A trace has been found.

Abbreviations
~M = exp(g,privEK_ED_1)
~M_1 = devEUI_3
~M_2 = appEUI_3
~M_3 = sign((exp(g,privEK_ED_1),devEUI_3,appEUI_3), EDsecretsignkey_1)
~M_4 = exp(g,privEK_AS_1)
~M_5 = appEUI_3
~M_6 = xor((cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),K_2m_constantstring),HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),IV_2m_constantstring),emptystring,(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),cred_AS))),HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),cred_AS)),HKDFexpand(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),emptystring))
~M_7 = sign((exp(g,privEK_AS_1),appEUI_3,xor((cred_AS,AEAD_enc(HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),K_2m_constantstring),HKDFexpand(HKDFextract(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),IV_2m_constantstring),emptystring,(sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),cred_AS))),HKDFexpand(HKDFextract(emptyextractKey,exp(exp(g,privEK_ED_1),privEK_AS_1)),sha256((sha256((exp(g,privEK_ED_1),devEUI_3,appEUI_3)),exp(g,privEK_AS_1),appEUI_3)),emptystring))),ASsecretsignkey_1)