NI-KRY - TRNG

Tomáš Chvosta (chvostom)

Říjen 2020

Postup

Úkolem bylo zjistit pomocí sady testů `STS` od `NIST`, jak kvalitní je náhodný generátor, který vygeneroval dodanou posloupnost bitů. Na každém řádku obsahujícím binárně vyjádřené slovo získané měřením vzájemných časových odchylek dvou nezávislých oscilátorů byly nejprve separovány jednotlivé bity do souborů `f0` pro 0. bit až po `f15` pro 15. bit. Dále byl implementován program založený na principu kompresního algoritmu `RLE`, který provedl analýzu posloupností opakujících se bitů (zdrojový kód ve složce `Komprese`). Pomocí této analýzy bylo zjištěno, že v sekvencích bitů v souborech `f4` až `f15` je při zvolení náhodného bitu šance, že následující bit bude shodný, vyšší než 75% (přesné naměřené hodnoty lze najít v přiloženém textovém souboru `bitsReport`). To je však nevyhovující z hlediska požadavků na kryptograficky bezpečné náhodné generátory. Proto se o těchto bitech dá říci, že nejsou zcela náhodné.

Posloupnosti bitů v souborech `f0` až `f3` byly testovány pomocí sady testů `STS` od `NIST`. `The NIST Test Suit` je baterie obsahující 15 testů, které byly vyvinuty pro testování náhodnosti libovolně dlouhých binárních souborů. Pro většinu testů byly jednotlivé soubory o velikosti 5400000 bitů rozděleny na 576 podposloupností o velikosti 9375 bitů. Pouze testy č.10 (`Universal Statistical test`), č.12 (`Random Excursions test`), č.13 (`Random Excursions Variant test`) a č.15 (`Linear Complexity test`) vyžadovaly pro přesnější výsledek testu posloupnosti, které byly delší než 390000 bitů resp. 10000000 bitů. Proto pro test číslo 10 byly vstupní soubory rozděleny na 12 podposloupností o velikosti 450000 bitů a pro test č.12, č.13 a č.15 na 5 podposloupností o velikosti 1080000 bitů. Dále byly pro některé testy zvoleny následující parametry, aby došlo k vhodnému rozdělení podposloupností na bloky:

- **Block Frequency Test** - délka bloku (M): 125
- **NonOverlapping Template Test** - délka bloku (m): 9
- **Overlapping Template Test** - délka bloku (m): 9
- **Approximate Entropy Test** - délka bloku (m): 5
- **Serial Test** - délka bloku (m): 5
- **Linear Complexity Test** - délka bloku (M): 1000

Stručný popis všech 15 testů včetně doporučení pro správné zvolení parametrů lze nalézt v přiloženém souboru `PopisTestu.pdf`

Výsledky testování

Pro testování byl vytvořen skript `runAllTest.sh`, který spustil všech 15 testů se zvolenými parametry pro všechny testované pozice bitů. V následující tabulce pak vidíme, kolik podposloupností v testu uspělo. Pokud je výsledek zapsán zelenou resp. červenou barvou, pak testované pozice bitů v testu uspěly resp. neuspěly. Pokud je výsledek oranžovou barvou, pak test neprošel kvůli malé p-hodnotě rovnoměrnosti rozložení elementárních p hodnot. Pro úspěch v testu bylo potřeba, aby v testu prošlo 563 z celkových 576 testovaných podposloupností (případně 10/12, 4/5 a 1/1 pro jinak rozdělené posloupnosti bitů). Přesné výsledky testování lze nalézt ve složce `Results`.

Tabulka 1: Tabulka s výsledky testování

	0.bit	**1.bit**	**2.bit**	**3.bit**
1-Frequency	563/576	563/576	564/576	294/576
2-Block Frequency	564/576	561/576	555/576	0/576
3-Cumulative Sums	562/576	563/576	561/576	138/576
4-Runs test	570/576	565/576	549/576	0/576
5-Longest Run of Ones	566/576	571/576	568/576	4/576
6-Rank test	572/576	572/576	574/576	571/576
7-Discrete FT[1]	568/576	565/576	568/576	562/576
8-Nonperiodic TM[2]	565/576	565/576	564/576	501/576
9-Overlapping TM[3]	571/576	572/576	568/576	19/576
10-Universal Statistical	11/12	12/12	12/12	0/12
11-Approximate Entropy	564/576	567/576	554/576	0/576
12-Random Excursions	-/-	-/-	1/1	0/1
13-Random Excursions V.[4]	-/-	-/-	1/1	1/1
14-Serial	569/576	565/576	560/576	1/576
15-Linear Complexity	5/5	5/5	4/5	5/5

Během testování bylo zjištěno, že původní vstupní soubory mají nedostatečný počet bitů pro testy `Random Excursions` a `Random Excursions Variant`, proto testy ve většině případů neproběhly. Nejlepších výsledků testování dosáhly posloupnosti 0. a 1. bitů a ze všech posloupností se tak nejvíce přiblížily k posloupnostem generovaným `TRNG`. Ty jen velmi těsně neuspěly v testu `Cumulative Sums` resp. `Block Frequency` a dále neuspěly v testu Rank kvůli malé p-hodnotě rovnoměrnosti rozložení elementárních p hodnot. Naopak u posloupností 2. a 3. bitů se dá předpokládat, že nesplňují vlastnosti čistě náhodné posloupnosti. Z provedených testů však nelze dělat žádné velké závěry vzhledem k tomu, že testované posloupnosti mají pouze 5400000 bitů.

[1] FT - Fourier Transform
[2] TM - Template Matchings
[3] TM - Template Matchings
[4] V. - Variant