2.6 Nichtlineare Schieberegister

Als weiteres Beispiel für die allgemeine Vorhersagemethode werden hier beliebige, nicht notwendig lineare, Schieberegister behandelt. Ein solches wird durch Abbildung 5 beschrieben.

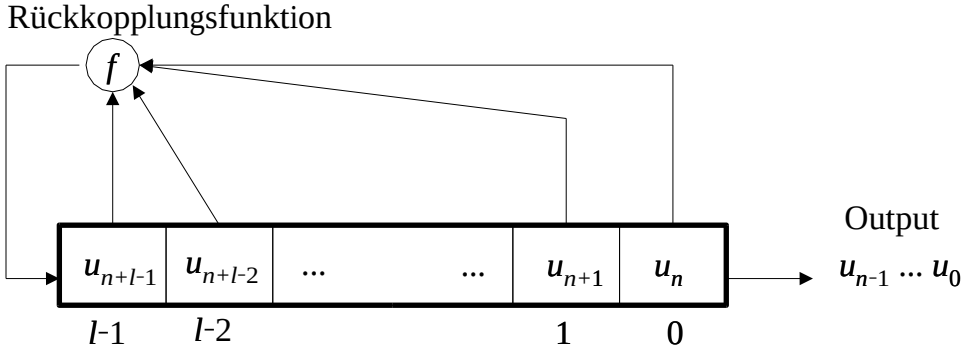

Abbildung 5: Ein Schieberegister der Länge l

Hierbei ist die Rückkopplungsfunktion $f : \mathbb{F}_2^l \longrightarrow \mathbb{F}_2$ eine beliebige Boolesche Funktion und lässt sich in algebraischer Normalform als Polynom

$$f(y_1, \dots, y_l) = \sum_{I \subseteq \{1,\dots,l\}} a_I y^I \qquad \text{mit } y^I = \prod_{j \in I} y_j$$

schreiben.

Die Funktion f ist genau dann effizient (etwa durch ein Boolesches Schaltnetz) berechenbar, wenn „fast alle“ Koeffizienten $a_I = 0$ sind; d. h., es gibt ein Polynom $p \in \mathbb{N}[X]$ mit

$$\#\{I \mid a_I \neq 0\} \leq p(l).$$

Es ist dem Kryptoanalytiker allerdings nicht bekannt, welche $a_I \neq 0$ sind – vielmehr ist es eins seiner Ziele, das herauszubekommen.

Für die Anwendung der Vorhersagemethode wird $R = X = \mathbb{F}_2$, $h = l$, $Z = \mathbb{F}_2^{2^l}$ gesetzt. Für $i \geq l$ ist

$$\Phi^{(i)} : \mathbb{F}_2^i \longrightarrow Z$$

gegeben durch

$$z_i := \Phi^{(i)}(x_1, \dots, x_i) = (y^I)_{I \subseteq \{1,\dots,l\}} \qquad \text{mit } y = (x_{i-l+1}, \dots, x_i).$$

Und schließlich ist

$$\alpha : Z \longrightarrow X, \quad \alpha((t_I)_{I \subseteq \{1,\dots,l\}}) = \sum a_I t_I.$$

Zunächst zwei konkrete Beispiele für die Vorhersage:

Beispiele

1. $l = 2$, $f = T_1T_2 + T_1$. Aus den Startwerten $u_0 = 1$, $u_1 = 0$ wird die Folge

$$u_0 = 1,\ u_1 = 0,\ u_2 = 1,\ u_3 = 0,\ \ldots$$

erzeugt (die offensichtlich die Periode 2 hat). Es ist

$$Z = \mathbb{F}_2^4, \qquad z_n = \begin{pmatrix} u_{n-1}u_{n-2} \\ u_{n-1} \\ u_{n-2} \\ 1 \end{pmatrix},$$

$$z_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad z_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad z_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = z_2, \quad \ldots$$

Also erkenntt der Kryptoanalytiker die lineare Rekursion

$$z_n = z_{n-2} = 0 \cdot z_{n-1} + 1 \cdot z_{n-2} \quad \text{für } n \geq 4,$$

ist sogar sicher, da er die Periode erkannt hat, und sagt korrekt voraus

$$u_n = 0 \cdot u_{n-1} + 1 \cdot u_{n-2} = u_{n-2} \quad \text{für } n \geq 4.$$

Die Folge kann also auch durch ein *lineares* Schieberegister der Länge 2 erzeugt werden. Benötigt wurden u_0 bis u_3.

2. $l = 3$, $f = T_1T_3 + T_2$. Aus den Startwerten $u_0 = 0$, $u_1 = 1$, $u_2 = 1$ wird die weitere Folge

$$u_3 = 1,\ u_4 = 0,\ u_5 = 1,\ u_6 = 1,\ u_7 = 1,\ u_8 = 0,\ u_9 = 1,\ \ldots$$

erzeugt. Es ist

$$Z = \mathbb{F}_2^8, \qquad z_n = \begin{pmatrix} u_{n-1}u_{n-2}u_{n-3} \\ u_{n-1}u_{n-2} \\ u_{n-1}u_{n-3} \\ u_{n-2}u_{n-3} \\ u_{n-1} \\ u_{n-2} \\ u_{n-3} \\ 1 \end{pmatrix},$$

$$z_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad z_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad z_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad z_6 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad z_7 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = z_3, \quad \ldots$$

Also ist die vermutete – wegen der Peiodizität sogar sichere – lineare Rekursion hier

$$z_n = z_{n-4} \quad \text{für } n \geq 4,$$
$$u_n = u_{n-4} \quad \text{für } n \geq 4,$$

und auch das ist wieder korrekt. Benötigt wurden u_0 bis u_6; und gefunden wurde ein „äquivalentes“ lineares Schieberegister der Länge 4.

Wegen der exponentiellen Zunahme der Dimension von Z sieht es zunächst so aus, als ob das Vorhersageverfahren bald an seine Grenzen stößt; der stationäre Zustand der aufsteigenden Unterräume, d. h., die gesuchte lineare Relation, wird womöglich erst nach 2^l Schritten erreicht. Immerhin ist dabei noch ein Schieberegister der Länge 32 mit linearer Algebra im 2^{32}-dimensionalen binären Vektorraum mit realistischem Aufwand vorhersagbar.

Im allgemeinen Fall kommt aber ein anderer Gesichtspunkt zum Tragen: Die Rückkopplungsfunktion f hängt ja von 2^l Parametern ab. Um zu einem handhabbaren Schlüsselraum zu kommen, muss man die möglichen Koeffizienten $\neq 0$ – d. h., die Größe eines beschreibenden Schaltnetzes – *von vorneherein* auf eine handhabbare Anzahl beschränken. Diese Auswahl ist aber Teil des Algorithmus – etwa des in Hardware realisierten Schieberegisters – und nicht Bestandteil des Schlüssels, wird also nach dem KERCKHOFFS-Prinzip früher oder später dem Gegner bekannt sein. Die Notwendigkeit, eine effizient berechenbare Rückkopplungsfunktion zu wählen, führt also dazu, dass die Vorhersagemethode ebenfalls effizient wird. Daher kann man sagen:

Satz 6 *Jede durch ein Schieberegister mit effizient berechenbarer Rückkopplungsfunktion erzeugte Bitfolge ist vorhersagbar.*

Die obige Diskussion war sehr grob. Für mathematisch korrekte Aussagen gibt es zwei Möglichkeiten:

1. Entweder man schätzt die Schaltnetzkomplexität des Vorhersage-Algorithmus direkt durch die Schaltnetzkomplexität der Rückkopplungsfunktion ab.

2. Oder man behandelt Familien von BOOLEschen Funktionen – als Beschreibung von Familien von Schieberegistern – deren Komplexität polynomial mit der Registerlänge wächst, und zeigt, dass die zugehörigen Vorhersage-Algorithmen ebenfalls nur polynomial anwachsen.

Schieberegister, ob linear oder nichtlinear, sind jedenfalls zur Erzeugung kryptographisch brauchbarer Zufallsfolgen nicht geeignet – jedenfalls nicht bei direkter Verwendung. Das bedeutet nicht, dass das Verfahren von BOYAR/KRAWCZYK eine Erfolgsgarantie für den Kryptoanalytiker liefert; allerdings kann der Kryptograph sich auch mit nichtlinearen Schieberegistern nicht sicher fühlen.