

A trace has been found.

Abbreviations
$\sim M_3 = \text{exp}(g, \text{privEK_AS_1})$
$\sim M_4 = \text{appEUI_3}$
$\sim M_5 = \text{xor}((\text{cred_AS}, \text{AEAD_enc}(\text{HKDFexpand}(\text{HKDFextract}(\text{HKDFextract}(\text{emptyextractKey}, \text{exp}(a, \text{privEK_AS_1})), \text{exp}(a, \text{privEK_AS_1})), \text{sha256}((\text{sha256}((a, \text{devEUI_3}, \text{appEUI_3})), \text{exp}(g, \text{privEK_AS_1}), \text{appEUI_3})), \text{K_2m_constantstring}), \text{HKDFexpand}(\text{HKDFextract}(\text{HKDFextract}(\text{emptyextractKey}, \text{exp}(a, \text{privEK_AS_1})), \text{exp}(a, \text{privEK_AS_1})), \text{sha256}((\text{sha256}((a, \text{devEUI_3}, \text{appEUI_3})), \text{exp}(g, \text{privEK_AS_1}), \text{appEUI_3})), \text{IV_2m_constantstring}), \text{emptystring}, (\text{sha256}((\text{sha256}((a, \text{devEUI_3}, \text{appEUI_3})), \text{exp}(g, \text{privEK_AS_1}), \text{appEUI_3})), \text{cred_AS}))), \text{HKDFexpand}(\text{HKDFextract}(\text{emptyextractKey}, \text{exp}(a, \text{privEK_AS_1})), \text{sha256}((\text{sha256}((a, \text{devEUI_3}, \text{appEUI_3})), \text{exp}(g, \text{privEK_AS_1}), \text{appEUI_3})), \text{exp}(g, \text{privEK_AS_1}), \text{appEUI_3})), \text{emptystring}))$

