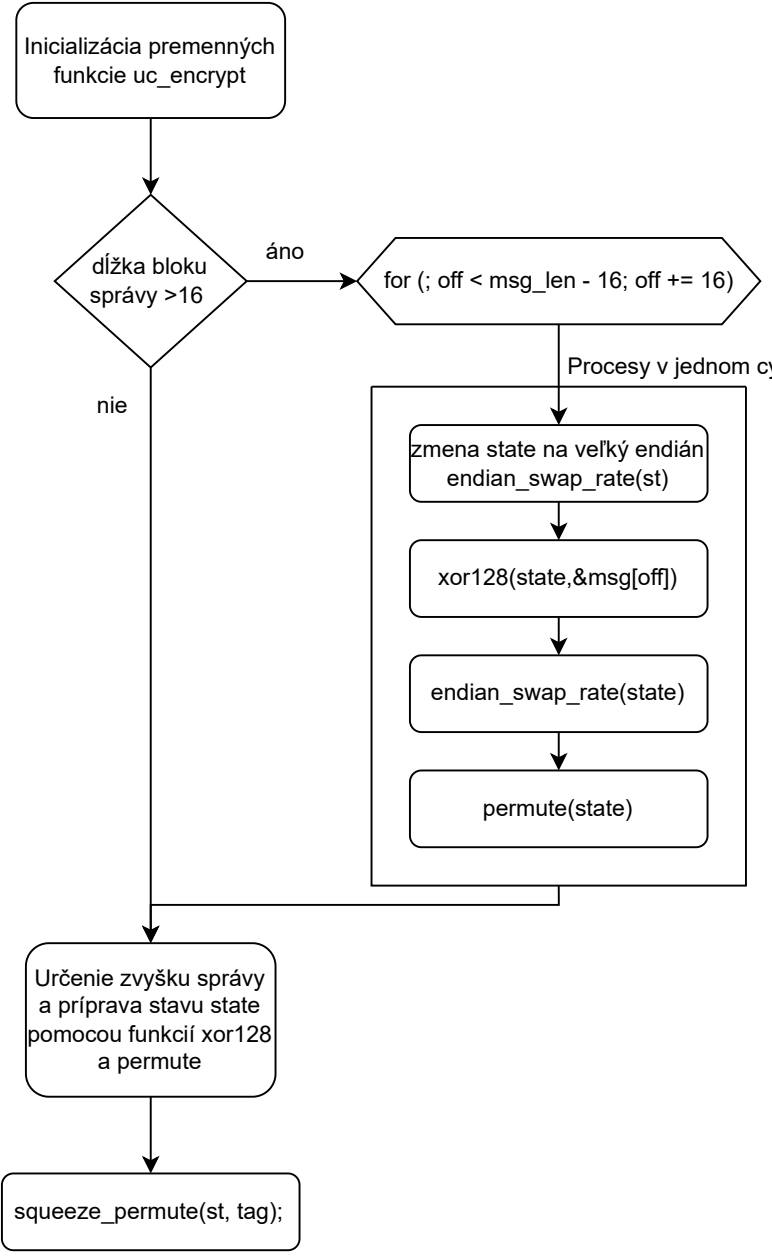
Inicializácia premenných funkcie uc_encrypt
dĺžka bloku správy >16
áno
for (; off < msg_len - 16; off += 16)
Procesy v jednom cykle
nie
zmena state na veľký endián endian_swap_rate(st)
xor128(state,&msg[off])
endian_swap_rate(state)
permute(state)
Určenie zvyšku správy a príprava stavu state pomocou funkcií xor128 a permute
squeeze_permute(st, tag);