POLYNOME UND POLYNOMFUNKTIONEN IN DER KRYPROGRAPHIE

Winfried B. Müller
Institut für Mathematik
Universität Klagenfurt

1. Konstruktion und Verwaltung elektronischer Schlüssel mittels der Polynominterpolation (A.Shamir (1979))

Ein Betrieb hat das folgende Problem: Er möchte n Teilschlüssel K_i $(1 \leq i \leq n)$ zu einem elektronischen Schloß ausgeben. Jede Teilmenge von $k(\leq n)$ Teilschlüsseln soll das Schloß öffnen. Weniger als k Teilschlüssel sollen ein Aufsperren nicht gestatten (bzw. nicht in absehbarer Zeit gestatten).

Die Lösung dieses Problems erfolgt mittels der Interpolation nach Lagrange. Ist K der Generalschlüssel, welcher das Schloß sperrt (in der Praxis eine natürliche Zahl), so wählt man ein primes $p > K$ und $p > n$ und ein zufälliges Polynom vom Grad k-1

$$g(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} \mod p$$

über den ganzen Zahlen mit $a_0 = K$. Es gilt dann also $g(0) = K$. Die Teilschlüssel K_i, $i=1,2,\ldots,n$, werden nun aus $g(x_i) = K_i$ berechnet. Damit ist jedes Paar (x_i, K_i) ein Punkt auf $y = g(x)$. Da je k Punkte eindeutig ein Polynom vom Grad k-1 bestimmen, kann g(x) und damit auch $K = g(0)$ aus je k Einzelschlüsseln berechnet werden. Aus weniger als k Teilschlüsseln ist dies bei genügend großem p in absehbarer Zeit jedoch nicht möglich. Sind z.B. $K_{i_1}, \ldots, K_{i_k}$ gegeben, so erhält man g(x) nach Lagrange als

$$g(x) = \sum_{s=1}^{k} K_{i_s} \prod_{\substack{j=1 \\ j \neq s}}^{k} \frac{(x - x_j)}{(x_i - x_j)} \mod p \ .$$

Beispiel: $k=3$, $n=5$, $p=17$, $K=13$

Wir wählen zufällig $g(x) = 2x^2 + 10x + 13 \mod 17$.

$K_1 = g(1) = 2 + 10 + 13 \mod 17 = 25 \mod 17 = 8$

$K_2 = g(2) = 8 + 20 + 13 \mod 17 = 41 \mod 17 = 7$

$K_3 = g(3) = 18 + 30 + 13 \mod 17 = 61 \mod 17 = 10$

$K_4 = g(4) = 32 + 40 + 13 \mod 17 = 85 \mod 17 = 0$

$K_5 = g(5) = 50 + 50 + 13 \mod 17 = 113 \mod 17 = 11$

Somit sind die 5 verschiedenen Teilschlüssel gegeben durch
(1,8), (2,7), (3,10), (4,0), (5,11).
g(x) kann z.B. aus den 3 Teilschlüsseln (1,8), (3,10)und (5,11) rekonstruiert werden:

$$g(x) = 8\,\frac{(x-3)(x-5)}{(1-3)(1-5)} + 10\,\frac{(x-1)(x-5)}{(3-1)(3-5)} + 11\,\frac{(x-1)(x-3)}{(5-1)(5-3)} \mod 17$$

$$g(x) = \frac{8}{8}(x-3)(x-5) + \frac{10}{13}(x-1)(x-5) + \frac{11}{8}(x-1)(x-3) \mod 17$$

$$= 8.15(x-3)(x-5) + 10.4(x-1)(x-5) + 11\text{-}15(x-1)(x-3) \mod 17$$

$$= (x-3)(x-5) + 6(x-1)(x-5) + 12(x-1)(x-3) \mod 17$$

$$= 19x^2 - 92x + 81 \mod 17$$

$$= 2x^2 + 10x + 13 \mod 17$$

Vorteile: (i) Man kann bei festen K_i durch Berechnung weiterer Werte von g(x) auch noch zusätzliche K_j ausgeben.

(ii) Durch Übergang zu einem neuen g(x) kann man einige ausgegebene Teilschlüssel beibehalten und andere vernichten.

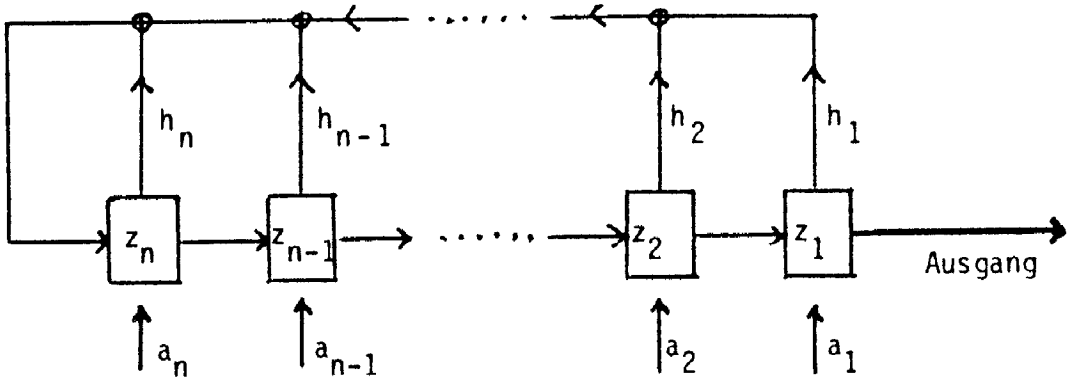
(iii) Die Einführung hierarchischer Systeme ist möglich, indem man an spezielle Personen mehrere Teilschlüssel vergibt.

2. Schieberegister und Polynome

1926 hat der Amerikaner G.S. Vernam die Methode der "Verschlüsselung mittels Ein-Weg-Schablone mit Zufallsziffern" entwickelt (vgl. W.B.Müller (1984)). Bei diesem Verfahren muß man als Schlüssel eine lange Zufallsfolge aus Bits auf einem sicheren Kanal übertragen.

In der Praxis verwendet man jedoch anstelle der binären Zufallsfolge eine durch einen Pseudozufallsgenerator erzeugte Pseudozufallsfolge aus Bits. Die Benutzer müssen dann bei Ausstattung mit dem gleichen Pseudozufallsgenerator lediglich gewisse Parameter austauschen und nicht mehr die gesamte Zufallsfolge. Diese Parameter dienen zur Synchronisation der identischen Pseudozufallsgeneratoren von Sender und Empfänger.

Eine Möglichkeit zur Erzeugung von binären Folgen mit einer hohen Periode bietet die Methode der rückgekoppelten Schieberegister. Wir betrachten ein n-stelliges Schieberegister mit Rückführungen



Die Rückkopplungskoeffizienten h_i sowie die Startwerte $a_n,\ldots,a_1$ sind boolesche Werte. Für $h_i = 0$ ist keine Rückführung vorhanden. Durch Schiebeimpulse werden die Inhalte jeder Stufe nach rechts geschoben, die Inhalte der rückgekoppelten Stufen ($h_i = 1$) werden modulo 2 addiert, und das so gebildete Summenbit wird an den Eingang (z_n) zurückgeführt.

Zustand zum Zeitpunkt t: $(z_n, z_{n-1}, \ldots, z_2, z_1)$

Zustand zum Zeitpunkt t+1: $(\sum_{i=1}^{n} h_i z_i, z_n, \ldots, z_3, z_2)$

Ausgangsfolge: $a_1, a_2, \ldots, a_n, a_{n+1} = \sum_{i=1}^{n} h_i a_i, \ldots, a_{n+j} = \sum_{i=1}^{n} h_i a_{i+j}$

Ein n-stelliges Schieberegister kann 2^n verschiedene Zustände annehmen. Sind alle $z_i = 0$, ändert sich der Zustand nicht mehr, daher muß man diesen Zustand ausschließen. Die Ausgangsfolge eines n-stelligen Schieberegisters muß sich daher spätestens nach $N = 2^n - 1$ Schiebeimpulsen wiederholen.

Man kann zeigen (vgl. S.W. Golomb (1967)), daß man Schieberegister mit einer maximalen Periode ($N = 2^n-1$) bekommt, falls

$$h_1 = 1,\ \sum_{i=1}^{n} h_i = 0 \bmod 2 \quad \text{und} \quad 1 + h_1 x + h_2 x^2 + \ldots + h_n x^n \text{ ein}$$

sogenanntes primitives Polynom vom Grad n über GF(2) ist.

Ein irreduzibles Polynom g(x) vom Grad n über GF(2) heißt primitives Polynom, wenn $g(x) \,/\, x^{2^n-1} - 1$ aber $g(x) \not/ x^k - 1$ für $k < 2^n - 1$.

Beispiel: $n = 4$, $(a_4,a_3,a_2,a_1) = (0,0,0,1)$, $(h_4,h_3,h_2,h_1) = (1,0,0,1)$

Somit ist $g(x) = x^4 + x + 1$, ein primitives Polynom über GF(2) vom Grad 4.

Zustände des Schieberegisters:

0	0	0	1
1	0	0	0
1	1	0	0
1	1	1	0
1	1	1	1
0	1	1	1
1	0	1	1
0	1	0	1
1	0	1	0
1	1	0	1
0	1	1	0
0	0	1	1
1	0	0	1
0	1	0	0
0	0	1	0

Ausgangsfolge: 1 0 0 0 1 1 1 1 0 1 0 1 1 0 0

Die folgende Tabelle gibt einen Oberblick über Schieberegister mit maximaler Periode und einer minimalen Anzahl von Rückführungen.

Registerlänge n	Periodenlänge N	minimale Rückführungen
2	3	(1,2)
3	7	(1,3)
4	15	(1,4)
5	31	(1,4)
6	63	(1,6)
7	127	(1,7)
8	255	(1,3,4,8)
9	511	(1,6)
10	1023	(1,8)
30	2 147 483 647	(1,15,16,30)

Bei der Verwendung derartiger Folgen für Vernam-Verschlüsselungen muß man jedoch beachten, daß der Feind die gesamte Pseudozufallsfolge kennt, sobald er einen zusammengehörigen Klartext und Schlüsseltext der Länge 2n kennt!
Derartige Folgen werden auch bei Entfernungsmessungen im Weltall verwendet (vgl. D.Dorninger und W.B.Müller (1984)).

3. Kommutative Kompositionshalbgruppen von Polynomen

Für viele Anwendungen in der Kryptographie benötigt man bezüglich der Koposition kommutative Verschlüsselungsfunktionen.
Beim Kryptosystem ohne Schlüsselaustausch, welches 1982 von A.Shamir vorgestellt wurde, sendet eine Person A an eine Person B eine geheime Nachricht m, indem sie m mittels der nur ihr bekannten Verschlüsselungsfunktion f_A zu $f_A(m)$ verschlüsselt und $f_A(m)$ an B durchgibt. B kann nun zwar m nicht rekonstruieren, verschlüsselt aber ihrerseits $f_A(m)$ mit der nur ihr bekannten Funktion f_B zu $f_B(f_A(m))$ und überträgt diese Nachricht zurück an A. Person A kann nun zwar die Nachricht auch selbst nicht mehr lesen, bildet aber mit der zu f_A inversen Funktion f_A^{-1} die Nachricht $f_A^{-1}(f_B(f_A(m)))$. Unter der Voraussetzung, daß f_A^{-1} mit f_B vertauschbar ist, gilt jedoch $f_A^{-1}(f_B(f_A(m) = f_B(m)$. Diese Nachricht sendet A an B und Person B kann nun mittels der inversen Funktion f_B^{-1} zu f_B den Text mittels $f_B^{-1}(f_B(m)) = m$ entschlüsseln. Unter der Voraussetzung der Kommutativität der verwendeten Verschlüsselungsfunktionen können daher A und B durch dreimaliges Obertragen geheime Nachrichten austauschen, ohne vorher geheime Entschlüsselungsinformationen vereinbart zu haben.

Auch das Diffie/Hellman Key-Distribution-System beruht auf der Verwendung gegenüber der Komposition kommutativer Funktionen. Eine Zahl m wird öffentlich bekanntgegeben. Will nun Person A einen gemeinsamen Schlüssel mit Person B generieren, so muß A mit einer nur ihn bekannten Funktion $f_A(m)$ berechnen und diesen Wert an B übermitteln. Analog berechnet B mit der nur ihr bekannten Funktion f_B die Zahl $f_B(m)$ und übermittelt diese an A. Zur Generierung eines gemeinsamen Schlüssels berechnet dann A die

Zahl $f_A(f_B(m))$ und Person B die Zahl $f_B(f_A(m))$. Sind f_A und f_B vertauschbar, dann erhalten A und B dieselbe Zahl und somit einen gemeinsamen geheimen Schlüssel.

Auch bei den 1976 von Diffie und Hellman eingeführten Public-Key Kryptosystemen erweisen sich kommutative Verschlüsselungsfunktionen als sehr zweckmäßig (vgl. W.B.Müller (1984)).

Leider kennt man bisher nicht sehr viele kommutative Kompositionshalbgruppen von Polynomen und damit von Polynomfunktionen, welche sich für kryptographische Zwecke eignen. Am häufigsten wurden bisher die Potenzpolynomfunktionen $x \longrightarrow x^k \bmod n$, $k,n \in \mathbb{N}$ als Verschlüsselungsfunktionen verwendet. Wegen $x^k \circ x^t = x^t \circ x^k$ für beliebige $k,t \in \mathbb{N}$, sind diese Funktionen kommutativ bezüglich der Komposition. Eine weitere Klasse von kommutativen Funktionen sind $x \longrightarrow t_k(x) \bmod n$, wobei $t_k(x)$ das Tschebyscheffpolynom erster Art vom Grad k bezeichnet. Aus der bekannten Halbgruppeneigenschaft der Tschebyscheffpolynome $t_k(x) \circ t_s(x) = t_{k.s}(x) = t_s(x) \circ t_k(x)$ folgt nämlich auch sofort die Kommutativität der durch sie induzierten Polynomfunktionen.
Eine genaue Diskussion weiterer kommutativer Kompositionshalbgruppen ist hier aus Platzgründen leider nicht möglich, kann aber in R.Lidl und W.B.Müller (1986) nachgelesen werden.

LITERATUR

S.W.Golomb: Shift Register Sequences, Holden-Day Inc., San Francisco, 1967.

R.Lidl und H.Niederreiter: Introduction to finite fields and their applications. Cambridge Univ. Press, 1986.

D.W.Dorninger und W.B.Müller: Allgemeine Algebra und Anwendungen. B.G.Teubner, Stuttgart, 1984.

W.B.Müller: Mathematische Methoden bei Problemen des Datenschutzes. 124-146, ÖMG Didaktik-Reihe, Heft 11, Wien, 1984.

W.B.Müller: Polynomial functions in modern cryptology. 7-32, Contributions to General Algebra 3, Hölder-Pichler-Tempsky Wien und B.G.Teubner Stuttgart, 1985.

A.Shamir: How to share a secret. Communications of the ACM, Vol.22, Number 11, 1979.