFexpand(HKDFextract(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),K_2m_constantstring),<br>HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),sha256(<br>(sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),IV_2m_constantstring),emptystring,<br>(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),cred_AS)))))),K_2m_constantstring),<br>HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),sha256(<br>(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),xor(HKDFexpand(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),emptystring),<br>(cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),K_2m_constantstring),HKDFexpand(HKDFextract(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),IV_2m_constantstring),<br>emptystring,(sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),cred_AS)))))),<br>IV_3ae_constantstring),(cred_ED,AEAD_enc(HKDFexpand(<br>HKDFextract(HKDFextract(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),exp(g,<br>privEK_ED_1)),sha256((sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),xor(HKDFexpand(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),emptystring),(cred_AS,AEAD_enc(HKDFexpand(<br>HKDFextract(HKDFextract(emptyextractKey,exp(g,<br>privEK_ED_1)),exp(g,privEK_ED_1)),sha256((sha256(<br>(exp(g,privEK_ED_1),devEUI_3,appEUI_3)),g,appEUI_3)),<br>K_2m_constantstring),HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),IV_2m_constantstring),emptystring,<br>(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),cred_AS)))))),K_3m_constantstring),<br>HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),sha256(<br>(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),xor(HKDFexpand(HKDFextract(emptyextractKey,<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),emptystring),<br>(cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),K_2m_constantstring),HKDFexpand(HKDFextract(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),IV_2m_constantstring),<br>emptystring,(sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),cred_AS)))))),<br>IV_3m_constantstring),emptystring,(sha256((sha256(<br>(exp(g,privEK_ED_1),devEUI_3,appEUI_3)),g,appEUI_3)),<br>cred_AS))),(emptystring,sha256((sha256((sha256(<br>(exp(g,privEK_ED_1),devEUI_3,appEUI_3)),g,appEUI_3)),<br>xor(HKDFexpand(HKDFextract(emptyextractKey,exp(<br>g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),emptystring),<br>(cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(<br>emptyextractKey,exp(g,privEK_ED_1)),exp(g,privEK_ED_1)),<br>sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),<br>g,appEUI_3)),K_2m_constantstring),HKDFexpand(HKDFextract(<br>HKDFextract(emptyextractKey,exp(g,privEK_ED_1)),<br>exp(g,privEK_ED_1)),sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),IV_2m_constantstring),<br>emptystring,(sha256((sha256((exp(g,privEK_ED_1),<br>devEUI_3,appEUI_3)),g,appEUI_3)),cred_AS)))))))) |

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
(~M,~M_1,~M_2) = (exp(g,privEK_ED_1),devEUI_3,
appEUI_3)
~X_1
{11}event EDgetmessage2
{32}event EDsendmessage3
~M_3
a
{35}event EDgetmessage4(a)