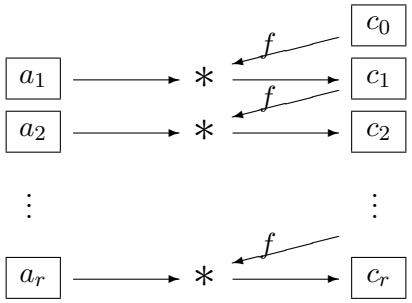
3.4 CFB = Cipher Feedback

Beschreibung (in der einfachsten Version)



Verschlüsselung: Beim CFB-Modus wird nach folgender Formel verschlüsselt:

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

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

Eigenschaften

- Der Startwert taugt auch hier nicht als zusätzlicher Schlüssel.
- Ein Angriff mit bekanntem Klartext wird auch durch diese Betriebsart nicht erschwert.
- Bemerkenswert ist, dass man auch zum Entschlüsseln nur f braucht, nicht etwa f^{-1}. Im Vorgriff sei hier schon vermerkt:
  - Der CFB-Modus ist für asymmetrische Chiffren ungeeignet.
  - Er kann aber mit einer echten (natürlich schlüsselabhängigen) Einweg- oder Hash-Funktion verwendet werden.
- Der CFB reduziert sich im Falle der identischen Abbildung $f = \mathbf{1}_\Sigma$ ebenfalls auf das Geheimtext-Autokey-Verfahren.
- (David Wagner) ECB $\circ$ CFB = CBC:

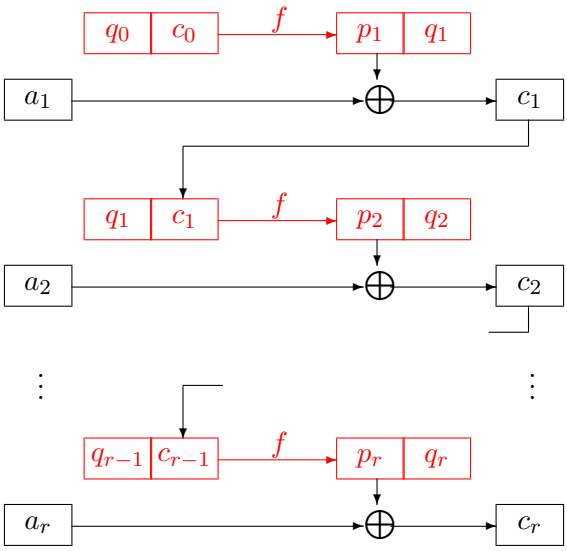
Dazu setzt man c_0 als Startwert für CFB und $c_0' := f(c_0)$ als Startwert für

CBC. Dann ist

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

Die genormte Version

... verwendet ein Schieberegister und ist daher nur im Falle $\Sigma = \mathbb{F}_2^n$ definiert. Hier ist $1 \leq t \leq n$, und verschlüsselt werden Blöcke $a_i \in \mathbb{F}_2^t$ der Länge t; der aktuelle Geheimtextblock c_i der Länge t wird von rechts in das (hier rot dargestellte) Schieberegister nachgeschoben:



Die q_i sind dabei stets Bitblöcke der Länge $n - t$.

Diese allgemeinere Version ist weniger sicher als die mit $t = n$ und wird daher kaum verwendet.