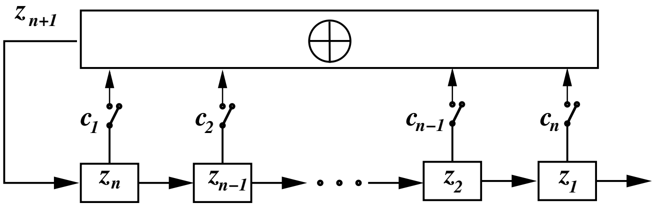
Lineárne posuvné registre Linear Feedback Shift Registers LFSR

Stanislav Palúch

Fakula riadenia a informatiky, Žilinská univerzita

28. októbra 2010

Lineárny posuvný register



Postupnosť $c_1, c_2, \ldots, c_n$ – zpätno-väzbová sekvencia – tap sequence

$$z_{n+1} = c_1 z_n \oplus c_2 z_{n-1} \oplus \cdots \oplus c_{n-1} z_2 \oplus c_n z_1 \qquad (1)$$

Maximálna perióda LFSR dĺžky n je $2^n - 1$.

Zpätno-väzbový polynóm – connection polynomial – je polynóm nad $\mathbb{Z}_2$:

$$1 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n$$

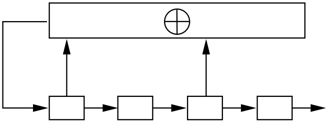
Primitívny polynóm stupňa n je taký polynóm ktorý je

- iredučibilný
- je deliteľom polynómu $x^{2^{n-1}} + 1$
- nie je deliteľom žiadneho polnómu tvaru $x^d + 1$, kde d delí $2^n - 1$

Zpätnoväzobný polynóm

Platí: Lineárny posuvný register dĺžky n má maximálnu periódu $2^n - 1$ práve vtedy, keď jeho zpätnoväzobný polynóm je primitívny.

Singulárny LFSR je taký LFSR, ktorého dĺžka je väčšia než stupeň väzobného polynómu.

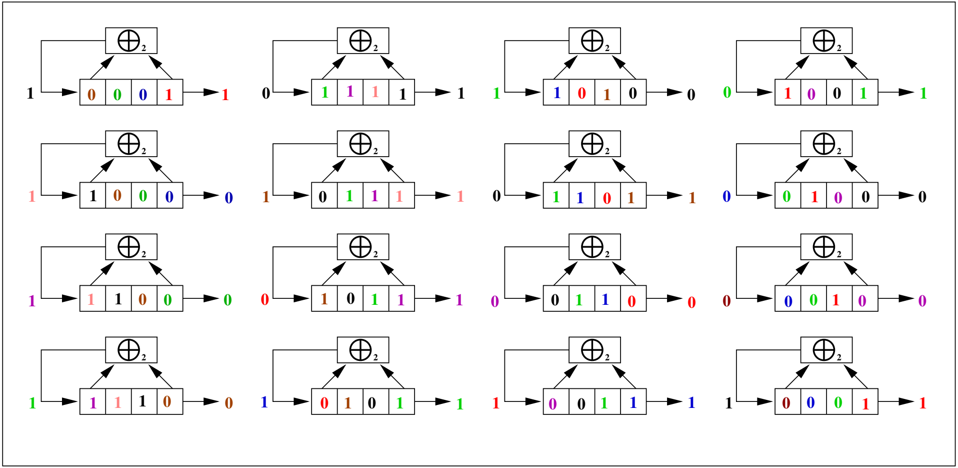


Nie sú zaručená periodicita pre každý počiatočný stav singulárnych LFSR, preto sa v kryptografii nepoužívajú.

Zistiť, či je daný polynóm primitívny je algoritmicky riešiteľný problém.

Hľadanie primitívnych polynómov je ťažké.

Príklad práce LFSR



LFSR v tabuľkovom procesore

	A	B	C	D	E
1	0	0	0	0	0
2	=MOD(A1+D1+ E1;2)	=A1	=B1	=C1	=D1

Druhý riadok tabuľky sa rozkopíruje do ďalších riadkov stĺpcov A až E.

Výstupné bity z LFSR sa použijú ako prúd pseudonáhodných binárnych čísel.

Kľúč:

- Počiatočné nastavenie registra – n bitov $z_1, z_2, \ldots, z_n$
- Nastavenie zpätnoväzbovej postupnosti n bitov $c_1, c_2, \ldots, c_n$

Ak poznáme zpätnoväzobnú postupnosť a ak a odchytíme porade n bitov z LFSR, ďalšie bity ľahko vypočítame podľa rovnice (1).

Útok na LFSR ak poznáme 2n bitov

Ak poznáme len dĺžky LFSR postupujeme nasledovne:
Predpokladajme, že poznáme n – dĺžku LFSR a $2n$ výstupných bitov:

$$z_{2n}, z_{2n-1}, \dots, z_2, z_1$$

$$\begin{array}{llll}
z_{n+1} = c_1 z_n & \oplus \dots \oplus c_{n-1} z_2 & & \oplus c_n z_1 \\
z_{n+2} = c_1 z_{n+1} & \oplus \dots \oplus c_{n-1} z_3 & & \oplus c_n z_2 \\
\dots\dots\dots & \dots\dots\dots & & \dots\dots \\
z_{2n} \; = c_1 z_{2n-1} & \oplus \dots \oplus c_{n-1} x_n z n - 1 & & \oplus c_n z_n
\end{array}$$

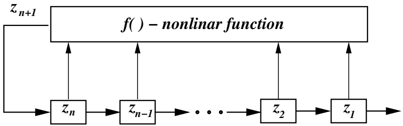
$$\begin{pmatrix} z_n & z_{n-1} & \dots & z_1 \\ z_{n-1} & z_{n-2} & \dots & z_2 \\ \dots & \dots & \dots & \dots \\ z_{2n-1} & z_{2n-2} & \dots & z_n \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_n \end{pmatrix}$$

$$\mathbf{Zc} = \mathbf{z} \qquad \mathbf{c} = \mathbf{Z}^{-1}\mathbf{z}$$

Dôsledok: Kryptografia pomocou LFSR je veľmi slabá a nesmie sa používať.

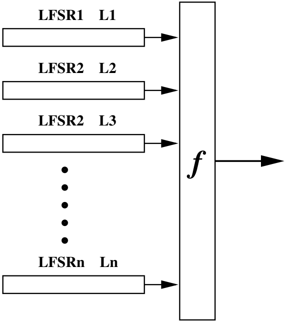
Pokusy o zlepšenie bezpečnosti LFSR

Náhrada $\oplus$ nelineárnou funkciou:

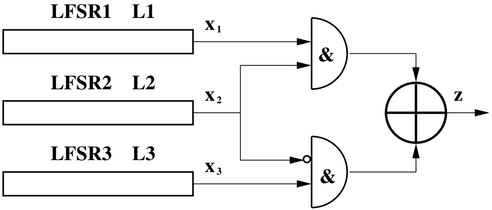


Nevýhoda: Ťažko sa teoreticky študujú, ťažko sa dokazujú vlastnosti ako napr. existencia krátkych cyklov.

Výstupy z viacerých LSFR použiť ako vstupy do nelineárnej funkcie.



Geffe-ho generátor



$$z = x_1.x_2 \oplus (1 \oplus x_2).x_3$$

$$P[z = x_1] = \underbrace{P[x_2 = 1]}_{=\frac{1}{2}} + \underbrace{P[x_2 = 0]}_{=\frac{1}{2}} . \underbrace{P[x_3 = x_1]}_{=\frac{1}{2}} = \frac{1}{2} + \frac{1}{2}.\frac{1}{2} = \frac{3}{4}$$

$$P[z = x_3] = \underbrace{P[x_2 = 0]}_{=\frac{1}{2}} + \underbrace{P[x_2 = 1]}_{=\frac{1}{2}} . \underbrace{P[x_3 = x_1]}_{=\frac{1}{2}} = \frac{1}{2} + \frac{1}{2}.\frac{1}{2} = \frac{3}{4}$$

Geffe-ho generátor

Iný spôsob zistenia pravdepodobností $P[x_i = z]$.

Tabuľka výstupnej funkcie $z = x_1.x_2 \oplus (1 \oplus x_2).x_3$

	x_1	x_2	x_3	$z = x_1.x_2 \oplus (1 \oplus x_2).x_3$	$x_1 = z$	$x_3 = z$
	0	0	0	0	+	+
	0	0	1	1	-	+
	0	1	0	0	+	+
	0	1	1	0	+	-
	1	0	0	0	-	+
	1	0	1	1	+	+
	1	1	0	1	+	-
	1	1	1	1	+	+

Z tejto tabuľky možno vypočítať pravdepodobnosti

$$P[x_1 = z] = \frac{6}{8} = \frac{3}{4}, \qquad P[x_3 = z] = \frac{6}{8} = \frac{3}{4}.$$

Korelačný útok

Kľúč Geffe-ho generátora – štartovacia náplň registrov LFSR1, LFSR2 a LFSR3 – t.j. $(2^{L_1}-1)(2^{L_2}-1)(2^{L_3}-1)$ možností.

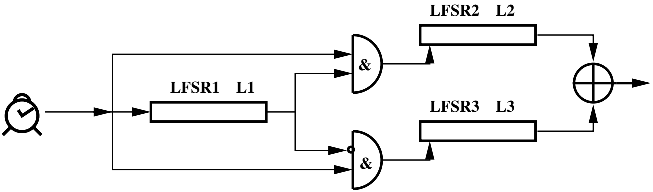
Korelačný útok:
Máme postupnosť $\mathbf{z} = z_1, z_2, \ldots, z_k, \ldots$ z výstupu generátora.

Krok 1.:
Ľubovoľne nastavíme LFSR2 a LFSR3 a postupne nastavujme LFSR1 a počítajme počet zhôd výstupu generátora s postupnosťou **z**. Ak počet zhôd stôpne zhruba na $\frac{3}{4}$, bude LFSR1 nastavený tak ako na začiatku postupnosti **z**.
Krok 2.:
Rovnakým spôsobom nastavíme počiatočný stav registra LFSR3.
Krok 3.:
Nakoniec dopočítame nastavenie registra LFSR2.

Namiesto $(2^{L_1}-1)(2^{L_2}-1)(2^{L_3}-1)$ možností počiatočného nastavenia registrov bude treba vyskúšať najviac $(2^{L_1}-1)+(2^{L_3}-1)$ možností.

Tento princíp je použiteľný pre akýkoľvek systém LFSR s akoukoľvek výstupnou funkciu, ak pre výstup x_i z i-teho LFSR platí $P[x_i = z] \neq \frac{1}{2}$.

Alternating Step Generator



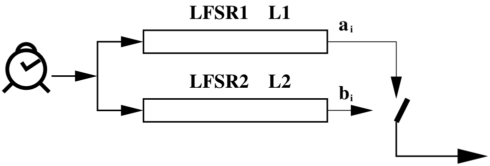
Podľa výstupu LFSR1 sa posúva práve jeden z generátorov LFSR2, LFSR3.
Ak je výstup z LFSR1 1, posunie sa generátor LFSR2, inak sa posunie LFSR3.
Ak sa LFSR1 modifikuje tak, aby po $(L_1 - 1)$ nulách vyslal ešte jednu nulu, cyklus tohoto generátora bude

$$2^{L_1}.(2^{L_2} - 1).(2^{L_3} - 1)$$

ak sú L_1, L_2, L_3 nesúdeliteľné.

PreL_1, L_2, L_3 nesúdeliteľné, $L_1 \approx L_2 \approx L_3 \approx 128$ je tento generátor bezpečný proti všetkým známym útokom.

Shrinking Generator



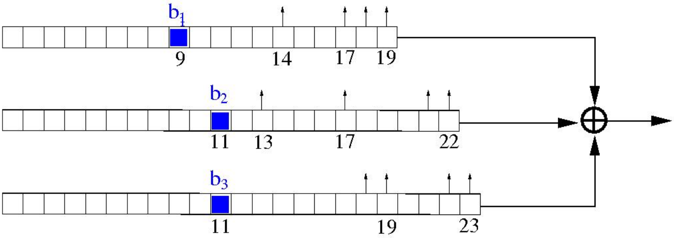
Ak $b_i = 1$, výstupom je bit a_i. Ak $b_i = 0$, zruš a_i.

Ak sú L_1, L_2 nesúdeliteľné, potom má generátor periódu

$$(2^{L_1} - 1).(2^{L_2} - 1)$$

GSM A5 algoritmus

LFSR1 – (19, 18, 17, 14, 0)
LFSR2 – (22, 21, 17, 13, 0)
LFSR3 – (23, 22, 19, 18, 0)



$$posun(i) = b_i \oplus \overline{T(b_1, b_2, b_3)}$$

$$\overline{T(b_1, b_2, b_3)} = \begin{cases} 0 & \text{ak } (b_1 + b_2 + b_3) \geq 2 \\ 1 & \text{ak } (b_1 + b_2 + b_3) \leq 1 \end{cases}$$

$$posun(i) = b_i \oplus \overline{T(b_1, b_2, b_3)}$$

Blum - Micalli generátor, RSA generátor

Blum - Micalli generátor:
g, p dve veľké prvočísla

$$
\begin{aligned}
x_{i+1} &= g^{x_i} \mod p \\
b_i &= \begin{cases} 1 & \text{ak } x_i < \frac{p-1}{2} \\ 0 & \text{inak} \end{cases}
\end{aligned}
$$

RSA generátor:

p, q dve veľké tajné prvočísla
$N = p.q$
e nesúdeliteľné s $(p-1)(q-1)$

$$
\begin{aligned}
x_{i+1} &= x_i^e \mod N \\
b_i &= x_i \mod 2 \text{ (– najmenej významný bit } x_i\text{)}
\end{aligned}
$$

Princíp testovania hypotéz

Majme postupnosť bitov

$$\mathbf{b} = b_1, b_2, \dots, b_n$$

z nejakého generátora náhodných čísel.
Treba zistiť, či táto postupnosť je skutočne náhodná.

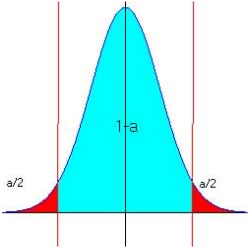
Nasledujúce testy umožnia vylúčiť také postupnosti, ktoré sa na šifrovanie nehodia.

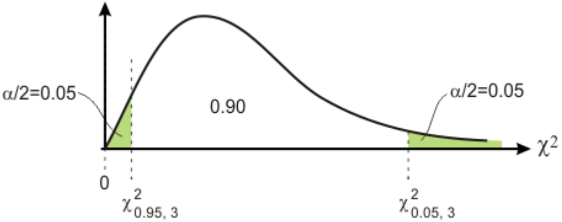
Princíp všetkých testov je nasledujúci:

- Stanoví sa hypotéza H (napríklad "$P[b_i = 1] = P[b_i = 0] = \frac{1}{2}$" – t. j. prevdepodobnosť nuly a jedničky je rovnaká).
- Stanovíme tzv. stupeň významnost α ako pravdepodobnosť zamietnutia hypotézy H napriek tomu, že hypotéza H platí (to je tzv. chyba prvého druhu).
  Najčastejšie používané hodnoty sú $\alpha = 0.05$ a $\alpha = 0.01$.

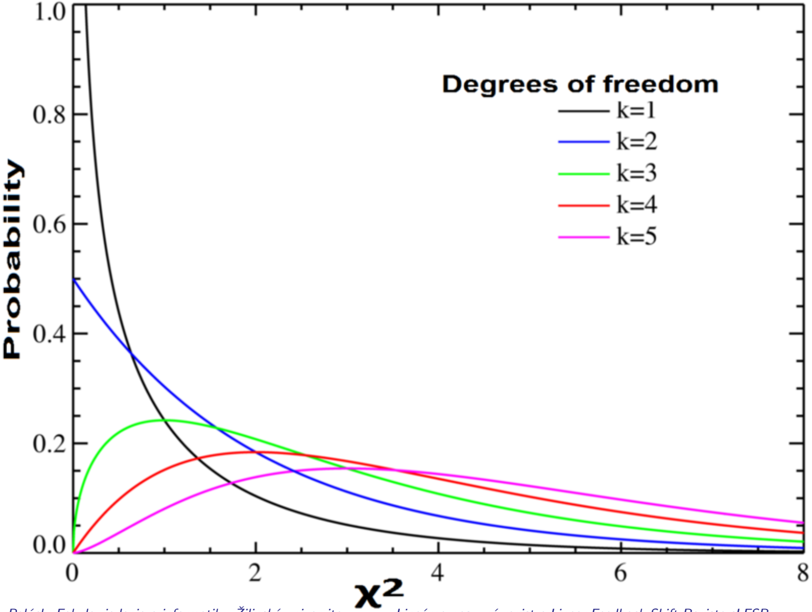
Princíp testovania hypotéz

- Určí sa náhodná veličina $X = f(b_1, b_2, \dots, b_n)$ (nazývaná tiež štatistika), ktorá má za predpokladu platnosti hypotézy H známe rozdelenie f (najčastejšie normálne $f = N(0,1)$ alebo $f = \chi^2(k)$ o k stupňoch voľnosti).
- Určí sa interval (a, b) – tzv. interval spoľahlivosti (confidence interval) taký, že $P[X \in (a, b)] = 1 - \alpha$.
  Oblasť na reálnej osi $(-\infty, a\rangle \cup \langle b, \infty)$ sa volá kritická oblasť.
- Ak X padne do kritickej oblasti, hypotézu H zamietame, pretože nastal neočakávaný jav.
- Ak X padne do intervalu (a, b), hypotézu H nezamietame.





Hustota rozdelenia χ^2 pre rôzne stupne voľností



Frekvenčný test

Máme postupnosť bitov $\mathbf{b} = b_1, b_2, \ldots, b_n$.

n_0 – počet núl n_1 – počet jednotiek $n = n_o + n_1$

Za predpokladu, že $\mathbf{b}$ je náhodná postupnosť s rovnakou pravdepodobnosťou núl a jednotiek má štatistika

$$X_1 = \frac{(n_0 - n_1)^2}{n}$$

$\chi^2(1)$ rozdelenie s jedným stupňom voľnosti pre $n \geq 10$ a testovaná hypotéza H je že $X_1 = 0$.

Dvojbitový sériový test

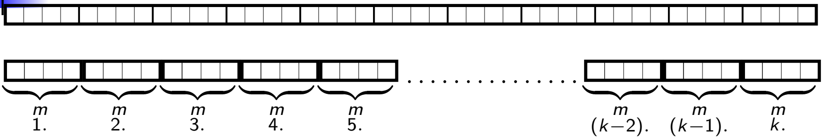
Dvojbitový sériový test
$n_{00}, n_{01}, n_{10}, n_{11}$ – počet výskytov dvojíc 00, 01, 10, 11 v postupnosti **b** .

Platí $n_{00} + n_{01} + n_{10} + n_{11} = n - 1$.

$$X_2 = \frac{4}{n-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1$$

Pre $n \geq 21$ má štatistika X_2 rozdelenie $\chi^2(2)$ s dvoma stupňami voľnosti.
Testujeme platnosť hypotézy $X_2 = 0$.

Poker test



Skúmanú n-prvkovú postupnosť bitov $\mathbf{b}$ rozdelíme na k m-tíc.

Zrejme je $k.m \leq n$.

Číslo m musí byť zvolené tak, aby $k \geq 5.2^m$.

Každá m-tica bitov predstavuje číslo v rozmedzí 0 až $2^m - 1$.
Pre $i = 0, 1, 2, \ldots, 2^m - 1$ označme n_i počet m-tíc takých, že predstavujú binárny rozvoj čísla i.

$$X_3 = \frac{2^m}{k} . \left(\sum_{i=0}^{2^m-1} n_i^2 \right) - k$$

Štatistika X_3 má rozdelenie $\chi^2(2^m - 1)$ a testujeme hypotézu $X_3 = 0$.

Runs test

Blok dĺžky n je postupnosť n jednotiek v postupnosti $\mathbf{b}$ z oboch strán ohraničená nulou alebo začiatkom alebo koncom postupnosti b.

Medzera (Gap) dĺžky n je postupnosť n núl v postupnosti $\mathbf{b}$ z oboch strán ohraničená jednotkou alebo začiatkom alebo koncom postupnosti b.
Pravdepodobnosť výskytu bloku dĺžky i: $\ldots 0 \underbrace{1\,1 \,\ldots\, 1}_{i} 0 \ldots$

v nekonečne dlhej náhodnej postupnosti bitov je $\dfrac{1}{2^{i+2}}$.

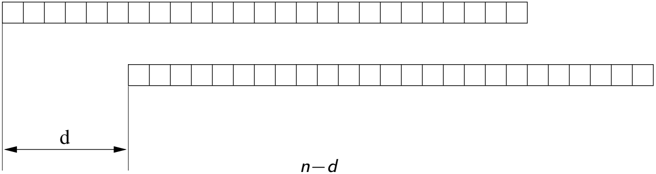
Očakávaný počet blokov dĺžky i v n-prvkovej postupnosti $\mathbf{b}$ je $e_i = \frac{n-i+3}{2^{i+2}}$.

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i}$$

kde k je najväčši také, že $e_i \geq 5$ a B_i, G_i je skutočný počet blokov, resp. medzier dĺžky i v postupnosti $\mathbf{b}$.
Štatistika X_4 má rozdelenie $\chi^2(2k-2)$, testovaná hypotéza je $X_4 = 0$.

Autokorelačný test

d – pevné číslo $1 \leq d \leq [\frac{n}{2}]$



$$A(d) = \sum_{i=1}^{n-d} b_i \oplus b_{i+d}$$

$$X_5 = 2.\frac{A(d) - \dfrac{n-d}{2}}{\sqrt{n-d}}$$

Štatistika X_5 má normálne rozdelenie $N(0,1)$.

Testujeme hypotézu $X_5 = 0$.

FIPS 140–1 štatistický test

Test je určený pre reťaze **b** dlhý 20000 bitov.

1. Monobit test: $1 < n_1 < 10346$
2. Poker test pre $m = 4$: $1.03 < X_3 < 57.4$
3. Runs test.
   Pre $i = 1, 2, 3, 4, 5$ B_i resp. G_i – počet blokov resp. medzier dĺžky i.
   Pre $i = 6$ B_6 resp. G_6 počet blokov resp. medzier dĺžky 6 a viac.

i	Dovolený rozsah B_i, G_i
1	2267 – 2733
2	1079 – 1421
3	502 – 748
4	223 – 402
5	90 – 223
6	90 – 223

4. Long run test. Nesmie existovať blok alebo medzera dĺžky 34 alebo viac.