Kryptologie, SS03 Aufgabenblatt 7

Eine lineare Schieberegisterfolge im Körper K sei gegeben durch das Rückkopplungsregister $(a_{n-1},\ldots,a_0)\in K^n$, den Startvektor $(x_{n-1},\ldots,x_0)\in K^n$ und die rekursive Definition $x_k := \sum_{i=0}^{n-1} a_i x_{k+i-n},\ k \geq n$. Die Abbildung $(x_{n-1},\ldots,x_0)\xrightarrow{\varphi}(x_n,\ldots,x_1)$ ist linear. Bezüglich der Basis $e_0=(0,\ldots,0,1),\ldots,e_{n-1}=(1,0,\ldots,0)$ wird sie offenbar dargestellt durch die Matrix

$$A=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 1 \\ a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix}$$

Setzen wir nun $\xi_0 := (x_{n-1},\ldots,x_0)$, $\xi_{k+1} := A\xi_k = (x_{k+n},\ldots,x_{k+1})$, so finden wir die Schieberegisterfolge (x_n) als jeweils niedrigstwertiges Bit in der Vektorfolge (ξ_n) wieder. Mit der Vektorfolge wird auch die Schieberegisterfolge periodisch und die Periode ist maximal, wenn in der Vektorfolge alle von Null verschiedenen Vektoren von K^n vorkommen. Mit $|K|=q$ ist daher q^n-1 die maximale Periode.

Aufgabe 1

a) Zeigen Sie, daß für das charakteristische Polynom gilt $\chi_A(t)=\det(tE-A)=t^n-\sum_{i=0}^{n-1} a_i t^i$.

(Hinweis: Induktion und Entwicklung nach der letzten Spalte.)

Ein linearer Teilraum $U \subset K^n$ heißt invariant unter *A*, wenn $AU \subset U$, d.h. $\forall x\in U: Ax\in U$. Wenn ein echter unter *A* invarianter linearer Teilraum *U* existiert, also $\{0\} \neq U \neq K^n$, so kann die Periode der Schieberegisterfolge nicht maximal sein, denn tritt die Folge (ξ_n) erst einmal in den Unterraum *U* ein, so kann sie diesen nicht mehr verlassen. Man kann eine Basis $v_1,\ldots,v_k$ des invarianten Unterraums zu einer Basis $v_1,\ldots,v_n$ des Gesamtraums ergänzen. Die Invarianz von *U* bedeutet dann gerade, daß die Matrixdarstellung von φ bezüglich dieser Basisaufteilung die Form $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$ besitzt, wobei *B* quadratisch und k-spaltig und *D* quadratisch und (n-k)-spaltig ist. Einerseits ist nun das charakteristische Polynom einer linearen Abbildung unabhängig von der Basis, bezüglich der man die zugehörige Matrix ausrechnet. Andererseits folgt aus der eben abgeleiteten Form der Matrixdarstellung, daß $\chi_A(t)=\chi_B(t)\chi_D(t)$. Daher ist das charakteristische Polynom nicht irreduzibel, wenn es einen echten invarianten Unterraum gibt. Also muß $t^n-\sum_{i=0}^{n-1} a_i t^i$ irreduzibel sein, wenn die Schieberegisterfolge maximale Periode haben soll.

Betrachten wir nun den durch Restebildung modulo χ_A gebildeten Körper

$E = K[X] \Big/ (X^n - \sum_{i=0}^{n-1} a_i X^i)$, dessen Elemente wir als Polynome vom Grad < n auffassen.

E bildet auch in natürlicher Weise einen n-dimensionalen Vektorraum über K mit der Basis $1, X, \ldots, X^{n-1}$. Die Abbildung $E \to E,\ f \to X \cdot f$ ist zweifellos linear und besitzt bezüglich dieser Basis von E offenbar die Matrixdarstellung

$$B := \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & 0 & 1 & 0 & a_{n-2} \\ 0 & 0 & 0 & 1 & a_{n-1} \end{pmatrix} = A^t$$

(In der letzten Spalte stehen ja die Koeffizienten von X^n und dieses ist modulo $X^n - \sum_{i=0}^{n-1} a_i X^i$ offenbar gleich $\sum_{i=0}^{n-1} a_i X^i$. Die Multiplikation mit X ist also „dual“ zu der vorher betrachteten Schieberegisterabbildung.

Wenn die Periode der Folge $X \to X^2 = A^t X \to X^3 = \left(A^t\right)^2 X \to \ldots$ maximal ist, darin also alle Elemente von E^* vorkommen, so heißt dies definitionsgemäß, daß das Polynom $X^n - \sum_{i=0}^{n-1} a_i X^i$ primitiv ist. Andererseits geht es primär nicht um diese Folge, sondern um die Folge $\xi_0 \to \xi_1 = A\xi_0 \to \xi_2 = A\xi_1 = A^2\xi_0 \to \ldots$, für deren maximale Periodizität wir eine hinreichende Bedingung suchen. Also versuche man die folgende Vermutung zu beweisen:

b)* Die Folge $\xi_0 \to A\xi_0 \to A^2\xi_1 \to \ldots$ hat die maximale Periode $q^n - 1$, wenn χ_A primitiv ist. (Hinweis: Ist B eine quadratische Matrix, so ist $\chi_B = \chi_{B^t}$.)

Wir haben in einem früheren Aufgabenblatt geübt, wie man die Primitivität eines Polynoms effektiv feststellt. Damit sind wir in der Lage, Schieberegisterfolgen maximaler Länge zu konstruieren. Jedoch wollen wir uns jetzt nicht noch einmal diese Mühe machen, sondern:

c) Mittels einer Suchmaschine finde man im Internet Hinweise auf primitive Polynome entsprechender Grade und gebe damit Rückkopplungskoeffizienten für lineare Schieberegisterfolgen maximaler Länge über $\mathbb{Z}_2$ mit Registerlängen 8, 16, 32, 64, 128, 256, 512, 1024 an. Dokumentieren Sie alle Schritte zur Erlangung der Information.

d) Sie beobachten folgenden Output einer linearen Schieberegisterfolge: 0001101000110100. Sie wissen, daß es sich um eine Folge über $\mathbb{Z}_2$ mit Registerlänge 8 handelt. Berechnen Sie die nächsten 8 Folgenglieder! (Hinweis: Berechnen Sie zunächst die Rückkopplungskoeffizienten. Benutzen Sie Pari zur Lösung der entsprechenden linearen Gleichungssysteme.)

Aufgabe 2.

Beschaffen Sie sich aus dem Internet eine Implementierung des DES-Algorithmus. Benutzen Sie den hex-codierten Schlüssel `3A4B5C6D7E2F1958`, um folgenden hex-codierten Bytestring zu dechiffrieren:

```
8d a3 90 e8 11 6e ab b0 82 db 60 76 91 81 16 81 f2 1d aa 57 10 a3 f2 30
dd c3 95 eb 93 53 bb 24 86 64 d5 4f 01 54 ef 0b 0e 6d a2 a4 6c 0e 35 39
```

(Man braucht also zunächst ein Utility, um einen Hex-String in den enstprechenden Bytestring zu konvertieren und achte darauf, daß das Dechiffrierprogramm den Schlüssel hex-codiert übernehmen kann.)

Dokumentieren Sie alle Schritte, beginnend mit der Beschaffung und ggf. Codierung und Kompilierung der notwendigen Software