SAT | **U_1** | **U_2**

Encrypt: $C_1 = enc(SK_{u1,\,SAT}, M)$

Generate: T_1

Compute: $MAC_1 = MAC(MK_{u1,\,SAT}, C_1 \| T_1)$

Pack: $msg_1 = (MAC_1 \| C_1 \| T_1)$

$msg_1 = (MAC_1 \| C_1 \| T_1)$ →

Verify: $MAC_1 ? = MAC(MK_{u1,\,SAT}, C_1 \| T_1)$

Generate: T_2

Check: $T_2 - T_1 <_{\Delta} T$

Decrypt: $M = dec(SK_{u1,\,SAT}, C_1)$

Process: $M = DF(M)$

Encrypt: $C_2 = enc(SK_{u1,\,u2}, M)$

Compute: $MAC_2 = MAC(MK_{u1,\,SAT}, C_2 \| T_2)$

Pack: $msg_2 = (MAC_2 \| C_2 \| T_2)$

$msg_2 = (MAC_2 \| C_2 \| T_2)$ →

Generate: T_3

Verify: $MAC_2 ? = MAC(MK_{u1,\,u2}, C_2 \| T_2)$

Check: $T_3 - T_2 <_{\Delta} T$

Decrypt: $M = dec(SK_{u1,\,u2}, C_2)$

Encrypt: $C_3 = enc(SK_{u1,\,u2}, M_1)$

Generate: T_4

Compute: $MAC_3 = MAC(MK_{u1,\,u2}, C_3 \| T_4)$

Pack: $msg_3 = (MAC_3 \| C_3 \| T_4)$

← $msg_3 = (MAC_3 \| C_3 \| T_4)$

Verify: $MAC_3 ? = MAC(MK_{u1,\,u2}, C_3 \| T_4)$

Generate: T_5

Check: $T_5 - T_4 <_{\Delta} T$

Decrypt: $M_1 = dec(SK_{u1,\,u2}, C_3)$

Process: $M_1 = DF(M_1)$

Encrypt: $C_4 = enc(SK_{u1,\,SAT}, M_1)$

Compute: $MAC_4 = MAC(MK_{u1,\,SAT}, C_4 \| T_5)$

Pack: $msg_4 = (MAC_4 \| C_4 \| T_5)$

← $msg_4 = (MAC_4 \| C_4 \| T_5)$

Generate: T_6

Verify: $MAC_4 ? = MAC(MK_{u1,\,SAT}, C_4 \| T_5)$

Check: $T_6 - T_5 <_{\Delta} T$

Decrypt: $M_1 = dec(SK_{u1,\,SAT}, C_4)$