LABORATORIUM BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH (CZ. 1)

Wykonali:

Jakub Kamiński, Emil Lewandowski

Data oddania
15.05.2025

Podstawa opracowania:

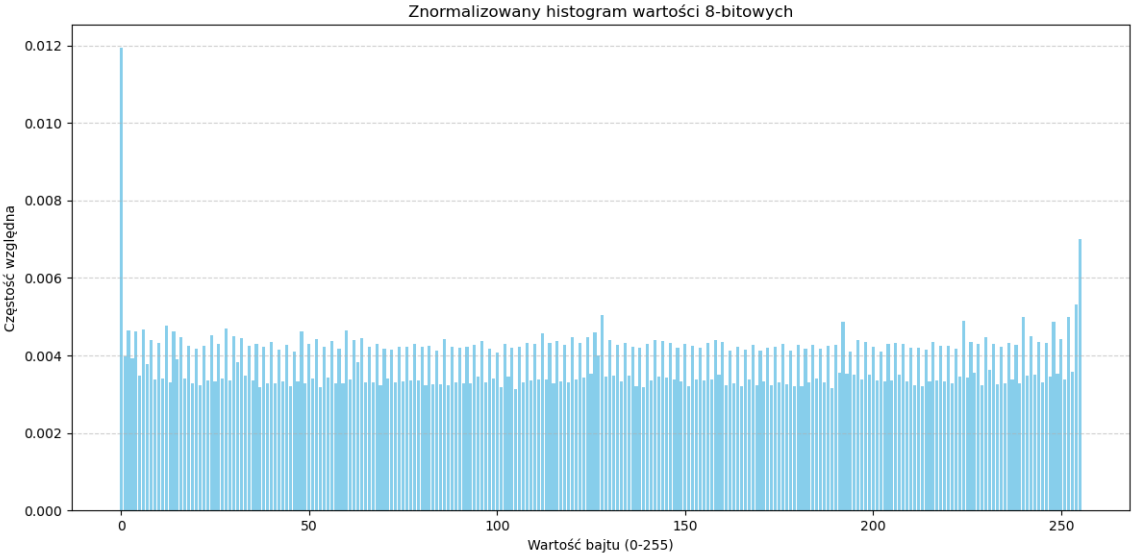
Y. Chen et al., "LETRNG—A Lightweight and Efficient True Random Number Generator for GNU/Linux Systems," in Tsinghua Science and Technology, vol. 28, no. 2, pp. 370-385, April 2023

Systematyczny przegląd literatury:

1. baza danych IEEE Xplore,
2. słowa kluczowe: TRNG, True Random Number Generator, PC, ubuntu
3. okres publikacji: 2020-2025,
4. Wybrane podejście: wykorzystanie warunku wyścigu pomiędzy wątkami w języku C++ jako źródła entropii.

Analiza źródła entropii:

Źródłem entropii w zaimplementowanym generatorze TRNG jest niedeterministyczne zachowanie harmonogramu (scheduler'a) systemu operacyjnego, które ujawnia się w warunkach race condition między współbieżnymi wątkami. Dwa wątki (threadA i threadB) modyfikują zmienną coin, zapisując do niej na przemian wartości 0 i 1. Równolegle inne wątki (samplerX i samplerY) w bardzo szybkim tempie odczytują tę zmienną. Z uwagi na brak synchronizacji i ogromną szybkość działania, nie można przewidzieć, czy dany odczyt pochodzi od zapisu z wątku A, czy z B.



Entropia wyliczona zgodnie ze wzorem: $e = -\sum_i p_i log_2(p_i)$, dla powyższego rozkładu wynosi **7,977** bita.

Wyniki testu statystycznego NIST 800-22

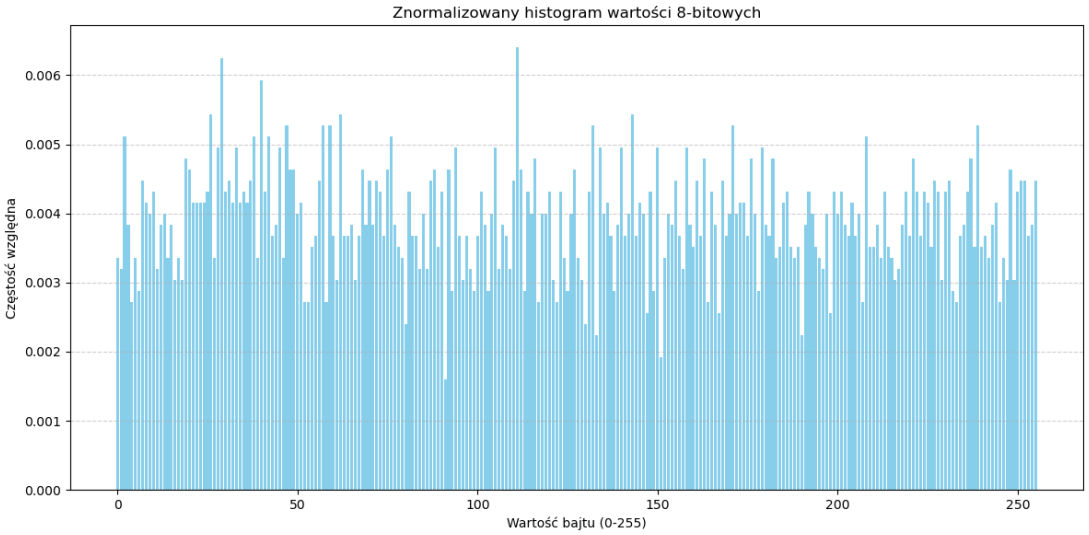
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE		PROPORTION		STATISTICAL TEST
9	1	2	4	3	4	5	1	6	5	0.141256		36/40	*	Frequency
7	7	0	2	3	3	6	5	3	4	0.242986		34/40	*	BlockFrequency
10	4	0	3	2	6	4	4	3	4	0.078086		37/40		CumulativeSums
10	1	3	1	3	7	3	7	3	2	0.017912		36/40	*	CumulativeSums
12	5	3	7	3	2	4	2	1	1	0.002465		36/40	*	Runs
8	5	4	5	5	3	3	3	3	1	0.534146		39/40		LongestRun
40	0	0	0	0	0	0	0	0	0	0.000000	*	0/40	*	Rank
8	3	3	5	0	10	0	8	0	3	0.000439		39/40		FFT
11	2	2	7	0	0	9	0	9	0	0.000001	*	36/40	*	NonOverlappingTemplate
7	1	5	7	0	0	8	0	7	5	0.002465		37/40		NonOverlappingTemplate
6	0	1	7	0	0	11	0	7	8	0.000008	*	39/40		NonOverlappingTemplate
8	1	3	6	0	0	6	0	12	4	0.000032	*	38/40		NonOverlappingTemplate
3	2	0	5	0	0	13	0	9	8	0.000000	*	40/40		NonOverlappingTemplate
10	0	0	5	0	0	6	0	11	8	0.000000	*	38/40		NonOverlappingTemplate
10	0	1	7	0	0	6	0	7	9	0.000012	*	38/40		NonOverlappingTemplate
12	1	2	2	0	0	10	0	6	7	0.000001	*	36/40	*	NonOverlappingTemplate
8	1	3	7	0	0	8	0	8	5	0.000648		38/40		NonOverlappingTemplate
7	0	1	6	0	0	10	0	10	6	0.000006	*	38/40		NonOverlappingTemplate
6	0	2	5	0	0	11	0	10	6	0.000006	*	37/40		NonOverlappingTemplate
6	0	1	10	0	0	7	0	10	6	0.000006	*	39/40		NonOverlappingTemplate
6	0	0	3	0	0	8	0	17	6	0.000000	*	38/40		NonOverlappingTemplate
2	1	2	7	0	0	5	0	14	9	0.000000	*	40/40		NonOverlappingTemplate
6	1	1	3	0	0	13	0	13	3	0.000000	*	39/40		NonOverlappingTemplate
8	0	3	5	0	0	11	0	11	2	0.000001	*	37/40		NonOverlappingTemplate
10	0	1	11	0	0	7	0	5	6	0.000002	*	38/40		NonOverlappingTemplate
9	0	0	4	0	0	10	0	13	4	0.000000	*	39/40		NonOverlappingTemplate
7	0	2	4	0	0	11	0	11	5	0.000001	*	38/40		NonOverlappingTemplate
3	0	2	3	0	0	13	0	16	3	0.000000	*	39/40		NonOverlappingTemplate
6	0	2	3	0	0	10	0	10	9	0.000003	*	38/40		NonOverlappingTemplate
3	0	2	5	0	0	8	0	12	10	0.000000	*	39/40		NonOverlappingTemplate
10	1	1	5	0	0	8	0	9	6	0.000026	*	37/40		NonOverlappingTemplate
6	1	0	5	0	0	7	0	14	7	0.000000	*	37/40		NonOverlappingTemplate
9	0	3	6	0	0	9	0	12	1	0.000000	*	38/40		NonOverlappingTemplate
3	1	1	3	0	0	12	0	11	9	0.000000	*	39/40		NonOverlappingTemplate

```
 6   0   2   3   0   0   9   0  14   6  0.000000 *   39/40       NonOverlappingTemplate
 6   1   2   7   0   0  10   0  11   3  0.000008 *   39/40       NonOverlappingTemplate
13   1   0   3   0   0   8   0   9   6  0.000000 *   38/40       NonOverlappingTemplate
 6   1   1   2   0   0   6   0  17   7  0.000000 *   39/40       NonOverlappingTemplate
 8   0   0   5   0   0  10   0  11   6  0.000000 *   38/40       NonOverlappingTemplate
 2   0   2   5   0   0   8   0  16   7  0.000000 *   40/40       NonOverlappingTemplate
 6   0   0   4   0   0  11   0  11   8  0.000000 *   40/40       NonOverlappingTemplate
 3   1   3   4   0   0   8   0  14   7  0.000001 *   40/40       NonOverlappingTemplate
 4   0   0   6   0   0  11   0  11   8  0.000000 *   40/40       NonOverlappingTemplate
 9   0   0   2   0   0  12   0  12   5  0.000000 *   40/40       NonOverlappingTemplate
 4   0   0   5   0   0  11   0  11   9  0.000000 *   40/40       NonOverlappingTemplate
 6   0   1   8   0   0  13   0   9   3  0.000000 *   38/40       NonOverlappingTemplate
 4   0   1   7   0   0   8   0  12   8  0.000001 *   39/40       NonOverlappingTemplate
 6   0   3   5   0   0  11   0   8   7  0.000040 *   39/40       NonOverlappingTemplate
 4   0   3   7   0   0   6   0  11   9  0.000017 *   38/40       NonOverlappingTemplate
 6   0   1   4   0   0  13   0   8   8  0.000000 *   38/40       NonOverlappingTemplate
 4   1   3   4   0   0  10   0  15   3  0.000000 *   40/40       NonOverlappingTemplate
 9   0   1   1   0   0  14   0  12   3  0.000000 *   38/40       NonOverlappingTemplate
 7   0   0   6   0   0  11   0  12   4  0.000000 *   38/40       NonOverlappingTemplate
 9   0   1   3   0   0   7   0  12   8  0.000000 *   37/40       NonOverlappingTemplate
 4   0   2   5   0   0   9   0  14   6  0.000000 *   38/40       NonOverlappingTemplate
 6   0   0   3   0   0  12   0  10   9  0.000000 *   40/40       NonOverlappingTemplate
 8   0   0   3   0   0   9   0  11   9  0.000000 *   38/40       NonOverlappingTemplate
 8   0   1   7   0   0  11   0   6   7  0.000008 *   39/40       NonOverlappingTemplate
 5   0   0   5   0   0  14   0   9   7  0.000000 *   39/40       NonOverlappingTemplate
 6   0   0   3   0   0   8   0  13  10  0.000000 *   40/40       NonOverlappingTemplate
 3   0   2   7   0   0  14   0  11   3  0.000000 *   40/40       NonOverlappingTemplate
 9   1   3   4   0   0  10   0  11   2  0.000002 *   37/40       NonOverlappingTemplate
 7   0   0   4   0   0  10   0  16   3  0.000000 *   39/40       NonOverlappingTemplate
 3   0   2   4   0   0  12   0  12   7  0.000000 *   40/40       NonOverlappingTemplate
 3   0   0   7   0   0  13   0  12   5  0.000000 *   40/40       NonOverlappingTemplate
 4   0   2   6   0   0   8   0  11   9  0.000006 *   40/40       NonOverlappingTemplate
 5   0   1   5   0   0  10   0  10   9  0.000002 *   40/40       NonOverlappingTemplate
 5   0   2   4   0   0   9   0  12   8  0.000002 *   40/40       NonOverlappingTemplate
 6   0   0   8   0   0   8   0  13   5  0.000000 *   39/40       NonOverlappingTemplate
 7   0   2   4   0   0  15   0   9   3  0.000000 *   40/40       NonOverlappingTemplate
 3   0   1   3   0   0  12   0  14   7  0.000000 *   38/40       NonOverlappingTemplate
 5   0   2   6   0   0   7   0   9  11  0.000012 *   39/40       NonOverlappingTemplate
 6   0   1   5   0   0   8   0  12   8  0.000002 *   40/40       NonOverlappingTemplate
 6   1   3   5   0   0   7   0  14   4  0.000002 *   37/40       NonOverlappingTemplate
 4   0   0   5   0   0  10   0  12   9  0.000000 *   39/40       NonOverlappingTemplate
```

Metoda poprawy właściwości statystycznych:

W naszym TRNG bazującym na race condition, wątki próbkujące (samplerX i samplerY) odczytują wartości zapisywane przez dwa niezależne wątki (threadA, threadB). Z tych odczytów składane są dwie 64-bitowe próbki, z których każda składana jest do pojedynczego bitu za pomocą funkcji fold_bits() (operacja XOR na wszystkich 64 bitach). Następnie te dwa bity są przekazywane do funkcji fair_coin(), która implementuje opisany wyżej algorytm von Neumanna. Zasada działania metody opiera się na analizie kolejnych par bitów generowanych przez generator:

-Jeśli para to 00 lub 11 – odrzucamy (bo nie wiadomo, który bit miał pierwszeństwo),
-Jeśli para to 01 – wynikowy bit to 0,
-Jeśli para to 10 – wynikowy bit to 1.



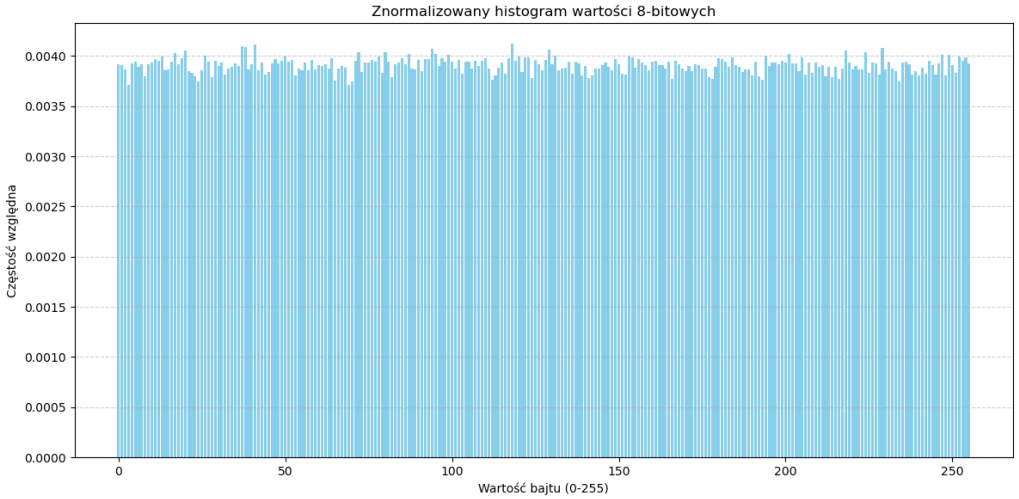
Entropia wyliczona zgodnie ze wzorem: $e = -\sum_i p_i log_2(p_i)$, dla powyższego rozkładu wynosi **7.972** bita.

Wyniki testu statystycznego NIST 800-22

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE		PROPORTION		STATISTICAL TEST
2	4	5	4	5	1	2	3	10	4	0.122325		40/40		Frequency
1	5	3	3	7	5	6	3	2	5	0.534146		39/40		BlockFrequency
2	3	7	5	4	5	2	5	4	3	0.788728		40/40		CumulativeSums
3	4	4	8	3	6	3	2	4	3	0.637119		40/40		CumulativeSums
5	7	4	1	3	2	3	1	5	9	0.090936		40/40		Runs
1	5	7	5	1	4	3	4	5	5	0.534146		40/40		LongestRun
40	0	0	0	0	0	0	0	0	0	0.000000	*	0/40	*	Rank
2	4	8	8	0	8	0	7	0	3	0.001156		40/40		FFT
3	0	2	7	0	0	11	0	10	7	0.000002	*	39/40		NonOverlappingTemplate
3	0	1	6	0	0	7	0	18	5	0.000000	*	38/40		NonOverlappingTemplate
8	0	1	8	0	0	7	0	10	6	0.000014	*	36/40	*	NonOverlappingTemplate
7	1	3	6	0	0	8	0	10	5	0.000296		38/40		NonOverlappingTemplate
5	0	0	7	0	0	7	0	13	8	0.000000	*	39/40		NonOverlappingTemplate
6	1	1	5	0	0	12	0	7	8	0.000008	*	38/40		NonOverlappingTemplate
6	0	2	3	0	0	8	0	13	8	0.000000	*	39/40		NonOverlappingTemplate
4	1	3	2	0	0	16	0	5	9	0.000000	*	40/40		NonOverlappingTemplate
7	0	2	3	0	0	12	0	10	6	0.000001	*	38/40		NonOverlappingTemplate
4	0	0	6	0	0	10	0	14	6	0.000000	*	40/40		NonOverlappingTemplate
4	0	2	6	0	0	12	0	14	2	0.000000	*	40/40		NonOverlappingTemplate
7	0	1	3	0	0	8	0	17	4	0.000000	*	36/40	*	NonOverlappingTemplate
8	0	1	5	0	0	6	0	12	8	0.000002	*	35/40	*	NonOverlappingTemplate
7	1	2	3	0	0	8	0	12	7	0.000008	*	38/40		NonOverlappingTemplate
10	0	1	1	0	0	9	0	15	4	0.000000	*	38/40		NonOverlappingTemplate
9	0	0	3	0	0	12	0	10	6	0.000000	*	36/40	*	NonOverlappingTemplate
5	0	2	8	0	0	10	0	7	8	0.000032	*	40/40		NonOverlappingTemplate
6	0	1	5	0	0	8	0	15	5	0.000000	*	39/40		NonOverlappingTemplate
2	0	3	3	0	0	14	0	8	10	0.000000	*	39/40		NonOverlappingTemplate
5	0	2	1	0	0	9	0	11	12	0.000000	*	39/40		NonOverlappingTemplate
8	1	3	6	0	0	5	0	12	5	0.000040	*	37/40		NonOverlappingTemplate
5	0	1	5	0	0	10	0	11	8	0.000001	*	38/40		NonOverlappingTemplate
8	0	1	3	0	0	11	0	9	8	0.000001	*	38/40		NonOverlappingTemplate
5	0	3	3	0	0	11	0	11	7	0.000002	*	39/40		NonOverlappingTemplate
6	1	1	8	0	0	6	0	11	7	0.000026	*	38/40		NonOverlappingTemplate
7	0	1	4	0	0	9	0	13	6	0.000000	*	38/40		NonOverlappingTemplate
26	19	10	6	9	9	5	4	5	7	0.000001	*	93/100	*	NonOverlappingTemplate
10	16	8	10	6	8	9	10	11	12	0.678686		100/100		NonOverlappingTemplate
32	12	6	7	5	10	8	3	9	8	0.000000	*	90/100	*	NonOverlappingTemplate
31	15	6	8	4	7	12	5	6	6	0.000000	*	92/100	*	NonOverlappingTemplate
16	12	11	12	13	12	8	6	6	4	0.162606		96/100		OverlappingTemplate
100	0	0	0	0	0	0	0	0	0	0.000000	*	0/100	*	Universal
89	6	2	1	1	0	1	0	0	0	0.000000	*	32/100	*	ApproximateEntropy
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursions
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
0	0	0	0	0	0	0	0	0	0	----		------		RandomExcursionsVariant
76	3	3	3	4	5	3	0	2	1	0.000000	*	32/100	*	Serial
67	5	4	6	6	3	2	3	4	0	0.000000	*	44/100	*	Serial
13	4	9	10	8	10	9	14	14	9	0.494392		96/100		LinearComplexity

Metoda poprawy właściwości statystycznych przez zastosowanie SHA3-256 (gr Nikonowicz):

Aby przetworzyć pobrane rzuty monetą, każde pobrane 256 bitów jest poddawane działaniu **SHA3-256**



Entropia wyliczona zgodnie ze wzorem: $e = -\sum_i p_i log_2(p_i)$, dla powyższego rozkładu wynosi **7,9997** bita.

Wyniki testu statystycznego NIST 800-22

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	11	9	11	7	14	10	6	12	12	0.779188	100/100	Frequency
9	8	12	10	12	12	10	10	7	10	0.978072	96/100	BlockFrequency
7	10	13	10	15	8	2	13	11	11	0.202268	100/100	CumulativeSums
8	8	12	6	14	6	12	8	11	15	0.401199	99/100	CumulativeSums
11	8	13	10	9	6	7	14	14	8	0.574903	99/100	Runs
8	9	11	11	13	12	8	12	10	6	0.883171	98/100	LongestRun
2	19	5	23	22	7	3	5	8	6	0.000000 *	100/100	Rank
11	9	9	12	7	11	8	13	12	8	0.924076	100/100	FFT
11	5	8	13	11	11	9	8	12	12	0.798139	98/100	NonOverlappingTemplate
6	6	8	9	9	9	16	18	9	10	0.122325	100/100	NonOverlappingTemplate
10	6	7	8	11	14	12	9	15	8	0.534146	97/100	NonOverlappingTemplate
2	8	6	11	13	8	18	13	7	14	0.020548	99/100	NonOverlappingTemplate
15	8	5	7	14	11	9	11	9	11	0.494392	98/100	NonOverlappingTemplate
8	7	12	10	11	8	7	12	13	12	0.851383	98/100	NonOverlappingTemplate
10	9	8	10	8	14	12	11	7	11	0.911413	99/100	NonOverlappingTemplate
6	10	8	6	11	7	13	14	12	13	0.494392	99/100	NonOverlappingTemplate
14	6	12	8	11	5	10	7	13	14	0.350485	100/100	NonOverlappingTemplate
13	12	9	2	10	11	9	14	7	13	0.249284	98/100	NonOverlappingTemplate
10	5	12	12	5	8	11	15	9	13	0.366918	98/100	NonOverlappingTemplate
13	13	11	9	4	10	10	10	7	13	0.595549	98/100	NonOverlappingTemplate
9	8	7	12	10	8	15	10	10	11	0.851383	99/100	NonOverlappingTemplate
10	1	12	6	9	11	13	16	13	9	0.071177	100/100	NonOverlappingTemplate
9	7	15	12	10	12	8	12	5	10	0.574903	99/100	NonOverlappingTemplate
8	11	9	6	8	10	11	12	15	10	0.779188	98/100	NonOverlappingTemplate
11	9	7	13	5	11	7	10	13	14	0.534146	98/100	NonOverlappingTemplate
13	10	7	14	8	7	13	7	9	12	0.637119	98/100	NonOverlappingTemplate
12	16	5	11	7	11	14	7	6	11	0.224821	97/100	NonOverlappingTemplate
13	6	12	6	9	8	14	9	13	10	0.574903	97/100	NonOverlappingTemplate
6	12	9	13	12	11	5	11	12	9	0.678686	99/100	NonOverlappingTemplate
6	10	7	10	11	16	8	13	10	9	0.574903	99/100	NonOverlappingTemplate
14	5	9	10	17	7	7	12	10	9	0.249284	97/100	NonOverlappingTemplate
10	11	11	10	8	14	11	10	7	8	0.935716	100/100	NonOverlappingTemplate
7	10	9	8	14	7	11	11	11	12	0.867692	99/100	NonOverlappingTemplate
4	8	11	11	14	14	11	6	8	13	0.319084	100/100	NonOverlappingTemplate

```
  9  15   5   8   8   9  16  17   7   6  0.048716     98/100      NonOverlappingTemplate
  4  10  14   5   8  18   9  10  14   8  0.055361     98/100      NonOverlappingTemplate
 14  12   4   8  14   8   9   7  10  14  0.304126     98/100      NonOverlappingTemplate
 12   8   6   9   7   7  18  13   9  11  0.224821    100/100      NonOverlappingTemplate
  8   9  12   8  13   6  11  13  11   9  0.834308    100/100      OverlappingTemplate
100   0   0   0   0   0   0   0   0   0  0.000000 *    0/100   *  Universal
 61  10  15   3   3   5   2   1   0   0  0.000000 *   74/100   *  ApproximateEntropy
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursions
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0     ----     ------     RandomExcursionsVariant
  9   8  11  11  10  17   9   8   7  10  0.637119     99/100      Serial
 15   6  10  11  11  12   8  12  10   5  0.534146    100/100      Serial
 12   6  13  13  11  10   7  12   4  12  0.419021     93/100   *  LinearComplexity
```

Uwagi:Generowanie liczb za pomocą tego generatora jest długotrwałe, a jeszcze dłuższe jest postprocessing zaproponowany przez autorów artykułu, który wykorzystany był do jego stworzenia. Do wygenerowania 15000000 bitów po ich złożeniu i wykorzystaniu algorytmu "fair coin" potrzebne by było 15 dni.