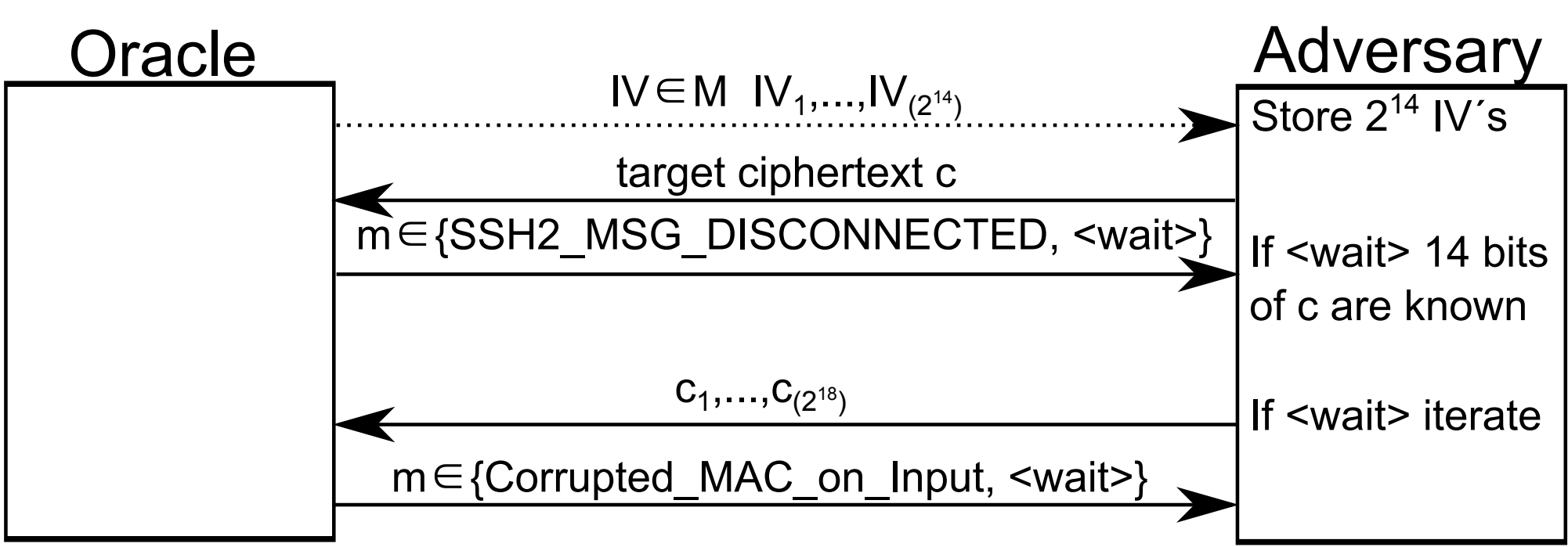
Oracle
Adversary
IV∈M IV1,...,IV(2^14)
Store 2^14 IV´s
target ciphertext c
m∈{SSH2_MSG_DISCONNECTED, <wait>}
If <wait> 14 bits of c are known
c1,...,c(2^18)
If <wait> iterate
m∈{Corrupted_MAC_on_Input, <wait>}