

Fixed-point implementation of Chebyshev sequence generators with applications to DS-CDMA and Giga bit/s vector stream ciphers

Ken Umeno^{*1,*2}, Han-lung Lin^{*2,*3}, and Shen-hung Shih^{*2}

^{*1}: Chaotic Cipher Chip Project, Communications Research Laboratory
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
e-mail: umeno@crl.go.jp

^{*2}: JST Chaos CDMA R&D, Shibuya 1-20-1, Tokyo 150-0002, Japan

^{*3}: The University of Electro-Communications, Koganei, Cho-fuTokyo 184-8795, Japan

Abstract: We developed a fast digital chaos generators based on the second order Chebyshev polynomial. This chaos generators have good randomness properties to be tested by the FIPS 140-1 randomness test and high-speed properties of random bit generations beyond 1 Giga bit/s. Applications include spreading sequences of DS-CDMA system, Monte Carlo methods, or high-speed encryption. [1-5] We implemented it in various FPGA chips.

I. Functional Description

The functional block diagram of the Chebyshev code generator is shown in Figure 1.

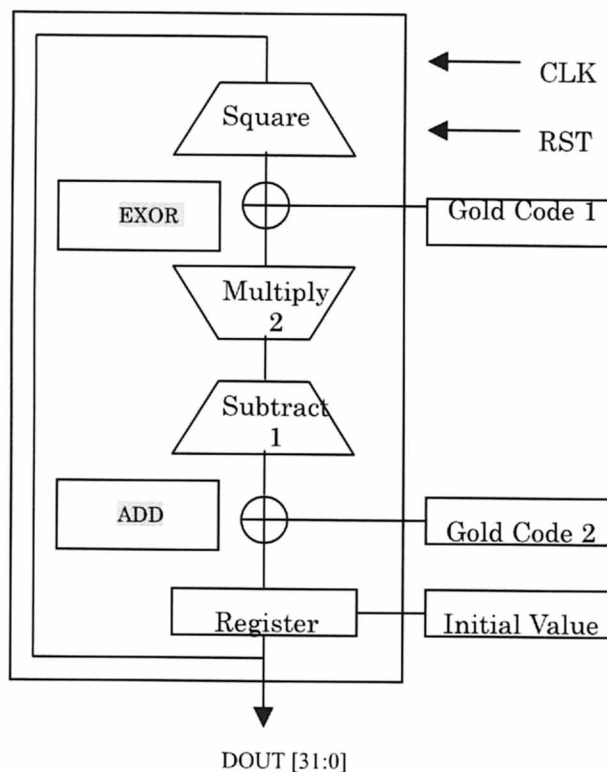


Figure 1: Chebyshev Code Generator Block Diagram

The code generator is based on Chebyshev polynomial ($2x^2-1$). After being squared, the LSB of the 32-bit data is EXORed with the Gold Code 1 sequence. Then the 32-bit data is multiplied by a factor 2, followed by a subtraction with 1 (7FFF in Hex). The output of subtraction is added with Gold Code 2 at LSB. A feedback from output of register to input of square function block is exploited to generate the succeeding code. As shown in Table I, Giga bit/sec performance is achieved on various kinds of FPGA chip implementations.

Supported FPGA	Device	System Clock (MHz)	Max Generation Speed (Mbps)
Vertex-E(Xilinx)	XCV100E-8	42.557	1361.8
Vertex-II(Xilinx)	XC2V250-4	63.203	2022.5
Vertex-II Pro(Xilinx)	XC2VP2-7	65.898	2108.7
Stratix(Altera)	EP1S10	39.16	1253.12

Table 1: 32-bit Core Implementation Data

II. FIPS 140-1 Test

Next, we apply the standard randomness test to each output (32 bit streams) of the generator. The randomness test chosen here is the FIPS 140-1 given by NIST [6]. As shown in the Appendix, all consecutive bit streams are passed along the period (period= $2^{25}-1$) with the Gold sequences with the same period which are used for complex scrambling in the W-CDMA systems.

V. Summary and Discussions

We have developed 32bit chaotic random-number generators based on the second order Chebyshev polynomials based on 32bit fixed point arithmetics. By adding two Gold sequences at LSB, we succeed that each bit streams passes standard randomness test called FIPS 140-1. We implemented it on Xilinx VertexII chips with more than 1 Gbps generation speed.

Acknowledgements

One (K.U) of the authors would like to thank Ms. Minghui Kao for her continual support during the JST pre-venture project.

References

- [1] K. Umeno and K. Kitayama, "Spreading sequences using periodic orbits of chaos for CDMA", Electronics letters, Vol.35, No.7, pp.545-546, 1999.
- [2] K. Umeno and K. Kitayama, "Improvement of SNR with chaotic spreading sequences for CDMA", Proc. of IEEE Information Theory Workshop, p.166, June, 1999.
- [3] C.C. Chen, K. Yao, K. Umeno, and E. Biglieri, "Design of Spread-Spectrum Sequences Using Chaotic Dynamical Systems and Ergodic Theory," IEEE Trans. Circuits and Systems- I vol.48 pp.1110-1114, Sep. 2001.
- [4] K. Umeno and A. Yamaguchi, "Construction of Optimal Chaotic Spreading Sequences Using Lebesgue Spectrum Filter", IEICE Trans. Fundamental. Vol.E58-A pp.849-852, Apr. 2002.
- [5] R. L. Adler and T. J. Rivlin, "Ergodic and mixing properties of Chebyshev polynomials," Proc. Amer. Math. Soc., vol.15 pp.794-796, 1964.
- [6] FIPS PUB 140-2, "Security Requirements for Cryptographic Module" (Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, 2001) <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

Appendix: FIPS 140-1 Test Results of the first 32*20000 bits.

1th Bit(LSB)

The monobit test	X=	10017	pass	(pass if 9654 < X < 10346)
The poker test	X=	11.872	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2490	2530	pass	(pass if 2267 < X < 2733)
2	1230	1176	pass	(pass if 1079 < X < 1421)
3	619	643	pass	(pass if 502 < X < 748)
4	321	293	pass	(pass if 223 < X < 402)
5	166	162	pass	(pass if 90 < X < 223)
6+	150	171	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

2th Bit

The monobit test	X=	9934	pass	(pass if 9654 < X < 10346)
The poker test	X=	19.4624	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2499	2481	pass	(pass if 2267 < X < 2733)
2	1209	1285	pass	(pass if 1079 < X < 1421)
3	629	608	pass	(pass if 502 < X < 748)
4	314	319	pass	(pass if 223 < X < 402)
5	181	131	pass	(pass if 90 < X < 223)
6+	153	161	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

3th Bit

The monobit test	X=	10062	pass	(pass if 9654 < X < 10346)
The poker test	X=	7.392	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2489	2458	pass	(pass if 2267 < X < 2733)
2	1255	1229	pass	(pass if 1079 < X < 1421)
3	617	628	pass	(pass if 502 < X < 748)
4	297	358	pass	(pass if 223 < X < 402)
5	150	151	pass	(pass if 90 < X < 223)
6+	162	148	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

4th Bit

The monobit test	X=	9977	pass	(pass if 9654 < X < 10346)
The poker test	X=	16.9216	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2525	2501	pass	(pass if 2267 < X < 2733)
2	1231	1271	pass	(pass if 1079 < X < 1421)
3	646	636	pass	(pass if 502 < X < 748)
4	308	330	pass	(pass if 223 < X < 402)
5	157	135	pass	(pass if 90 < X < 223)
6+	154	148	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

5th Bit

The monobit test	X=	10014	pass	(pass if 9654 < X < 10346)
The poker test	X=	6.6048	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2539	2566	pass	(pass if 2267 < X < 2733)
2	1254	1253	pass	(pass if 1079 < X < 1421)
3	646	624	pass	(pass if 502 < X < 748)
4	312	280	pass	(pass if 223 < X < 402)
5	157	154	pass	(pass if 90 < X < 223)
6+	138	170	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

6th Bit

The monobit test	X=	10048	pass	(pass if 9654 < X < 10346)
The poker test	X=	12.4864	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2537	2528	pass	(pass if 2267 < X < 2733)
2	1260	1254	pass	(pass if 1079 < X < 1421)
3	659	635	pass	(pass if 502 < X < 748)
4	274	318	pass	(pass if 223 < X < 402)
5	152	131	pass	(pass if 90 < X < 223)
6+	149	166	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

7th Bit

The monobit test	X=	10060	pass	(pass if 9654 < X < 10346)
The poker test	X=	14.6048	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2518	2493	pass	(pass if 2267 < X < 2733)
2	1278	1268	pass	(pass if 1079 < X < 1421)
3	629	643	pass	(pass if 502 < X < 748)
4	286	310	pass	(pass if 223 < X < 402)
5	162	142	pass	(pass if 90 < X < 223)
6+	144	162	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

8th Bit

The monobit test	X=	9916	pass	(pass if 9654 < X < 10346)
The poker test	X=	6.2464	pass	(pass if 1.03 < X < 57.4)
The runs test				
Run length	Zeros	Ones		
1	2481	2558	pass	(pass if 2267 < X < 2733)
2	1260	1211	pass	(pass if 1079 < X < 1421)
3	608	583	pass	(pass if 502 < X < 748)
4	331	333	pass	(pass if 223 < X < 402)
5	142	153	pass	(pass if 90 < X < 223)
6+	172	157	pass	(pass if 90 < X < 223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

9th Bit

The monobit test	X=	10075	pass	(pass if $9654 < X < 10346$)
The poker test	X=	17.024	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2560	2543	pass	(pass if $2267 < X < 2733$)
2	1243	1241	pass	(pass if $1079 < X < 1421$)
3	657	625	pass	(pass if $502 < X < 748$)
4	282	310	pass	(pass if $223 < X < 402$)
5	148	166	pass	(pass if $90 < X < 223$)
6+	150	156	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

10th Bit

The monobit test	X=	10097	pass	(pass if $9654 < X < 10346$)
The poker test	X=	17.472	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2591	2550	pass	(pass if $2267 < X < 2733$)
2	1223	1224	pass	(pass if $1079 < X < 1421$)
3	612	624	pass	(pass if $502 < X < 748$)
4	323	317	pass	(pass if $223 < X < 402$)
5	147	164	pass	(pass if $90 < X < 223$)
6+	144	162	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

11th Bit

The monobit test	X=	10024	pass	(pass if $9654 < X < 10346$)
The poker test	X=	18.2528	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2523	2458	pass	(pass if $2267 < X < 2733$)
2	1189	1265	pass	(pass if $1079 < X < 1421$)
3	626	626	pass	(pass if $502 < X < 748$)
4	309	313	pass	(pass if $223 < X < 402$)
5	173	148	pass	(pass if $90 < X < 223$)
6+	154	164	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

12th Bit

The monobit test	X=	10056	pass	(pass if $9654 < X < 10346$)
The poker test	X=	14.3616	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2487	2446	pass	(pass if $2267 < X < 2733$)
2	1228	1216	pass	(pass if $1079 < X < 1421$)
3	611	648	pass	(pass if $502 < X < 748$)
4	315	332	pass	(pass if $223 < X < 402$)
5	154	160	pass	(pass if $90 < X < 223$)
6+	163	157	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

13th Bit

The monobit test	X=	9984	pass	(pass if $9654 < X < 10346$)
The poker test	X=	19.0656	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2401	2379	pass	(pass if $2267 < X < 2733$)
2	1268	1326	pass	(pass if $1079 < X < 1421$)
3	622	624	pass	(pass if $502 < X < 748$)
4	351	310	pass	(pass if $223 < X < 402$)
5	162	157	pass	(pass if $90 < X < 223$)
6+	139	148	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

14th Bit

The monobit test	X=	10070	pass	(pass if $9654 < X < 10346$)
The poker test	X=	21.664	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2518	2417	pass	(pass if $2267 < X < 2733$)
2	1235	1319	pass	(pass if $1079 < X < 1421$)
3	640	663	pass	(pass if $502 < X < 748$)
4	312	311	pass	(pass if $223 < X < 402$)
5	172	142	pass	(pass if $90 < X < 223$)
6+	128	154	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

15th Bit

The monobit test	X=	10069	pass	(pass if $9654 < X < 10346$)
The poker test	X=	12.736	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2467	2443	pass	(pass if $2267 < X < 2733$)
2	1265	1239	pass	(pass if $1079 < X < 1421$)
3	621	641	pass	(pass if $502 < X < 748$)
4	320	331	pass	(pass if $223 < X < 402$)
5	150	160	pass	(pass if $90 < X < 223$)
6+	150	160	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

16th Bit(MSB)

The monobit test	X=	10087	pass	(pass if $9654 < X < 10346$)
The poker test	X=	7.5648	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2515	2537	pass	(pass if $2267 < X < 2733$)
2	1254	1260	pass	(pass if $1079 < X < 1421$)
3	667	566	pass	(pass if $502 < X < 748$)
4	302	324	pass	(pass if $223 < X < 402$)
5	142	171	pass	(pass if $90 < X < 223$)
6+	143	166	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

17th Bit(LSB)

The monobit test	X=	10002	pass	(pass if $9654 < X < 10346$)
The poker test	X=	11.8848	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2531	2531	pass	(pass if $2267 < X < 2733$)
2	1211	1210	pass	(pass if $1079 < X < 1421$)
3	634	637	pass	(pass if $502 < X < 748$)
4	315	315	pass	(pass if $223 < X < 402$)
5	163	162	pass	(pass if $90 < X < 223$)
6+	153	153	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

18th Bit

The monobit test	X=	10067	pass	(pass if $9654 < X < 10346$)
The poker test	X=	12.2752	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2551	2482	pass	(pass if $2267 < X < 2733$)
2	1214	1290	pass	(pass if $1079 < X < 1421$)
3	625	618	pass	(pass if $502 < X < 748$)
4	321	304	pass	(pass if $223 < X < 402$)
5	149	147	pass	(pass if $90 < X < 223$)
6+	152	172	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

19th Bit

The monobit test	X=	10075	pass	(pass if $9654 < X < 10346$)
The poker test	X=	23.2384	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2411	2437	pass	(pass if $2267 < X < 2733$)
2	1280	1215	pass	(pass if $1079 < X < 1421$)
3	623	602	pass	(pass if $502 < X < 748$)
4	287	320	pass	(pass if $223 < X < 402$)
5	154	171	pass	(pass if $90 < X < 223$)
6+	167	178	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

20th Bit

The monobit test	X=	10085	pass	(pass if $9654 < X < 10346$)
The poker test	X=	16.7552	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2519	2424	pass	(pass if $2267 < X < 2733$)
2	1234	1304	pass	(pass if $1079 < X < 1421$)
3	589	620	pass	(pass if $502 < X < 748$)
4	343	315	pass	(pass if $223 < X < 402$)
5	148	166	pass	(pass if $90 < X < 223$)
6+	152	157	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

21th Bit

The monobit test	X=	9934	pass	(pass if $9654 < X < 10346$)
The poker test	X=	6.6432	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2442	2459	pass	(pass if $2267 < X < 2733$)
2	1233	1298	pass	(pass if $1079 < X < 1421$)
3	648	603	pass	(pass if $502 < X < 748$)
4	347	312	pass	(pass if $223 < X < 402$)
5	144	137	pass	(pass if $90 < X < 223$)
6+	156	162	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

22th Bit

The monobit test	X=	10003	pass	(pass if $9654 < X < 10346$)
The poker test	X=	13.44	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2418	2450	pass	(pass if $2267 < X < 2733$)
2	1279	1221	pass	(pass if $1079 < X < 1421$)
3	606	635	pass	(pass if $502 < X < 748$)
4	303	291	pass	(pass if $223 < X < 402$)
5	169	180	pass	(pass if $90 < X < 223$)
6+	164	163	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

23th Bit

The monobit test	X=	9880	pass	(pass if $9654 < X < 10346$)
The poker test	X=	18.5984	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2511	2592	pass	(pass if $2267 < X < 2733$)
2	1236	1281	pass	(pass if $1079 < X < 1421$)
3	661	580	pass	(pass if $502 < X < 748$)
4	326	290	pass	(pass if $223 < X < 402$)
5	147	143	pass	(pass if $90 < X < 223$)
6+	159	155	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

24th Bit

The monobit test	X=	10017	pass	(pass if $9654 < X < 10346$)
The poker test	X=	11.5136	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2487	2470	pass	(pass if $2267 < X < 2733$)
2	1240	1225	pass	(pass if $1079 < X < 1421$)
3	624	628	pass	(pass if $502 < X < 748$)
4	298	333	pass	(pass if $223 < X < 402$)
5	164	159	pass	(pass if $90 < X < 223$)
6+	159	158	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

25th Bit

The monobit test	X=	9987	pass	(pass if $9654 < X < 10346$)
The poker test	X=	10.0672	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2521	2491	pass	(pass if $2267 < X < 2733$)
2	1225	1262	pass	(pass if $1079 < X < 1421$)
3	604	622	pass	(pass if $502 < X < 748$)
4	292	297	pass	(pass if $223 < X < 402$)
5	191	162	pass	(pass if $90 < X < 223$)
6+	158	158	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

26th Bit

The monobit test	X=	10036	pass	(pass if $9654 < X < 10346$)
The poker test	X=	8.8448	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2496	2480	pass	(pass if $2267 < X < 2733$)
2	1288	1263	pass	(pass if $1079 < X < 1421$)
3	593	639	pass	(pass if $502 < X < 748$)
4	309	316	pass	(pass if $223 < X < 402$)
5	158	148	pass	(pass if $90 < X < 223$)
6+	160	159	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

27th Bit

The monobit test	X=	9854	pass	(pass if $9654 < X < 10346$)
The poker test	X=	25.1328	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2541	2561	pass	(pass if $2267 < X < 2733$)
2	1181	1229	pass	(pass if $1079 < X < 1421$)
3	629	621	pass	(pass if $502 < X < 748$)
4	308	313	pass	(pass if $223 < X < 402$)
5	162	132	pass	(pass if $90 < X < 223$)
6+	184	150	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

28th Bit

The monobit test	X=	10032	pass	(pass if $9654 < X < 10346$)
The poker test	X=	12.1984	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2472	2491	pass	(pass if $2267 < X < 2733$)
2	1301	1277	pass	(pass if $1079 < X < 1421$)
3	597	620	pass	(pass if $502 < X < 748$)
4	344	298	pass	(pass if $223 < X < 402$)
5	152	166	pass	(pass if $90 < X < 223$)
6+	142	157	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

29th Bit

The monobit test	X=	10001	pass	(pass if $9654 < X < 10346$)
The poker test	X=	10.6368	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2512	2533	pass	(pass if $2267 < X < 2733$)
2	1248	1237	pass	(pass if $1079 < X < 1421$)
3	649	618	pass	(pass if $502 < X < 748$)
4	304	318	pass	(pass if $223 < X < 402$)
5	155	160	pass	(pass if $90 < X < 223$)
6+	148	151	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

30th Bit

The monobit test	X=	10004	pass	(pass if $9654 < X < 10346$)
The poker test	X=	21.504	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2488	2554	pass	(pass if $2267 < X < 2733$)
2	1286	1253	pass	(pass if $1079 < X < 1421$)
3	657	599	pass	(pass if $502 < X < 748$)
4	312	296	pass	(pass if $223 < X < 402$)
5	144	163	pass	(pass if $90 < X < 223$)
6+	142	165	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

31th Bit

The monobit test	X=	10063	pass	(pass if $9654 < X < 10346$)
The poker test	X=	10.72	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2580	2522	pass	(pass if $2267 < X < 2733$)
2	1238	1287	pass	(pass if $1079 < X < 1421$)
3	615	594	pass	(pass if $502 < X < 748$)
4	293	311	pass	(pass if $223 < X < 402$)
5	164	161	pass	(pass if $90 < X < 223$)
6+	145	161	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

32th Bit(MSB)

The monobit test	X=	10084	pass	(pass if $9654 < X < 10346$)
The poker test	X=	16.7296	pass	(pass if $1.03 < X < 57.4$)
The runs test				
Run length		Zeros	Ones	
1	2500	2425	pass	(pass if $2267 < X < 2733$)
2	1216	1269	pass	(pass if $1079 < X < 1421$)
3	632	632	pass	(pass if $502 < X < 748$)
4	292	311	pass	(pass if $223 < X < 402$)
5	151	168	pass	(pass if $90 < X < 223$)
6+	166	165	pass	(pass if $90 < X < 223$)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)