CTR mód

Vytvoříme zprávy $m_0 = 0^n$ a $m_1 = 1^n$ a dostaneme zpět challenge ciphertext (IV, c) pro zprávu m_b, kde $c = c_1 c_2 \dots c_l$. Dotážeme se dešifrovacího orákula na ciphertext $(IV + 1, c')$ pro $c' = c_2 c_3 \dots c_l c_1$ a obdržíme zprávu m'.

Z fungování CTR módu snadno vidíme, že pokud je $b = 0$, prvních $l - 1$ bloků m' bude nulových, jelikož

$$m'_i \oplus F_k(IV + 1 + i) = c_{i+1} = m_{b(i+1)} \oplus F_k(IV + i + 1)$$

pro $i \in \{1, \dots, l - 1\}$. Pokud je naopak (IV, c) ciphertextem m_1, stejným argumentem bude prvních $l - 1$ bloků m' zaplněno jedničkami. Sestrojili jsme tedy adversaryho úspěšného v CCA experimentu s pravděpodobností 1, tudíž CTR mód není CCA-secure.

OFB mód

Mějme zprávy a ciphertext stejně jako v předchozím případě. Po obdržení challenge ciphertextu se dotážeme dešifrovacího orákula na ciphertext (IV, c'), kde $c' = c_1 c_2 \dots c_{l-1} d$ pro nějaké $d \neq c_l$ a obdržíme zprávu m'. Jelikož šifrování a dešifrování zprávy v OFB módu můžeme zapsat jako

$$c_i = m_i \oplus F_k(F_k(\cdots F_k(IV)))$$
$$m_i = c_i \oplus F_k(F_k(\cdots F_k(IV))),$$

kde funkce F_k je do sebe i-krát vnořená, vidíme, že hodnota (de)šifrovaného bloku není závislá na hodnotách ostatních bloků. Jelikož se navíc prvních $l - 1$ bloků c' a c shodují (a používají stejnou IV), vyplývá z toho, že prvních $l - 1$ bloků m' se bude shodovat s prvními $l - 1$ bloky m_b, čímž snadno určíme, která zpráva byla šifrována. Ani OFB mód tedy není CCA-secure.

CBC mód

Mějme zprávy a ciphertext jako v předchozích případech. Zeptáme se dešifrovacího orákula na ciphertext (IV, c'), kde $c' = c_1 c_2 \dots c_{l-1} d$ pro nějaké $d \neq c_l$ a obdržíme zprávu m'. Protože dešifrování je definováno jako

$$m_i = F_k^{-1}(c_i) \oplus c_{i-1},$$

vidíme, že hodnota i-tého bloku dešifrované zprávy závisí pouze na c_i a c_{i-1}, popř. IV pro první blok. Tyto hodnoty jsou pro prvních $l - 1$ bloků c' a c shodné, tudíž i prvních $l - 1$ bloků m' a m_b musí být shodných. Z toho snadno identifikujeme b a dokážeme tak, že CBC mód není CCA-secure.