1.6 Lineare Schieberegister

Neben den bisher behandelten linearen Kongruenzgeneratoren gibt es eine andere klassische und weitverbreitete Methode zur Erzeugung von Pseudozufallsfolgen: die Schieberegister-Methode. Diese Methode wurde von GOLOMB 1955 erstmals vorgeschlagen, wird aber meist nach TAUSWORTHE benannt, der die Idee 1965 in einer Arbeit aufgriff. Sie ist besonders leicht in Hardware zu realisieren. Für die theoretische Beschreibung fasst man Blöcke von jeweils l Bits als Elemente des Vektorraums $\mathbb{F}_2^l$ über dem Körper $\mathbb{F}_2$ aus zwei Elementen auf.

Eine lineare Abbildung

$$A\colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2$$

ist nichts anderes als eine Vorschrift, aus einem l-Bit-Block eine Teilsumme zu bilden:

$$Au = \sum_{i=1}^{l} a_i u_i,$$

wobei alle Koeffizienten a_i ja 0 oder 1 sind. Als potentielle Zufallsfolge wird die Folge von Bits betrachtet, die nach der Vorschrift

$$u_n = a_1 u_{n-1} + \cdots + a_l u_{n-l}$$

entsteht. Man braucht als Parameter des Verfahrens

- die **Registerlänge** l mit $l \geq 2$,
- eine **Rückkopplungsvorschrift** A, die eine Folge $(a_1, \ldots, a_l) \in \mathbb{F}_2^l$ ist, und daher auch durch eine Teilmenge $I \subseteq \{1, \ldots, l\}$ beschríeben werden kann.
- einen **Startwert** $u = (u_{l-1} \ldots u_0)$ aus l Bits.

Die Iterationsformal lässt sich damit auch in der Form

$$u_n = \sum_{j \in I} u_{n-j}$$

schreiben.

Die Hardware-Realisierung stellt man sich so vor, daß das rechte Bit des Schieberegisters ausgegeben wird, die übrigen $l - 1$ Bits nach rechts nachrücken und auf der linken Seite als „Rückkopplung“ die Summe der durch I angegebenen Bits nachgeschoben wird, siehe Abbildung 2.

Bei der Anwendung für die Bitstrom-Verschlüsselung wird der Startwert u oder aber alle drei Parameter l, I, u als Schlüssel betrachtet, d. h., geheim gehalten.

Bei geschickter Wahl der Parameter, die hier nicht weiter behandelt wird, hat die Folge eine Periode nahe 2^l und ist durch statistische Tests praktisch nicht von einer gleichverteilten Zufallsfolge zu unterscheiden.

Abbildung 2: Ein lineares Schieberegister