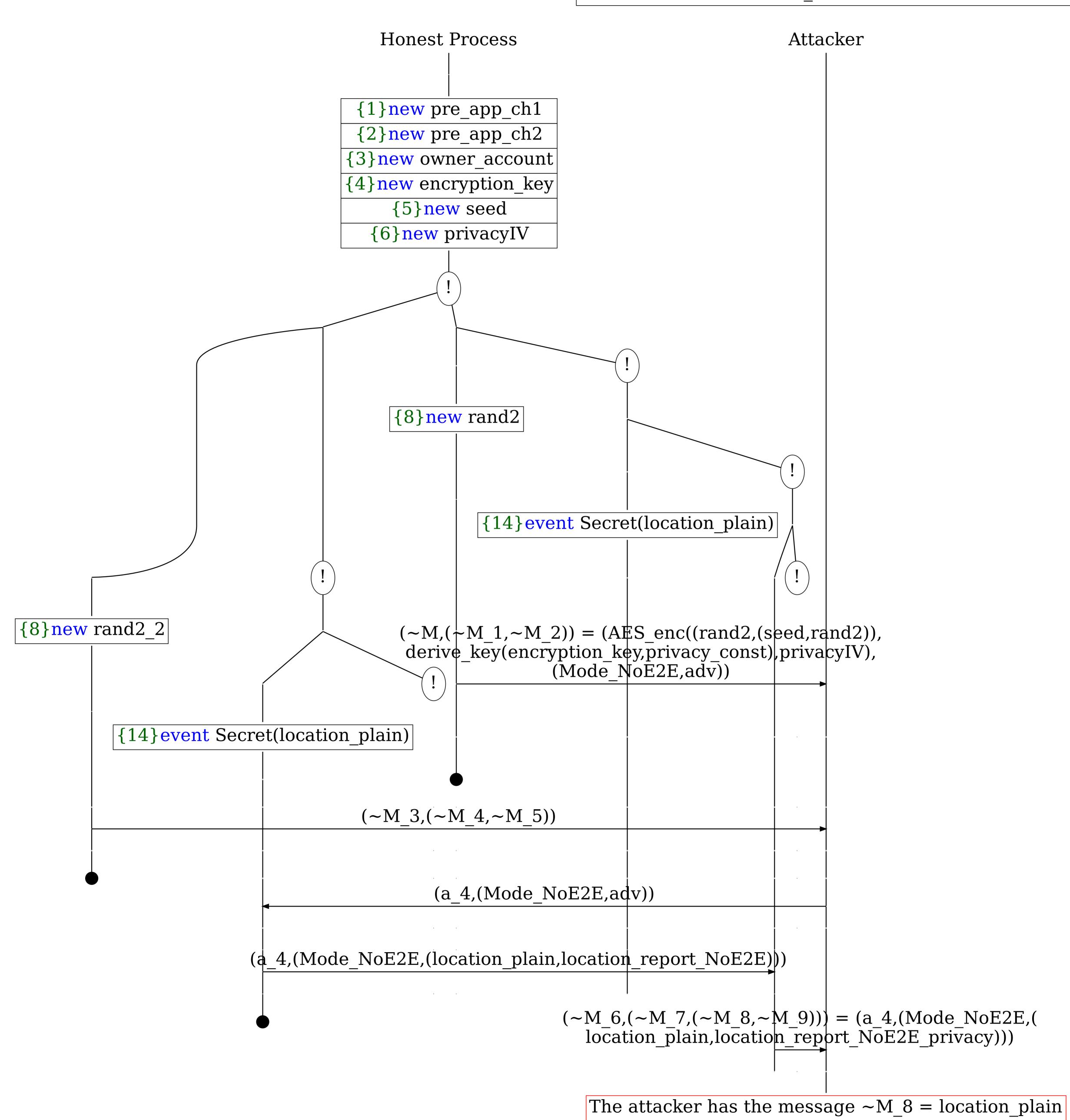
Abbreviations

~M_3 = AES_enc((rand2_2,(seed,rand2_2)),derive_key(encryption_key,privacy_const),privacyIV)

 \sim M_4 = Mode_NoE2E

 \sim M 5 = adv



A trace has been found.