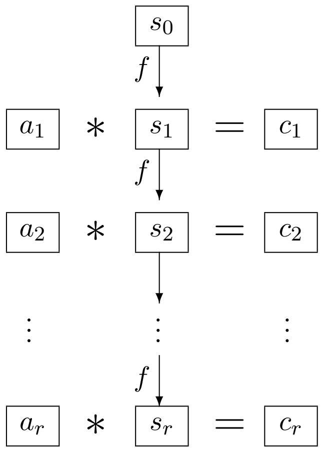
3.5 OFB = Output Feedback

Description (of the simplest version)



This mode also was originally defined as shift register version. Here too using a blocklength of $t < n$ weakens the security [Jueneman, Crypto 82].

Encryption in OFB mode is by the formula

$$c_i := a_i * s_i, \quad s_i := f(s_{i-1}) \quad \text{for } i = 1, \ldots, r.$$

Decryption by the formula

$$a_i = c_i * s_i^{-1}, \quad s_i := f(s_{i-1}) \quad \text{for } i = 1, \ldots, r.$$

Properties

- There is no diffusion. However identical plaintext blocks in general yield different ciphertext blocks.
- In the case $\Sigma = \mathbb{F}_2^s$ OFB simply is a bitstream cipher where f serves as "random generator".
- If encryption or decryption is time critical, the sender or the receiver (or both) might precalculate the "key stream" s_i.
- Here too the decryption uses only f, not f^{-1}.
- For $\Sigma = \mathbb{F}_2^s$ the cipher is an involution, that is encryption and decryption are the same function. More generally this holds when the group Σ has exponent 2.

- Under an attack with known plaintext the pair (a_1, c_1) reveals the value of s_1, the next pair (a_2, c_2), the value of $s_2 = f(s_1)$. This leads to an attack with known plaintext against the function f itself.
- Keeping the initialization vector s_0 secret doesn't increase the security of the cipher for OFB (like for the other modes).

Variant: Counter Mode CTR

The simplest case is

$$c_i := a_i * f(i) \quad \text{for } i = 1, \ldots, r.$$

There are same slight variants, for example starting with another number than 1.