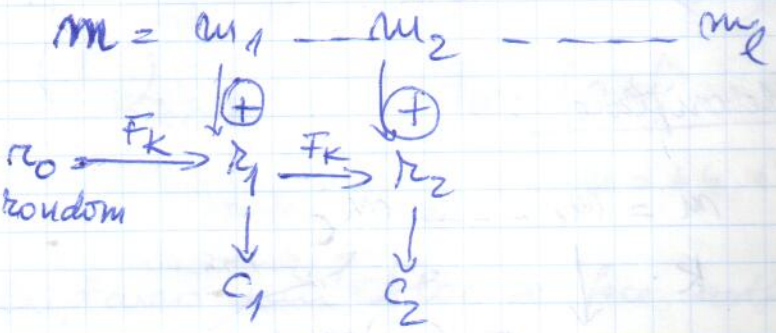
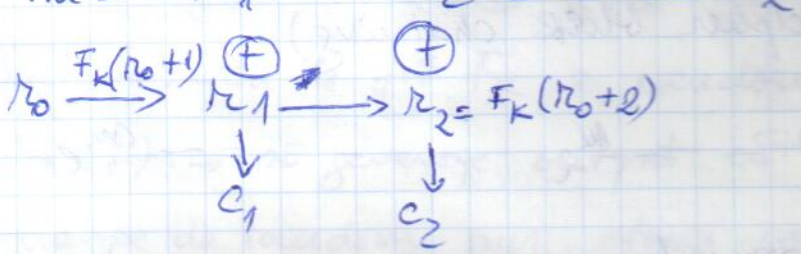
OFB - (output feedback)



$c_i = m_i \oplus F_K^i(r_0)$ funcționează ca un criptosistem oarecare.

CPA dacă r_0 = random. Metoda de initializare = random

CTR (counter).



$c_i = m_i \oplus F_K(r_0 + i)$

r_0 = random, F_K = pseudorandom $\Rightarrow$ metoda e CPA dacă.

$\Rightarrow$ avem acces direct la blocul de criptotext pt că nu depinde un bloc de blocuri de anterioare.

- CTR = teoretic mai eficientă decât CBC și OFB.