3.7 Nichtlineare Kombinierer

Ein nichtlinearer Kombinierer wird beschrieben durch eine BOOLEsche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ sowie eine Batterie aus n linearen Schieberegistern der Längen $l_1, \ldots, l_n$.

Bemerkungen

1. Sind die Schieberegister und f bekannt, so besteht ein Schlüssel der zugehörigen Bitstrom-Chiffre aus dem n-Tupel der Startvektoren, also hat der Schlüsselraum die Größe $2^{l_1} \cdots 2^{l_n}$.

2. Die lineare Komplexität der erzeugten Bitfolge ist „im allgemeinen“ $f(l_1, \ldots, l_n)$, wobei f in algebraischer Normalform geschrieben und als Polynom $f \in \mathbb{Z}[X]$ ausgewertet wird. Insbesondere ist ein möglichst hoher Grad von f erstrebenswert.

Beispiele

1. Der GEFFE-Generator ließ sich als nichtlinearer Kombinierer mit $f(x, t, y) = x + tx + ty$ deuten. Er hat die sehr große Periode $(2^{l_1} - 1)(2^{l_2} - 1)(2^{l_3} - 1)$, einen Schlüsselraum der Größe $2^{l_1+l_2+l_3}$, sowie die recht beachtliche lineare Komplexität $l_1 + l_1 l_2 + l_2 l_3$.

2. Nimmt man bei n beliebigen „Batterie-Registern“ als Kombinier-Funktion $f = T_1 \cdots T_n \in \mathbb{F}_2[T]$, also einfach die Multiplikation in $\mathbb{F}_2$, so hat die erzeugte Folge die lineare Komplexität $\leq l_1 \cdots l_n = f(l_1, \ldots, l_n)$. Hinreichend für die Gleichheit ist:

   (a) Alle charakteristischen Polynome der Batterie-Register sind irreduzibel,

   (b) die Längen $l_1, \ldots, l_n$ sind paarweise teilerfremd.