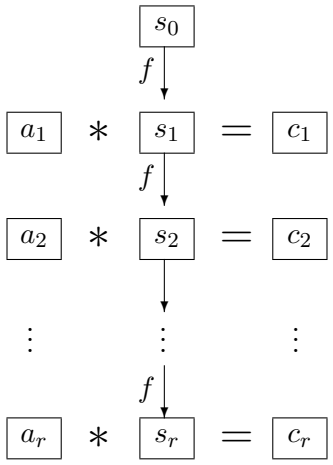
3.5 OFB = Output Feedback

Beschreibung (in der einfachsten Version)



Auch diese Betriebsart war ursprünglich als Schieberegister-Version definiert; auch hier bedeutet die Verwendung eines $t <$ Blocklänge n eine Schwächung des Verfahrens [Jueneman, Crypto 82].

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

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

Entschlüsselung: nach der Formel

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

Eigenschaften

- Es gibt keine Diffusion, aber gleiche Klartextblöcke werden im allgemeinen verschieden verschlüsselt.
- Im Falle $\Sigma = \mathbb{F}_2^s$ handelt es sich um eine Bitstrom-Chiffre mit f als „Zufallsgenerator“.
- Wird eine besonders schnelle Ver- und Entschlüsselung benötigt, so kann man den „Schlüsselstrom“ s_i auf beiden Seiten (beim Sender und beim Empfänger) vorausberechnen.
- Auch hier wird zum Entschlüsseln nur f benötigt, nicht f^{-1}.
- Falls $\Sigma = \mathbb{F}_2^s$, ist die Chiffre sogar involutorisch, d. h., Verschlüsselung = Entschlüsselung (als Funktion). Allgemeiner gilt das, wenn Σ eine Gruppe vom Exponenten 2 ist.

- Bei einem Angriff mit bekanntem Klartext liefert ein Paar (a_1, c_1) den Wert s_1, ein weiteres Paar (a_2, c_2) den Wert $f(s_1)$. Damit ist also ein Angriff mit bekanntem Klartext auf f selbst möglich.
- Das Geheimhalten des Startwerts s_0 bringt also auch hier praktisch keine zusätzliche Sicherheit.

Variante: Der Counter-Mode CTR

Hier ist im einfachsten Fall

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