3.6 Nichtlinearität für Schieberegister – Ansätze

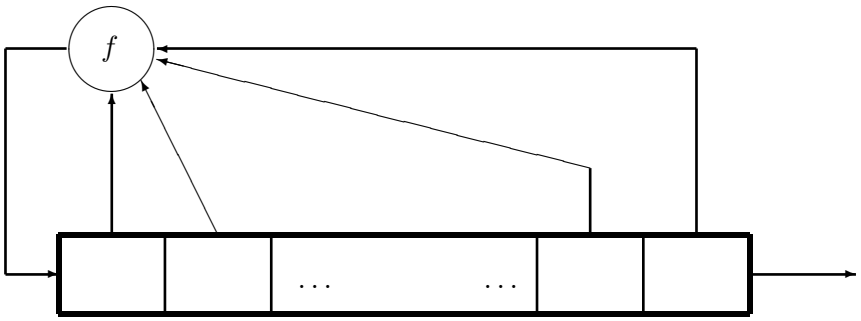
Lineare Schieberegister sind beliebt – vor allem bei Elektro-Ingenieuren und beim Militär – denn sie sind

- sehr einfach zu realisieren,
- extrem effizient, vor allem in Hardware,
- als Zufallsgeneratoren für statistische Zwecke sehr gut geeignet,
- problemlos parallel zu betreiben,
- aber leider kryptologisch völlig unsicher.

Um die positiven Eigenschaften zu nutzen und die kryptologische Schwäche zu vermeiden, gibt es verschiedene Ansätze.

Ansatz 1: Nichtlineare Rückkopplung

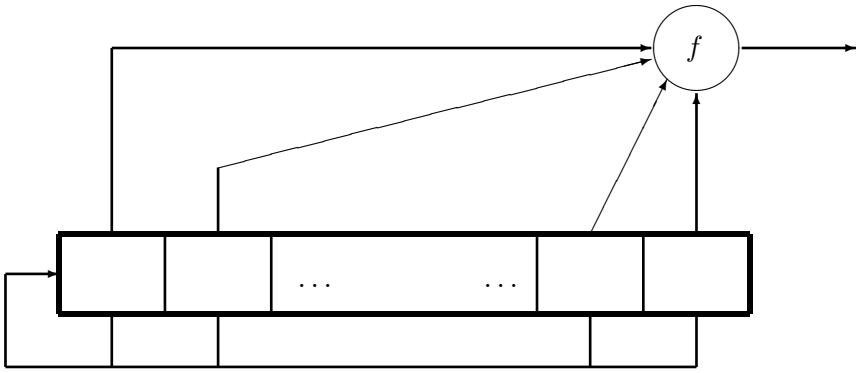
Die nichtlineare Rückkopplung (nonlinear feedback) folgt dem Schema:



Sie wurde schon in Abschnitt 2.6 behandelt und dort als kryptographisch nicht hinreichend sicher eingestuft.

Ansatz 2: Nichtlinearer Ausgabefilter

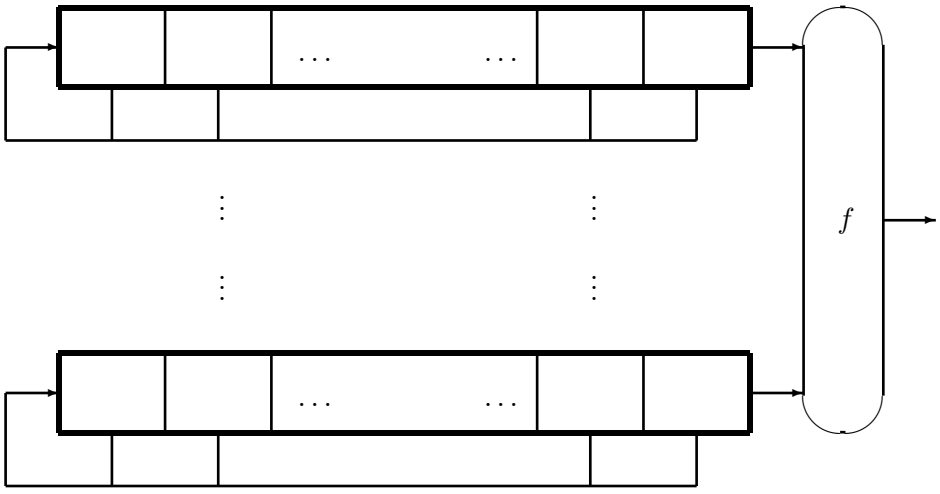
Der nichtlineare Ausgabefilter (nonlinear feed forward) folgt dem Schema:



Das Schieberegister selbst ist linear. Der nichtlineare Ausgabefilter ist ein Spezialfall des nächsten Ansatzes. (**Übungsaufgabe:** Wie?)

Ansatz 3: Nichtlinearer Kombinierer

Hier wird eine „Batterie“ aus n linearen Schieberegistern – die durchaus unterschiedliche Länge haben können und sollen – parallel betrieben. Ihre Outputfolgen werden in eine BOOLEsche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gefüttert:



Die ausführliche Diskussion dieses Verfahrens folgt in Abschnitt 3.7 ff. Natürlich kann man auch allgemeiner eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ verwenden, die in jedem Takt q Bits ausgibt.

Ansatz 4: Auswahlsteuerung/Dezimierung/Taktung

Weitere Möglichkeiten bestehen in verschiedenen Ansätzen zur Steuerung einer Batterie von n parallel betriebenen linearen Schieberegistern

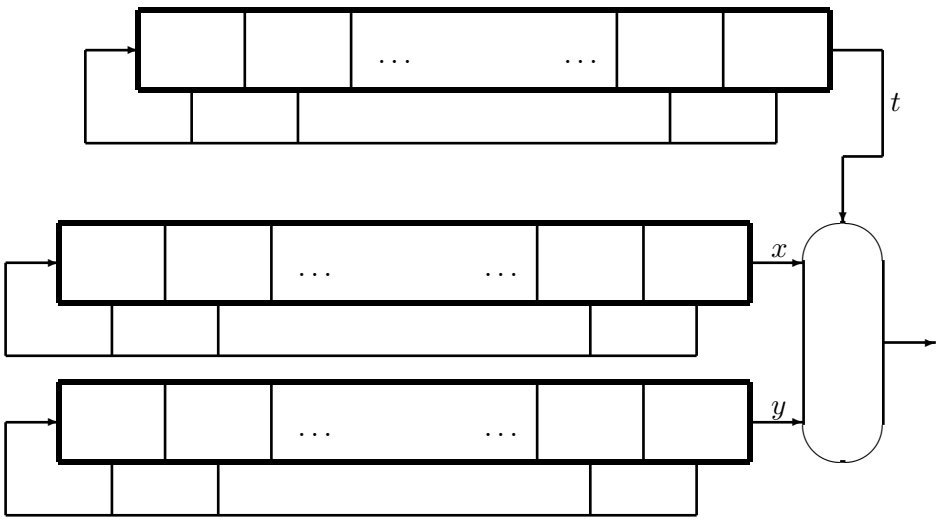
durch ein weiteres lineares Schieberegister:

- Bei der **Auswahlsteuerung** wird je nach Zustand des „Hilfsregisters“ das aktuelle Output-Bit von genau einem der „Batterie-Register“ als Output des Zufallsgenerators ausgewählt. Allgemeiner kann man auch eine Auswahl „r aus n“ treffen.
- Bei der **Dezimierung** nimmt man im allgemeinen $n = 1$ an und gibt das Output-Bit des einen Batterie-Registers nur dann aus, wenn das Hilfsregister einen bestimmten Zustand hat. Diese Art der Dezimierung kann man natürlich analog auf jede Bitfolge anwenden.
- Bei der **Taktung** gibt der Zustand des Hilfsregisters an, welche der Batterie-Register im aktuellen Taktzyklus weitergeschoben werden (und um wieviele Positionen) und welche in ihrem momentanen Zustand bleiben. Das ist vergleichbar mit der Steuerlogik von Rotor-Maschinen.

Diese Ansätze lassen sich oft bequem auch als nichtlineare Kombinierer schreiben, so dass Ansatz 3 als *der* Ansatz zur Rettung der linearen Schieberegister angesehen werden kann.

Beispiel: Der Geffe-Generator

Das einfachste Beispiel für die Auswahlsteuerung ist der Geffe-Generator, der durch das folgende Schema beschrieben wird:



Die Ausgabe ist x, wenn $t = 0$, und y, wenn $t = 1$. Das kann man so als Formel ausdrücken:

$$\begin{aligned} u &= \begin{cases} x, & \text{wenn } t = 0, \\ y, & \text{wenn } t = 1 \end{cases} \\ &= (1-t)x + ty = x + tx + ty. \end{aligned}$$

Also lässt sich der GEFFE-Generator auch durch einen nichtlinearen Kombinierer mit einer BOOLEschen Funktion $f\colon \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ vom Grad 2 beschreiben.