Návrh a kryptoanalýza šifier - Zadanie 3

Peter Čuřík

10. októbra 2021

1 LFSR

Na účely zadania bol skonštruovaný 32 bitový lineárny spätnoväzobný register. Zvolený polynóm je ireducibilný a primitívny, z poľa Z_{32}:

$$x^{32} + x^{22} + x^2 + x + 1$$

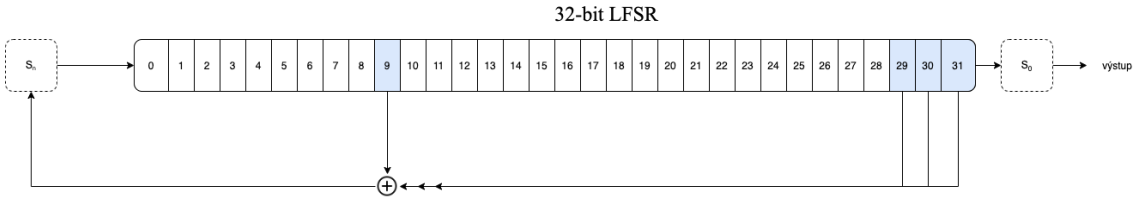
Na výpočet nového prvku postupnosti je potrebné aplikovanie bitovej operácie XOR správnych bitov v LFSR. Matematické vyjadrenie toho, ktoré členy postupnosti majú byť spájané pomocou XOR na vznik nového člena postupnosti je nasledovné:

$$S_{32} = S_{22} + S_2 + S_1 + S_0$$
$$S_{32+k} = S_{22+k} + S_{2+k} + S_{1+k} + S_k$$
$$n = 32 + k$$
$$S_n = S_{n-10} + S_{n-30} + S_{n-31} + S_{n-32}$$

2 Implementácia

Vlastné riešenie v jazyku C. Dôvody výberu jazyka - jednoduchá práca s bitmi, vysoká rýchlosť behu programu, čo implikuje časovo uľahčené testovanie kódu a vzoriek.

LFSR je reprezentované ako pole dĺžky 32. Tým pádom na základe matematického vyjadrenia nového člena postupnosti (vyššie) vieme na pevno určiť indexy, ktorých hodnoty budeme XORovať. Čísla indexov v tomto prípade sú nasledovné: 31, 30, 29, 9. Grafická reprezentácia:



Výstupný bit je vpísaný do char buffera, ktorý kumuluje bity po ôsmich a potom vytvorí výstupný bajt, ktorý je zapísaný do súboru.

Pre každú postupnosť zo vzorky bol náhodne vygenerovaný prvotný obsah registra LFSR, okrem prvého a posledného bitu. Tie sú vždy na začiatku inicializované na 1, kvôli zamedzeniu prípadu, kedy je všetkých 32 bitov nastavených na nulu.

3 Výsledky

3.1 Experiment 1: 100 postupností po 1MB (8 miliónov bitov)

Postupnosti boli podrobené štatistickým NIST testom. Tabuľka nižšie zobrazuje úspešnosť vzorky voči testom (pre prehľadnosť dokumentu ukážem iba podmnožinu všetkých výsledkov testov).

P-Value	Proportion	Test
0.897763	100/100	Frequency
0.49439	100/100	BlockFrequency
0.015598	100/100	CumulativeSums
0.202268	100/100	CumulativeSums
0.249284	99/100	Runs
0.162606	100/100	LongestRun
0.000000	0/100	Rank
0.236810	96/100	FFT
0.971699	100/100	NonOverlappingTemplate
0.455937	99/100	NonOverlappingTemplate
0.021999	98/100	NonOverlappingTemplate
0.574903	99/100	NonOverlappingTemplate
0.236810	98/100	NonOverlappingTemplate
0.883171	100/100	NonOverlappingTemplate
0.334538	99/100	NonOverlappingTemplate
0.058984	99/100	NonOverlappingTemplate
0.350485	100/100	NonOverlappingTemplate
0.834308	100/100	NonOverlappingTemplate
...	...	...
0.334538	99/100	NonOverlappingTemplate
0.262249	96/100	NonOverlappingTemplate
0.304126	98/100	NonOverlappingTemplate
0.637119	100/100	NonOverlappingTemplate
0.350485	99/100	OverlappingTemplate
0.991468	97/100	Universal
0.129620	98/100	ApproximateEntropy
0.360699	85/85	RandomExcursions
0.381687	84/85	RandomExcursions
0.977331	82/85	RandomExcursions
0.087559	84/85	RandomExcursions
0.999091	84/85	RandomExcursions
0.117948	85/85	RandomExcursions
0.081137	85/85	RandomExcursions
0.206354	84/85	RandomExcursions
0.206354	85/85	RandomExcursionsVariant
0.752361	84/85	RandomExcursionsVariant
0.015734	83/85	RandomExcursionsVariant
0.340461	83/85	RandomExcursionsVariant
0.572333	82/85	RandomExcursionsVariant
...	...	...
0.776784	85/85	RandomExcursionsVariant
0.934318	84/85	RandomExcursionsVariant
0.425817	85/85	RandomExcursionsVariant
0.275709	100/100	Serial
0.334538	100/100	Serial
0.000000	0/100	LinearComplexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately = 81 for a sample size = 85 binary sequences.

3.2 Experiment 2: 100 postupností po 10MB (80 miliónov bitov)

Vzorka bola podrobená softvéru Paranoya. Výsledky sú podobné ako pri experimente 1: pre každý test prešlo 96 - 100% postupností z celej vzorky. Zlyhali Rank a Linear Complexity.

4 Záver

Z výsledkov oboch testov vyplýva, že registrom sa generovali dobré seedy, polynóm bol vhodne zvolený, psuedonáhodnosť bola do uspokojujúcej miery nerozlíšiteľná od pravej náhodnosti. Avšak dva testy v oboch prípadoch zlyhali. Aj Rank, aj Linear Complexity test vykazujú P-value rovnú nule pre celú vzorku.

4.1 Linear Complexity

Podľa dokumentácie k softvéru od NIST, znie princíp Linear Complexity testu nasledovne:

,,The focus of the test is the rank of disjoint sub-matrices of the entire sequence. The purpose of this test is to check for linear dependence among fixed length substrings of the original sequence."

Z uvedeného usudzujem, že nakoľko je LFSR lineárny register, je ľahké nájsť lineárne závislosti medzi jednotlivými blokmi bitov. Na takýto test je zrejme potrebný iný pseudonáhodný generátor.

4.2 Rank test

Podľa dokumentácie k softvéru od NIST, znie princíp Rank testu nasledovne:

,,The focus of this test is the length of a linear feedback shift register (LFSR). The purpose of this test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by longer LFSRs. An LFSR that is too short implies non-randomness."

Z uvedeného usudzujem, že dĺžka LFSR nebola dostatočná. Šance na prejdenie týmto testom sa zvyšujú s každým zväčšením LFSR (napríklad z aktuálnych 32 bitov na 64).

4.3 Ďalšie komentáre

Prínosy experimentu 2 oproti experimentu 1 nepovažujem za veľké, ak vôbec nejaké nastali. Niektoré problémy by mohli byť vyriešené dlhším LFSR registrom. Výsledky by mohla zlepšiť aj tzv. filtračná funkcia. Celkovo hodnotím výsledky testov pre LFSR ako pozitívne. Na druhej strane, bolo možné vidieť aj zopár bezpečnostných dier tohto registra.