

Abbreviations
$\sim M = \text{symenc}(\text{hkdf}(\text{hash}(\text{exp}(\text{P}, \text{emul}(\text{r}_2, \text{b}))), \text{concat}(\text{exp}(\text{P}, \text{a}), \text{exp}(\text{P}, \text{b}), \text{getid}(\text{exp}(\text{P}, \text{a})), \text{getid}(\text{exp}(\text{P}, \text{b})), \text{kCTX})), \text{secretMsg})$
$\sim M_1 = \text{symtag}(\text{hkdf}(\text{hash}(\text{exp}(\text{P}, \text{emul}(\text{r}_2, \text{b}))), \text{concat}(\text{exp}(\text{P}, \text{a}), \text{exp}(\text{P}, \text{b}), \text{getid}(\text{exp}(\text{P}, \text{a})), \text{getid}(\text{exp}(\text{P}, \text{b})), \text{kCTX})), \text{symenc}(\text{hkdf}(\text{hash}(\text{exp}(\text{P}, \text{emul}(\text{r}_2, \text{b}))), \text{concat}(\text{exp}(\text{P}, \text{a}), \text{exp}(\text{P}, \text{b}), \text{getid}(\text{exp}(\text{P}, \text{a})), \text{getid}(\text{exp}(\text{P}, \text{b})), \text{kCTX})), \text{secretMsg}))$
$\sim M_2 = \text{ediv}(\text{r}_2, \text{eadd}(\text{symtag}(\text{hkdf}(\text{hash}(\text{exp}(\text{P}, \text{emul}(\text{r}_2, \text{b}))), \text{concat}(\text{exp}(\text{P}, \text{a}), \text{exp}(\text{P}, \text{b}), \text{getid}(\text{exp}(\text{P}, \text{a})), \text{getid}(\text{exp}(\text{P}, \text{b})), \text{kCTX})), \text{symenc}(\text{hkdf}(\text{hash}(\text{exp}(\text{P}, \text{emul}(\text{r}_2, \text{b}))), \text{concat}(\text{exp}(\text{P}, \text{a}), \text{exp}(\text{P}, \text{b}), \text{getid}(\text{exp}(\text{P}, \text{a})), \text{getid}(\text{exp}(\text{P}, \text{b})), \text{kCTX})), \text{secretMsg})), \text{a}))$

A trace has been found.

