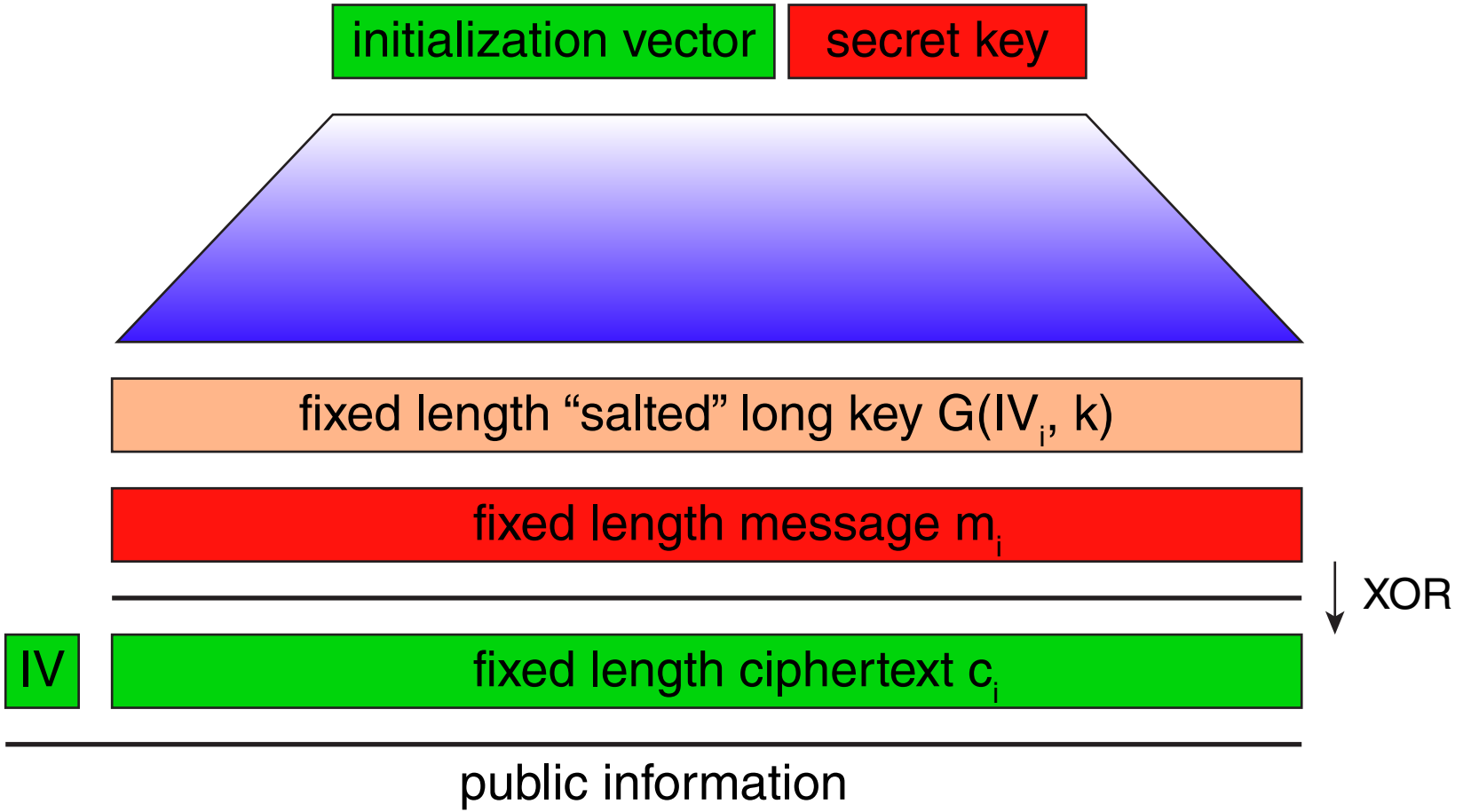
initialization vector
secret key
fixed length “salted” long key G(IV$_i$, k)
fixed length message m$_i$
XOR
IV
fixed length ciphertext c$_i$
public information