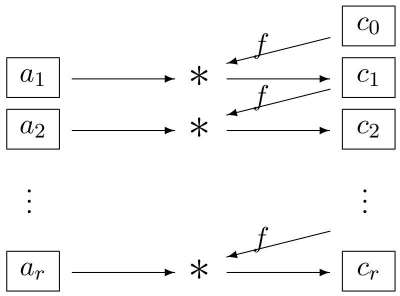
3.4 CFB = Cipher Feedback

Description (of the simplest version)



Encryption in CFB mode is by the formula

$$\begin{aligned} c_i &:= a_i * f(c_{i-1}) \quad \text{for } i = 1, \ldots, r \\ &= a_i * f(a_{i-1} * f(\cdots a_1 * f(c_0) \ldots)). \end{aligned}$$

Decryption: $a_i = c_i * f(c_{i-1})^{-1}$ for $i = 1, \ldots, r$.

Properties

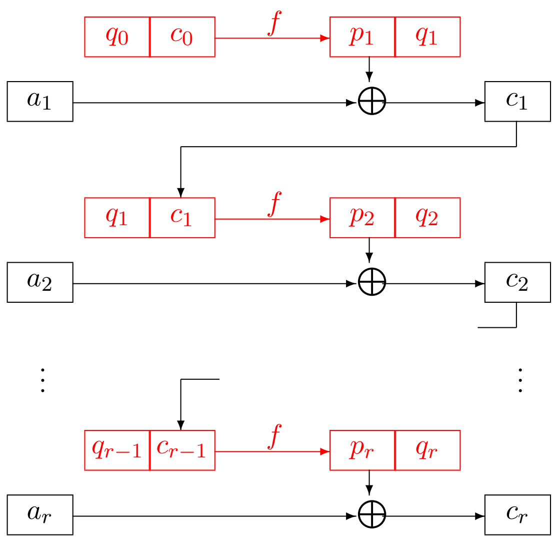
- As before the initialization vector is unsuited as additional key component.
- As before this mode doesn't make an attack with known plaintext more difficult.
- Note that also decryption uses f, not f^{-1}. Therefore:
  - CFB mode doesn't make sense for asymmetric ciphers.
  - On the other hand CFB mode may be used with a (key dependent) one-way or hash function f.
- For the identical map $f = \mathbf{1}_\Sigma$ CFB again reduces to ciphertext autokey.
- (David Wagner) ECB ∘ CFB = CBC:

For a proof take c_0 as initialization vector for CFB, and $c_0' := f(c_0)$ as initialization vector for CBC. Then

$$\begin{aligned} c_1 &= \text{CFB}(a_1) = a_1 * f(c_0), \\ c_1' &= \text{ECB}(c_1) = f(a_1 * f(c_0)) = f(a_1 * c_0') = \text{CBC}(a_1), \\ c_2 &= \text{CFB}(a_2) = a_2 * f(c_1), \\ c_2' &= \text{ECB}(c_2) = f(a_2 * f(c_1)) = f(a_2 * c_1') = \text{CBC}(a_2), \\ &\text{etc.} \end{aligned}$$

The Standardized Version

...uses a shift register, hence is defined only in the case of $\Sigma = \mathbb{F}_2^n$. Here $1 \leq t \leq n$, and the encryption procedure uses blocks $a_i \in \mathbb{F}_2^t$ of length t. The current ciphertext block c_i of length t is shifted from the right into the shift register (drawn in red):



The q_i are bitblocks of length $n - t$.

As it turned out later the security of this more general version decreases with t. Therefore its use is not recommended.