Kwantowy Generator Liczb Losowych Wykorzystujący Szum Śrutowy

Jakub Niemczuk

Politechnika Wrocławska
jakub@niemczuk.tech

10 lutego 2020

Streszczenie

Dokument ten przedstawia podsumowanie prac nad kwantowym generatorem liczb losowych wykonanych w czasie od poprzedniego raportu. Opracowano w pełni funkcjonalny prototyp małego, integralnego, niezależnego generatora liczb losowych wykorzystującego szum śrutowy, występujący w fotodiodzie jako źródła fundamentalnie niedeterministycznej losowości. Urządzenie generuje strumień bitów z prędkością 1 Mb/s. Dane wyjściowe generatora zostały przetestowane zestawem testów statystycznych będących standardem przemysłowym w zakresie weryfikacji jakości kryptograficznych generatorów liczb losowych. Generator wykazuje najwyższy stopień losowości i użyteczności.

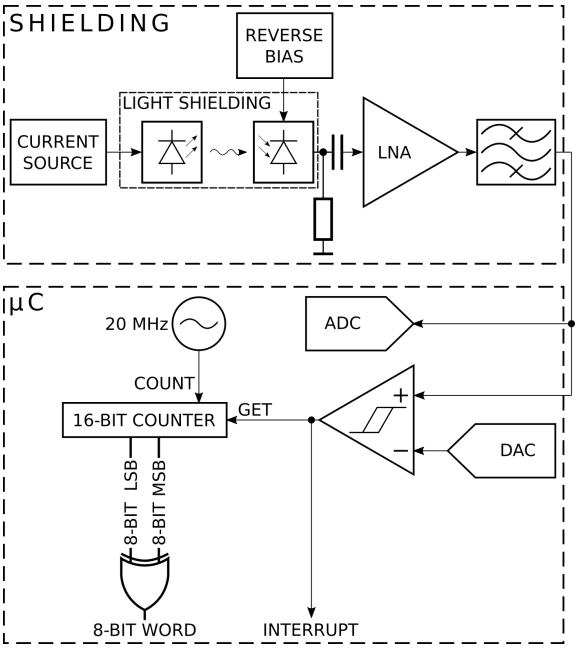
I. Wstęp

Pomyślnie zakończono pracę nad kwantowym generatorem liczb losowych wykorzystującym szum śrutowy w fotodiodach jako źródło kwantowego szumu. Po pomyślnym zidentyfikowaniu źródeł szumów w półprzewodnikach i opracowaniu sposobów eliminacji szumów potencjalnie deterministycznych, bo wywodzących się z efektów klasycznych, opisanych w poprzednim raporcie, rozwiązano problemy implementacyjne i układowe, zakańczając pracę budową układu i opracowaniem technologi która generuje liczby spełniające najsurowsze kryteria kryptograficzne i statystyczne za pomocą efektów czysto kwantowych. Przedstawiana konstrukcja zawiera szereg ulepszeń w stosunku do poprzedniej. Zrezygnowano z wzmacniacza transimpedancyjnego na rzecz prostego przekształtnika sygnału prądowego na napięciowy, opartego o układ rezystora i kondensatora. Zrezygnowano z metody generacji strumienia bitów polegającej na porównywaniu czasów pomiędzy impulsami w niezależnych parach na rzecz układu inkrementalnego zegara pracującego w trybie ciągłym z którego liczby pobierane są w momencie wykrycia zdarzenia wynikającego z szumu śrutowego. Urządzenie wyposażono w kontroler portu szeregowego USB dzięki któremu możliwe jest zastosowanie generatora w każdym systemie informatycznym, generując entropię z prędkością 1 MB/s. Cały system zawiera się w wymiarach 28x10x46,5 mm z pominięciem złącza USB. Dane wygenerowane przez urządzenie wykazują cechy losowości oraz pozytywnie przechodzą wszystkie testy statystyczne pakietu dieharder oraz pakietu NIST SP-800-22.

II. Opis urządzenia

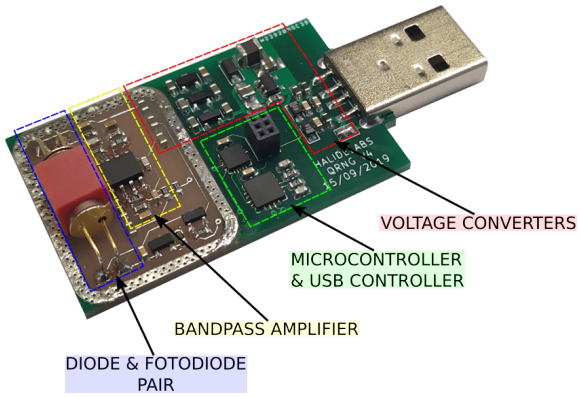
Największą zmianą w stosunku do poprzedniej iteracji było zastąpienie wzmacniacza transimpedancyjnego przekształtnikiem zmiennego prądu na zmienne napięcie składającego się z układu rezystora i kondensatora w układzie

filtru górnoprzepustowego. Spolaryzowana zaporowo fotodioda generuje fotoprąd zawierający szumy, które przenoszone przez kondensator blokujący składową stałą są wzmacniane i filtrowane. Selektywnie odfiltrowany szum śrutowy wprowadzany jest do mikrokontrolera realizującego funkcje próbkowania, analizowania i ekstraktownia entropii z sygnału. Rys. 1 przedstawia uproszczony schemat blokowy ekranowanej części fizycznej generującej szum śrutowy i część sprzętową mikrokontrolera odpowiedzialną za generację losowych liczb z uzyskanego szumu. Rys. 2 przedstawia finalne urządzenie z zaznaczonymi poszczególnymi blokami funkcjonalnymi.



Rysunek 1: *Schemat blokowy układu*

Podczas każdego uruchomienia urządzenia mikrokontroler wykonuje serię testów poprawności działania źródła szumu śrutowego. Najważniejszym warunkiem jest znacząco większa amplituda szumu zawierającego szum śrutowy (po włączeniu LED) niż szumu bazowego urządzenia. W celu testu tego warunku mikrokontroler próbkuje szum z wyłączoną i włączoną diodą elektroluminescencyjną, oblicza średnią sygnałów i ich odchylenie standardowe; które wykorzystuje do ustawienia przetwornika cyfrowo analogowego do którego porównywany jest szum za pomocą wbudowanego komparatora. Rys. 3 przedstawia uproszczony schemat potoku oprogramowania z warunkami startu generacji liczb i konfiguracji przetwornika cyfrowo analogowego.

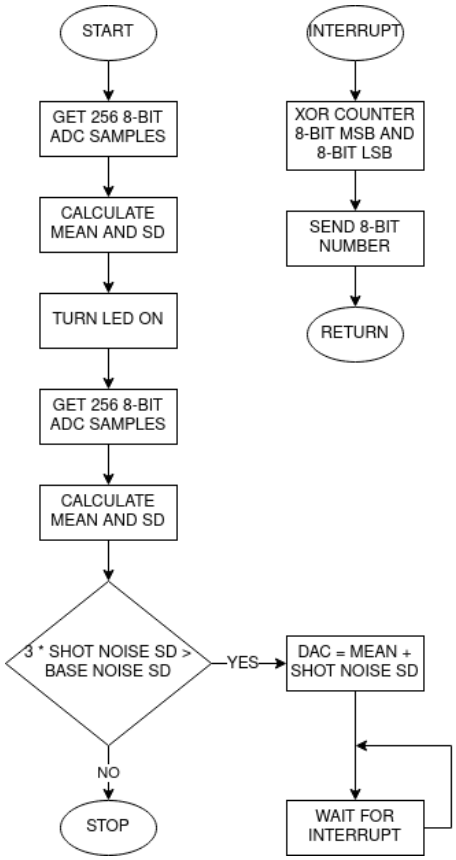


Rysunek 2: *Zdjęcie układu z zaznaczonymi poszczególnymi blokami funkcjonalnymi*

III. Wyniki

W celu testu generatora wygenerowano próbkę 2 GiB. Próbkę jak poprzednio poddano testom z użyciem pakietu NIST SP-800-22, dieharder oraz kilku innym narzędziom. Rys, 4 przedstawia histogram próbki o rozmiarze 100 MiB z którego wynika normalny rozkład generowanych liczb. Rys. 5 przedstawia bitmapę wielkości 256 x 256 px wykonaną z losowo wybranej próbki. Nie są widoczne żadne korelacje. Lis. 1, 2 i 3 przedstawiają skondensowany raport dotyczący wyników testów poszczególnych narzędzi. Dane generowane przez urządzenie spełniają wszystkie wymagania sprzętowego kryptograficznego generatora liczb losowych.

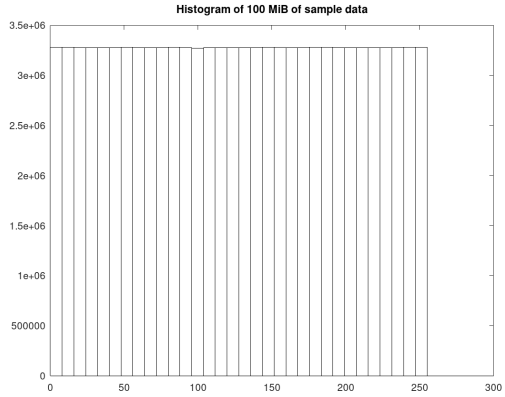
Pomyślnie zakończono budowę i testy kwantowego generatora liczb losowych wykorzystującego szum śrutowy jako źródło entropii. Zidentyfikowano potencjalne problemy w aktualnie stosowanych konkurencyjnych rozwiązaniach które będą przedmiotem osobnej pracy. W przyszłej pracy urządzenie zostanie poddane dalszej miniaturyzacji poprzez implementację rozwiązania w specjalizowanym ukła-



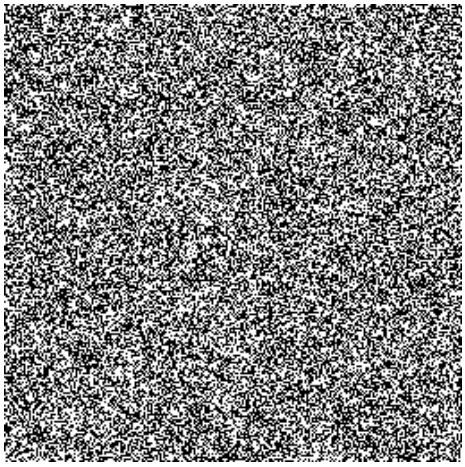
Rysunek 3: *Uproszczony schemat blokowy oprogramowania przedstawiający sekwencję startową urządzenia oraz sposób generacji liczb.*

dzie scalonym (ang. ASIC), co umożliwi tanią masową produkcję i implementację wewnątrz urządzeń wymagających źródła entropii o bardzo wysokiej jakości.

Próbka danych wielkości 2 GiB dostępna jest pod adresem: `https://halidelabs.eu/QRNG/data.bin`.



Rysunek 4: *Histogram próbki o rozmiarze 100 MiB.*



Rysunek 5: *Bitmapa wielkości 256 x 256 px.*

Listing 1: *Wynik testów z pakietu NIST SP-800-22.*

RESULTS FOR THE UNIFORMITY OF P–VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/data.bin> 1000000 bits sample size times 100

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P–VALUE	PROPORTION	STATISTICAL TEST
10	11	10	10	5	14	11	11	7	11	0.798139	100/100	Frequency
8	13	8	13	8	9	10	10	11	10	0.955835	99/100	BlockFrequency
10	11	11	9	6	13	3	15	10	12	0.304126	100/100	CumulativeSums
9	16	1	14	11	12	9	10	8	10	0.108791	100/100	CumulativeSums
5	14	9	15	4	14	12	11	7	9	0.145326	99/100	Runs
7	11	9	8	10	11	11	9	11	13	0.971699	99/100	LongestRun
5	8	12	12	10	6	7	12	15	13	0.350485	98/100	Rank
10	9	10	8	5	8	18	13	13	6	0.153763	100/100	FFT
11	12	11	9	10	11	8	8	15	5	0.678686	99/100	NonOverlappingTemplate
15	7	7	12	15	11	13	8	7	5	0.213309	99/100	NonOverlappingTemplate
16	14	9	4	8	10	7	8	9	15	0.153763	98/100	NonOverlappingTemplate
11	12	8	6	14	10	9	11	13	6	0.657933	98/100	NonOverlappingTemplate
11	8	8	11	10	17	10	7	9	9	0.637119	100/100	NonOverlappingTemplate
4	12	10	13	7	10	10	12	12	10	0.678686	100/100	NonOverlappingTemplate
5	9	15	4	13	19	11	7	10	7	0.020548	100/100	NonOverlappingTemplate
12	12	10	12	6	9	13	8	9	9	0.883171	97/100	NonOverlappingTemplate
11	7	10	10	15	8	9	11	11	8	0.867692	96/100	NonOverlappingTemplate
10	7	15	10	9	11	8	10	11	9	0.897763	100/100	NonOverlappingTemplate
12	14	7	13	9	15	7	8	9	6	0.401199	99/100	NonOverlappingTemplate
5	17	10	12	14	5	11	9	10	7	0.162606	100/100	NonOverlappingTemplate
11	8	16	6	6	12	8	7	13	13	0.289667	99/100	NonOverlappingTemplate
12	5	15	7	13	11	12	8	6	11	0.366918	99/100	NonOverlappingTemplate
13	8	8	10	11	10	8	8	9	15	0.816537	98/100	NonOverlappingTemplate
7	14	9	9	12	14	9	10	10	6	0.699313	100/100	NonOverlappingTemplate
6	15	14	7	11	2	8	11	10	16	0.045675	100/100	NonOverlappingTemplate
10	12	15	8	14	10	5	8	10	8	0.514124	96/100	NonOverlappingTemplate
13	8	8	10	15	11	9	11	6	9	0.719747	100/100	NonOverlappingTemplate
11	10	13	15	11	7	10	9	6	8	0.678686	100/100	NonOverlappingTemplate
13	8	10	9	12	10	11	9	10	8	0.983453	99/100	NonOverlappingTemplate
8	12	7	13	12	8	10	3	12	15	0.262249	100/100	NonOverlappingTemplate
10	9	9	15	17	3	11	7	6	13	0.066882	100/100	NonOverlappingTemplate
12	6	9	10	11	13	10	9	10	10	0.955835	99/100	NonOverlappingTemplate
5	12	6	13	5	15	14	13	7	10	0.129620	100/100	NonOverlappingTemplate
10	10	12	9	11	13	11	9	8	7	0.964295	100/100	NonOverlappingTemplate
11	12	12	8	9	12	15	4	9	8	0.494392	98/100	NonOverlappingTemplate
10	9	15	9	5	12	14	8	13	5	0.275709	97/100	NonOverlappingTemplate
6	6	17	16	11	4	8	11	13	8	0.045675	99/100	NonOverlappingTemplate
7	11	13	6	12	11	8	11	11	10	0.867692	100/100	NonOverlappingTemplate
12	16	11	7	8	10	6	7	10	13	0.455937	97/100	NonOverlappingTemplate
9	8	9	10	13	7	11	10	6	17	0.437274	99/100	NonOverlappingTemplate
7	13	6	9	11	7	13	16	8	10	0.401199	100/100	NonOverlappingTemplate
16	12	8	10	9	12	6	11	10	6	0.514124	97/100	NonOverlappingTemplate
6	12	11	9	10	13	7	9	13	10	0.834308	100/100	NonOverlappingTemplate
7	5	8	9	16	7	15	14	9	10	0.181557	97/100	NonOverlappingTemplate
14	7	6	10	5	11	15	11	10	11	0.401199	99/100	NonOverlappingTemplate
14	10	7	12	10	12	10	6	7	12	0.719747	99/100	NonOverlappingTemplate
8	7	16	5	8	10	3	12	15	16	0.023545	98/100	NonOverlappingTemplate
11	11	10	9	12	15	3	10	9	10	0.514124	98/100	NonOverlappingTemplate
8	8	13	10	10	15	7	11	11	7	0.719747	98/100	NonOverlappingTemplate
3	12	11	13	10	11	14	7	12	7	0.334538	98/100	NonOverlappingTemplate
13	14	9	7	9	11	10	11	8	8	0.867692	99/100	NonOverlappingTemplate
7	9	8	11	16	6	13	9	10	11	0.554420	100/100	NonOverlappingTemplate

8	8	5	6	10	7	21	15	7	13	0.008266	100/100		NonOverlappingTemplate
14	11	10	8	11	6	7	7	14	12	0.574903	99/100		NonOverlappingTemplate
12	12	16	13	3	2	13	6	17	6	0.002374	98/100		NonOverlappingTemplate
11	8	8	10	10	12	13	9	9	10	0.983453	99/100		NonOverlappingTemplate
13	8	12	10	10	8	10	7	9	13	0.911413	97/100		NonOverlappingTemplate
14	6	11	14	11	9	8	8	10	9	0.739918	100/100		NonOverlappingTemplate
9	8	12	14	10	8	10	10	9	10	0.964295	99/100		NonOverlappingTemplate
8	15	8	12	12	6	8	7	12	12	0.554420	99/100		NonOverlappingTemplate
12	10	14	12	5	9	10	8	14	6	0.474986	97/100		NonOverlappingTemplate
7	9	8	11	14	10	13	10	12	6	0.739918	100/100		NonOverlappingTemplate
12	9	14	8	11	8	10	7	11	10	0.911413	99/100		NonOverlappingTemplate
15	8	9	11	9	9	8	9	10	12	0.897763	98/100		NonOverlappingTemplate
10	7	12	14	12	14	8	3	9	11	0.319084	100/100		NonOverlappingTemplate
7	8	16	12	8	8	14	13	6	8	0.304126	98/100		NonOverlappingTemplate
5	10	13	4	15	8	7	9	13	16	0.080519	100/100		NonOverlappingTemplate
6	11	9	9	3	15	9	15	9	14	0.137282	100/100		NonOverlappingTemplate
12	8	8	8	12	14	9	6	9	14	0.637119	100/100		NonOverlappingTemplate
10	9	11	13	14	11	7	8	6	11	0.759756	97/100		NonOverlappingTemplate
15	7	11	13	12	7	10	9	9	7	0.657933	95/100	*	NonOverlappingTemplate
7	16	9	10	9	9	12	11	6	11	0.637119	98/100		NonOverlappingTemplate
5	8	9	12	15	10	12	9	11	9	0.678686	99/100		NonOverlappingTemplate
6	8	12	8	12	13	12	11	9	9	0.851383	100/100		NonOverlappingTemplate
6	9	16	10	10	14	8	5	12	10	0.334538	99/100		NonOverlappingTemplate
12	12	12	11	10	10	6	11	10	6	0.867692	99/100		NonOverlappingTemplate
4	13	12	12	13	7	5	11	12	11	0.334538	98/100		NonOverlappingTemplate
12	13	6	9	13	7	9	6	13	12	0.554420	99/100		NonOverlappingTemplate
13	6	7	10	14	7	14	10	10	9	0.574903	99/100		NonOverlappingTemplate
14	2	7	10	11	8	13	5	16	14	0.035174	98/100		NonOverlappingTemplate
8	7	10	11	9	13	10	9	13	10	0.946308	99/100		NonOverlappingTemplate
9	15	15	15	8	6	6	8	12	6	0.137282	100/100		NonOverlappingTemplate
11	12	11	9	10	11	8	8	15	5	0.678686	99/100		NonOverlappingTemplate
16	11	8	5	13	10	8	13	9	7	0.366918	99/100		NonOverlappingTemplate
10	10	11	13	10	5	8	12	11	10	0.883171	100/100		NonOverlappingTemplate
8	9	6	9	10	11	7	15	12	13	0.637119	100/100		NonOverlappingTemplate
11	14	4	11	8	6	11	13	8	14	0.319084	100/100		NonOverlappingTemplate
14	12	7	10	12	7	8	9	11	10	0.851383	99/100		NonOverlappingTemplate
9	11	10	7	7	9	16	11	8	12	0.678686	100/100		NonOverlappingTemplate
8	10	8	13	11	15	7	6	5	17	0.115387	98/100		NonOverlappingTemplate
9	7	13	6	13	12	11	6	14	9	0.514124	99/100		NonOverlappingTemplate
8	6	10	13	17	9	13	9	6	9	0.304126	99/100		NonOverlappingTemplate
11	7	12	5	13	10	5	5	17	15	0.045675	100/100		NonOverlappingTemplate
7	9	12	9	13	9	10	8	13	10	0.924076	99/100		NonOverlappingTemplate
10	7	9	12	7	9	9	13	12	12	0.897763	99/100		NonOverlappingTemplate
16	12	9	10	4	7	8	11	14	9	0.289667	97/100		NonOverlappingTemplate
9	11	10	10	10	6	12	12	9	11	0.971699	99/100		NonOverlappingTemplate
15	11	12	7	6	10	12	8	10	9	0.699313	98/100		NonOverlappingTemplate
13	13	13	7	9	7	15	5	11	7	0.304126	99/100		NonOverlappingTemplate
9	12	8	11	8	10	12	12	7	11	0.955835	98/100		NonOverlappingTemplate
11	13	10	12	13	14	8	7	8	4	0.419021	100/100		NonOverlappingTemplate
9	7	12	10	11	8	14	10	8	11	0.911413	100/100		NonOverlappingTemplate
9	9	12	15	13	10	9	4	7	12	0.437274	100/100		NonOverlappingTemplate
10	10	7	8	12	8	15	8	8	14	0.637119	100/100		NonOverlappingTemplate
13	5	16	12	13	7	12	9	8	5	0.181557	98/100		NonOverlappingTemplate
15	12	18	6	11	10	3	9	5	11	0.028817	100/100		NonOverlappingTemplate
16	15	9	6	6	13	10	6	8	11	0.191687	98/100		NonOverlappingTemplate
10	9	13	9	15	9	8	8	10	9	0.867692	99/100		NonOverlappingTemplate
11	11	8	7	9	8	11	11	13	11	0.955835	98/100		NonOverlappingTemplate
7	7	15	10	3	14	15	7	11	11	0.108791	99/100		NonOverlappingTemplate
8	13	6	9	13	6	11	9	11	14	0.595549	99/100		NonOverlappingTemplate
9	11	9	13	10	6	13	11	10	8	0.897763	100/100		NonOverlappingTemplate
5	10	15	10	9	3	7	10	20	11	0.012650	100/100		NonOverlappingTemplate

13	12	10	8	8	10	10	10	5	14	0.719747	99/100	NonOverlappingTemplate
10	7	9	13	9	11	11	6	12	12	0.867692	98/100	NonOverlappingTemplate
8	11	10	8	14	6	11	17	9	6	0.289667	99/100	NonOverlappingTemplate
8	7	7	13	12	8	13	14	9	9	0.678686	99/100	NonOverlappingTemplate
7	8	12	14	5	15	8	8	13	10	0.350485	99/100	NonOverlappingTemplate
9	14	9	6	11	8	7	12	15	9	0.554420	100/100	NonOverlappingTemplate
6	10	14	9	8	9	14	10	10	10	0.798139	99/100	NonOverlappingTemplate
8	8	13	9	6	6	15	13	12	10	0.455937	99/100	NonOverlappingTemplate
11	11	11	13	5	12	8	9	7	13	0.699313	100/100	NonOverlappingTemplate
10	11	12	12	6	13	11	8	10	7	0.851383	97/100	NonOverlappingTemplate
11	8	7	10	12	12	7	9	12	12	0.911413	100/100	NonOverlappingTemplate
5	6	13	12	7	16	12	11	7	11	0.249284	100/100	NonOverlappingTemplate
12	8	9	8	7	13	13	12	9	9	0.867692	99/100	NonOverlappingTemplate
8	11	10	15	12	9	6	10	10	9	0.816537	100/100	NonOverlappingTemplate
6	7	12	13	13	13	8	8	9	11	0.678686	100/100	NonOverlappingTemplate
8	11	9	10	13	9	13	9	6	12	0.867692	100/100	NonOverlappingTemplate
8	10	13	9	7	11	17	4	7	14	0.145326	99/100	NonOverlappingTemplate
5	5	10	10	10	11	11	6	13	19	0.071177	99/100	NonOverlappingTemplate
12	8	18	5	9	6	13	7	7	15	0.055361	99/100	NonOverlappingTemplate
9	7	11	6	5	17	8	10	12	15	0.145326	100/100	NonOverlappingTemplate
8	4	10	7	6	17	12	9	12	15	0.096578	98/100	NonOverlappingTemplate
8	10	8	10	20	4	9	11	12	8	0.080519	100/100	NonOverlappingTemplate
9	3	7	12	5	14	9	13	14	14	0.102526	99/100	NonOverlappingTemplate
5	17	10	13	9	5	13	11	8	9	0.191687	100/100	NonOverlappingTemplate
8	7	14	18	7	13	11	6	10	6	0.108791	99/100	NonOverlappingTemplate
12	12	12	7	9	8	13	10	8	9	0.911413	98/100	NonOverlappingTemplate
11	7	8	6	11	11	15	9	10	12	0.719747	97/100	NonOverlappingTemplate
16	8	10	8	7	10	13	10	10	8	0.678686	99/100	NonOverlappingTemplate
11	8	10	8	14	11	9	8	11	10	0.955835	97/100	NonOverlappingTemplate
8	12	9	9	9	10	10	16	11	6	0.699313	100/100	NonOverlappingTemplate
13	12	5	9	7	11	13	9	9	12	0.699313	97/100	NonOverlappingTemplate
12	15	8	10	9	9	8	11	9	9	0.897763	99/100	NonOverlappingTemplate
9	14	9	10	11	7	10	9	11	10	0.964295	100/100	NonOverlappingTemplate
7	10	9	9	12	12	11	9	13	8	0.946308	100/100	NonOverlappingTemplate
12	8	10	6	10	12	13	5	12	12	0.637119	99/100	NonOverlappingTemplate
11	7	10	12	10	9	14	11	5	11	0.759756	99/100	NonOverlappingTemplate
11	4	11	12	13	5	12	8	13	11	0.401199	100/100	NonOverlappingTemplate
10	7	11	7	8	8	14	14	13	8	0.616305	98/100	NonOverlappingTemplate
10	14	7	15	8	6	13	9	6	12	0.350485	99/100	NonOverlappingTemplate
11	9	12	12	5	11	12	10	11	7	0.834308	99/100	NonOverlappingTemplate
8	10	8	14	7	14	13	9	10	7	0.657933	100/100	NonOverlappingTemplate
14	13	12	12	2	8	8	9	12	10	0.275709	98/100	NonOverlappingTemplate
9	15	15	15	8	6	6	8	12	6	0.137282	100/100	NonOverlappingTemplate
6	10	10	12	12	8	12	10	6	14	0.699313	99/100	OverlappingTemplate
10	9	11	15	9	11	3	8	11	13	0.419021	100/100	Universal
8	8	13	12	6	13	12	9	7	12	0.699313	99/100	ApproximateEntropy
5	3	7	5	4	5	10	6	13	9	0.086458	67/67	RandomExcursions
11	4	5	2	10	9	8	7	5	6	0.170294	66/67	RandomExcursions
5	7	8	7	8	6	3	11	5	7	0.551026	67/67	RandomExcursions
6	7	5	8	11	8	5	4	5	8	0.585209	66/67	RandomExcursions
5	10	5	6	10	3	7	8	6	7	0.517442	67/67	RandomExcursions
8	5	9	5	7	8	4	8	11	2	0.242986	64/67	RandomExcursions
3	8	12	7	6	5	5	10	6	5	0.242986	67/67	RandomExcursions
9	7	6	5	6	8	6	6	10	4	0.756476	66/67	RandomExcursions
4	4	9	11	7	7	1	8	7	9	0.128379	66/67	RandomExcursionsVariant
5	6	3	11	7	8	8	3	4	12	0.078086	66/67	RandomExcursionsVariant
5	4	8	8	5	7	12	5	6	7	0.452799	66/67	RandomExcursionsVariant
6	6	5	8	10	4	10	5	5	8	0.551026	67/67	RandomExcursionsVariant
6	6	7	8	7	6	7	8	8	4	0.957319	66/67	RandomExcursionsVariant
8	3	7	7	7	9	8	3	6	9	0.551026	66/67	RandomExcursionsVariant
7	1	7	7	5	6	9	14	2	9	0.011931	67/67	RandomExcursionsVariant

```
  6   6   4   5   8   9   7   7   8   7  0.900104     67/67     RandomExcursionsVariant
 10   4   5   7   9   4   9  10   6   3  0.242986     67/67     RandomExcursionsVariant
  6   3   4   8  10   8   9   4   4  11  0.155209     67/67     RandomExcursionsVariant
  5   7   4   9   3   7   9   5  10   8  0.422034     67/67     RandomExcursionsVariant
  3  10   9   3   4  10   3   6   7  12  0.033288     67/67     RandomExcursionsVariant
  3   5  13   5   6   2  15   5   8   5  0.001313     67/67     RandomExcursionsVariant
  6   7   8   5   9  10   7   7   3   5  0.619772     67/67     RandomExcursionsVariant
 10   6   5   8   9   8   6   2   7   6  0.484646     67/67     RandomExcursionsVariant
 11   7   9   2   8   4   1   5  11   9  0.018969     66/67     RandomExcursionsVariant
  6  10   9   6   3   5   7  10   6   5  0.452799     66/67     RandomExcursionsVariant
  8   8   8   3   7   2   5  12   8   6  0.155209     66/67     RandomExcursionsVariant
  8   8  16   6   6  10  17   7  10  12  0.129620    100/100    Serial
 10  12   4   7   9   6  13  10  23   6  0.002043    100/100    Serial
 11  14  11   5   5  10  14  12  10   8  0.419021     99/100    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 = 63 for a sample size = 67 binary sequences.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Listing 2: *Wynik testów z pakietu dieharder.*

```
#==========================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown       #
#==========================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|                       data.bin |  2.89e+07  |
#==========================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#==========================================================================#
   diehard_birthdays|  0|       100|     100|0.60051170|  PASSED
      diehard_operm5|  0|   1000000|     100|0.97500007|  PASSED
  diehard_rank_32x32|  0|     40000|     100|0.91323452|  PASSED
    diehard_rank_6x8|  0|    100000|     100|0.20150330|  PASSED
   diehard_bitstream|  0|   2097152|     100|0.52444005|  PASSED
        diehard_opso|  0|   2097152|     100|0.55268288|  PASSED
        diehard_oqso|  0|   2097152|     100|0.31433466|  PASSED
         diehard_dna|  0|   2097152|     100|0.02870652|  PASSED
diehard_count_1s_str|  0|    256000|     100|0.89128121|  PASSED
diehard_count_1s_byt|  0|    256000|     100|0.17830673|  PASSED
 diehard_parking_lot|  0|     12000|     100|0.90999882|  PASSED
    diehard_2dsphere|  2|      8000|     100|0.03045671|  PASSED
    diehard_3dsphere|  3|      4000|     100|0.09232689|  PASSED
     diehard_squeeze|  0|    100000|     100|0.73508382|  PASSED
        diehard_sums|  0|       100|     100|0.32859051|  PASSED
        diehard_runs|  0|    100000|     100|0.39448969|  PASSED
        diehard_runs|  0|    100000|     100|0.91979270|  PASSED
       diehard_craps|  0|    200000|     100|0.63592245|  PASSED
       diehard_craps|  0|    200000|     100|0.99705343|   WEAK
 marsaglia_tsang_gcd|  0|  10000000|     100|0.89785836|  PASSED
 marsaglia_tsang_gcd|  0|  10000000|     100|0.90694936|  PASSED
         sts_monobit|  1|    100000|     100|0.88611040|  PASSED
            sts_runs|  2|    100000|     100|0.88636360|  PASSED
          sts_serial|  1|    100000|     100|0.69514952|  PASSED
          sts_serial|  2|    100000|     100|0.65066530|  PASSED
          sts_serial|  3|    100000|     100|0.98477641|  PASSED
          sts_serial|  3|    100000|     100|0.93570553|  PASSED
```

sts_serial	4	100000	100	0.36790727	PASSED
sts_serial	4	100000	100	0.43119210	PASSED
sts_serial	5	100000	100	0.77091411	PASSED
sts_serial	5	100000	100	0.93215225	PASSED
sts_serial	6	100000	100	0.49537143	PASSED
sts_serial	6	100000	100	0.12735839	PASSED
sts_serial	7	100000	100	0.66858983	PASSED
sts_serial	7	100000	100	0.46903469	PASSED
sts_serial	8	100000	100	0.72869342	PASSED
sts_serial	8	100000	100	0.84368973	PASSED
sts_serial	9	100000	100	0.97343461	PASSED
sts_serial	9	100000	100	0.70326584	PASSED
sts_serial	10	100000	100	0.68757847	PASSED
sts_serial	10	100000	100	0.88008633	PASSED
sts_serial	11	100000	100	0.62658582	PASSED
sts_serial	11	100000	100	0.97527660	PASSED
sts_serial	12	100000	100	0.75728176	PASSED
sts_serial	12	100000	100	0.70454659	PASSED
sts_serial	13	100000	100	0.58688663	PASSED
sts_serial	13	100000	100	0.22544542	PASSED
sts_serial	14	100000	100	0.92448547	PASSED
sts_serial	14	100000	100	0.10628221	PASSED
sts_serial	15	100000	100	0.10422121	PASSED
sts_serial	15	100000	100	0.06270602	PASSED
sts_serial	16	100000	100	0.47988228	PASSED
sts_serial	16	100000	100	0.58138571	PASSED
rgb_bitdist	1	100000	100	0.75291211	PASSED
rgb_bitdist	2	100000	100	0.70573197	PASSED
rgb_bitdist	3	100000	100	0.17255477	PASSED
rgb_bitdist	4	100000	100	0.72698824	PASSED
rgb_bitdist	5	100000	100	0.92965714	PASSED
rgb_bitdist	6	100000	100	0.95980790	PASSED
rgb_bitdist	7	100000	100	0.44217394	PASSED
rgb_bitdist	8	100000	100	0.56533812	PASSED
rgb_bitdist	9	100000	100	0.95363509	PASSED
rgb_bitdist	10	100000	100	0.78010739	PASSED
rgb_bitdist	11	100000	100	0.49712631	PASSED
rgb_bitdist	12	100000	100	0.58114274	PASSED
rgb_minimum_distance	2	10000	1000	0.14633759	PASSED
rgb_minimum_distance	3	10000	1000	0.29147111	PASSED
rgb_minimum_distance	4	10000	1000	0.41460656	PASSED
rgb_minimum_distance	5	10000	1000	0.41332874	PASSED
rgb_permutations	2	100000	100	0.87640614	PASSED
rgb_permutations	3	100000	100	0.90191973	PASSED
rgb_permutations	4	100000	100	0.48251261	PASSED
rgb_permutations	5	100000	100	0.32495343	PASSED
rgb_lagged_sum	0	1000000	100	0.14977844	PASSED
rgb_lagged_sum	1	1000000	100	0.16925441	PASSED
rgb_lagged_sum	2	1000000	100	0.82534744	PASSED
rgb_lagged_sum	3	1000000	100	0.77897152	PASSED
rgb_lagged_sum	4	1000000	100	0.38030521	PASSED
rgb_lagged_sum	5	1000000	100	0.99740807	WEAK
rgb_lagged_sum	6	1000000	100	0.53543136	PASSED
rgb_lagged_sum	7	1000000	100	0.12236663	PASSED
rgb_lagged_sum	8	1000000	100	0.14445512	PASSED
rgb_lagged_sum	9	1000000	100	0.42429361	PASSED
rgb_lagged_sum	10	1000000	100	0.83658043	PASSED
rgb_lagged_sum	11	1000000	100	0.00346929	WEAK
rgb_lagged_sum	12	1000000	100	0.94449173	PASSED
rgb_lagged_sum	13	1000000	100	0.63923470	PASSED
rgb_lagged_sum	14	1000000	100	0.98479596	PASSED

```
      rgb_lagged_sum|  15|   1000000|      100|0.06141705|  PASSED
      rgb_lagged_sum|  16|   1000000|      100|0.83700121|  PASSED
      rgb_lagged_sum|  17|   1000000|      100|0.50267624|  PASSED
      rgb_lagged_sum|  18|   1000000|      100|0.38051886|  PASSED
      rgb_lagged_sum|  19|   1000000|      100|0.68032691|  PASSED
      rgb_lagged_sum|  20|   1000000|      100|0.81007207|  PASSED
      rgb_lagged_sum|  21|   1000000|      100|0.33236621|  PASSED
      rgb_lagged_sum|  22|   1000000|      100|0.41150631|  PASSED
      rgb_lagged_sum|  23|   1000000|      100|0.04839325|  PASSED
      rgb_lagged_sum|  24|   1000000|      100|0.57240490|  PASSED
      rgb_lagged_sum|  25|   1000000|      100|0.20466249|  PASSED
      rgb_lagged_sum|  26|   1000000|      100|0.17603521|  PASSED
      rgb_lagged_sum|  27|   1000000|      100|0.87819636|  PASSED
      rgb_lagged_sum|  28|   1000000|      100|0.89304522|  PASSED
      rgb_lagged_sum|  29|   1000000|      100|0.91222017|  PASSED
      rgb_lagged_sum|  30|   1000000|      100|0.59190888|  PASSED
      rgb_lagged_sum|  31|   1000000|      100|0.01853238|  PASSED
      rgb_lagged_sum|  32|   1000000|      100|0.97387055|  PASSED
     rgb_kstest_test|   0|     10000|     1000|0.05918341|  PASSED
     dab_bytedistrib|   0|  51200000|        1|0.28445837|  PASSED
             dab_dct| 256|     50000|        1|0.35328651|  PASSED
Preparing to run test 207.  ntuple = 0
        dab_filltree|  32|  15000000|        1|0.52303780|  PASSED
        dab_filltree|  32|  15000000|        1|0.73098748|  PASSED
Preparing to run test 208.  ntuple = 0
       dab_filltree2|   0|   5000000|        1|0.43543928|  PASSED
       dab_filltree2|   1|   5000000|        1|0.50795861|  PASSED
Preparing to run test 209.  ntuple = 0
        dab_monobit2|  12|  65000000|        1|0.26259528|  PASSED
```

Listing 3: *Wynik testów z pakietu linux-ent.*

```
Entropy = 8.000000 bits per byte.

Optimum compression would reduce the size
of this 2064385896 byte file by 0 percent.

Chi square distribution for 2064385896 samples is 255.90, and randomly
would exceed this value 47.23 percent of the times.

Arithmetic mean value of data bytes is 127.5014 (127.5 = random).
Monte Carlo value for Pi is 3.141579925 (error 0.00 percent).
Serial correlation coefficient is -0.000035 (totally uncorrelated = 0.0).
```