Bias in the nonlinear filter generator output sequence

Sui-Guan Teo, Leonie Simpson and Ed Dawson

Information Security Institute
Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia
sg.teo,lr.simpson,e.dawson@qut.edu.au

Abstract. Nonlinear filter generators are common components used in the keystream generators for stream ciphers and more recently for authentication mechanisms. They consist of a Linear Feedback Shift Register (LFSR) and a nonlinear Boolean function to mask the linearity of the LFSR output. Properties of the output of a nonlinear filter are not well studied. Anderson noted that the m-tuple output of a nonlinear filter with consecutive taps to the filter function is unevenly distributed. Current designs use taps which are not consecutive. We examine m-tuple outputs from nonlinear filter generators constructed using various LFSRs and Boolean functions for both consecutive and uneven (full positive difference sets where possible) tap positions. The investigation reveals that in both cases, the m-tuple output is not uniform. However, consecutive tap positions result in a more biased distribution than uneven tap positions, with some m-tuples not occurring at all. These biased distributions indicate a potential flaw that could be exploited for cryptanalysis.

1 Introduction

Linear Feedback Shift Registers (LFSRs) are commonly used to produce sequences for cryptographic purposes. For example, they may be used as components of the keystream generator in a stream cipher. The theory regarding the properties of LFSR sequences is well known. The research presented in this paper focuses on the sequences produced by binary LFSRs, where each stage of the shift register contains a single bit.

If the feedback polynomial of the LFSR is primitive, the binary sequence produced has several properties which are useful for cryptographic applications. Firstly, the sequence has a known period: provided the initial state is non-zero, a LFSR of length L with primitive feedback polynomial produces a binary sequence of length $2^L - 1$. Thus a large period can be guaranteed by choosing an appropriate value for L. Secondly; the sequence has some good statistical properties. The distribution of all m-tuple patterns, for $m = \{1, 2, ...L\}$ is almost uniform. For example, when $m = 1$, one period of the LFSR output sequence contains 2^{L-1} ones, and $2^{L-1} - 1$ zeroes. When $m = 2$, if we consider one period of the LFSR output sequence as a series of overlapping two bit patterns, each of the two-bit patterns 01, 10 and 11 occurs 2^{L-2} times, and the pattern 00 occurs $2^{L-2}-1$ times. Similarly, in one period of the LFSR output sequence, each m-bit pattern occurs 2^{L-m} times, except for the all-zero m-bit pattern which occurs $2^{L-m}-1$ times. The distribution of m-tuple patterns in random sequences is expected to be uniform.

Although LFSR sequences have many desirable properties, using the LFSR output sequence directly as keystream is not advisable due to the linearity of LFSR sequences. To make use of the desirable properties of the LFSR in a keystream generator for a stream cipher, it is necessary to introduce nonlinearity. A simple method is to use the contents of several stages of the LFSR as inputs to a nonlinear Boolean function, and use the output of the function as the keystream. The nonlinear Boolean function is referred to as a filter function, and keystream generators based on a single LFSR and a nonlinear combining functions are known as nonlinear filter generators (NLFG). A diagram of a NLFG is shown in Figure 1.

The NLFG aims to make use of the good properties of the underlying LFSR, so it is worthwhile examining the NLFG output sequence to determine which of the desirable properties of the LFSR sequence are maintained in the NLFG output sequence. The period of the NLFG keystream sequence is known to be 2^L-1 (the same as the underlying LFSR sequence) if the LFSR feedback function is primitive and of degree L and the nonlinear filter function is balanced [7]. For most cryptographic purposes, a balanced filter function is used as a balanced output sequence is required.

A balanced filter function applied to the stages of a LFSR with primitive feedback function and non-zero initial state results in an output keystream where the difference between the number of zeroes and the number of ones occurring in one period of the keystream sequences is exactly one, that is, close to uniform. Much less is known about the frequency distribution of m-bit patterns in the NLFG output sequence for $m > 1$. An early paper by Anderson [1] discusses the distribution of m-bit patterns in the NLFG output sequence in the context of a correlation attack on the NLFG. Anderson considers that the common NLFG

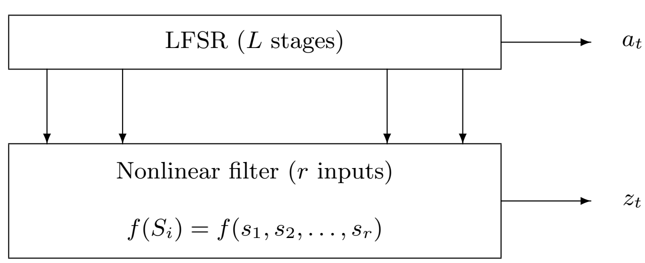

Fig. 1: Nonlinear Filter Generator.

correlation attack strategy, which regards the keystream as a series of individual bits, discards information about the nonlinear structure of the filter function. Instead, for a given m-input Boolean filter function, he defines an augmented function which maps a $2m-1$-bit input to an m-bit output. Essentially this is applying the m-input filter function m times in succession, assuming that the inputs to the filter function are from consecutive positions of the underlying sequence, although this is not stated explicitly in the paper. For the augmented function Anderson examined, the m-bit pattern distributions are clearly biased. For a particular Boolean function, certain m-tuples do not occur as outputs at all. This function was a bent function, which, due to its unbalanced nature, is not suitable as the filter function for a nonlinear filter generator. However, it was not clear whether distributions with non-occurring m-tuples are possible when balanced functions are used. Furthermore, the relationship between the characteristics of the Boolean filter function and the degree of bias in the output is not revealed.

To provide resistance to guess-and-determine style attacks, NLFG-style designs now commonly take the inputs to the filter from positions in the LFSR which are not consecutive, ideally tap positions which form a full positive difference set. The effect of this change in the positions of the input stages of the m-tuple pattern distribution of the NLFG output sequence warrants further investigation.

This paper presents the results of an investigation into the distribution of m-bit patterns in NLFG output sequences. This extends the earlier work of Anderson, where the value of m was used as both the number of inputs to the filter function and the length of the bit patterns examined in the NLFG output sequence. We make a clear distinction between these two parameters. We denote the number of inputs to the filter function by r, and consider the distribution of m-bit patterns in the NLFG output sequence for $m = \{1, 2, ...L\}$. We examine the output sequence of NLFGs constructed using various LFSRs and balanced nonlinear Boolean functions. In additional, we investigate both the case where the inputs to the filter function are from consecutive LFSR stages and the case where the inputs are non-consecutive from irregularly selected stages (full positive difference sets where possible).

The remainder of this paper is organised as follows. In Section 2, we describe our experimental design. In Section 3, the results of our experiments are described. In Section 4, we discuss the possible implications of our findings on the use of outputs of nonlinear filters for cryptographic purposes. Section 5 concludes this paper and suggests some future work.

2 Experimental Design

There are two main components of a NLFG, the LFSR and the nonlinear Boolean function. The goal of our experiments was to determine how these components affect the output sequence of the NLFG. We examine how choices in length and feedback polynomials for the LFSR and tap-settings to a nonlinear Boolean function affect the distribution of m-tuple outputs of the keystream sequence. In order to accurately determine the m-tuple distribution, it is necessary to produce an entire period of the keystream sequence. This constrained the length of the LFSRs used in our experiments. LFSR of length L, for L ranging from 13 to 20 bits, were chosen in our experiments. The primitive feedback polynomials chosen are:

$$
\begin{aligned}
L1 &: x^{13} + x^4 + x^3 + x^1 + 1 \\
L2 &: x^{13} + x^{12} + x^{10} + x^9 + x^6 + x^3 + 1 \\
L3 &: x^{15} + x^{10} + x^5 + x^1 + 1 \\
L4 &: x^{15} + x^1 + 1 \\
L5 &: x^{16} + x^5 + x^3 + x^2 + 1 \\
L6 &: x^{16} + x^{15} + x^{14} + x^8 + x^4 + x^3 + 1 \\
L7 &: x^{18} + x^5 + x^2 + x^1 + 1 \\
L8 &: x^{18} + x^{16} + x^{15} + x^{12} + x^{11} + x^9 + x^7 + ?x^6 + x^5 + x^4 + x^2 + x^1 + 1 \\
L9 &: x^{20} + x^{19} + x^4 + x^3 + 1 \\
L10 &: x^{20} + x^{19} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^4 + x^2 + 1
\end{aligned}
$$

Three balanced Boolean functions, $F1$, $F2$ and $F3$ were chosen for use as nonlinear filters. All three appear in the cryptographic literature. $F1$ is a 5-bit Boolean function used in the Grain stream cipher [4]. $F2$ is a 6-bit Boolean function obtained from a report by Faugère and Ars [3]. $F3$ is a 7-bit Boolean function used in Pomraranch [5]. The algebraic normal forms of these nonlinear Boolean functions are:

$$F1 : x2 + x5 + x1x4 + x3x4 + x4x5 + x1x2x3 + x1x3x4 + x1x3x5 + x2x3x5 + x3x4x5$$

$$F2 : x1x2x3 + x2x3x6 + x1x2 + x3x4 + x5x6 + x4 + x5$$

$F3$: ANF omitted due to size.

Relevant characteristics of these three Boolean functions, namely the algebraic degree, nonlinearity and correlation immunity are shown in Table 1 . For each of the feedback polynomials, three different sets of tap settings for the Boolean functions were chosen. One set of tap settings used consecutive taps from the LFSR and two sets used uneven (or FPDS where possible) taps from the LFSR. In the uneven tap settings scenario, two sets of tap settings were used. These are denoted T1 and T2 in Table 2.

Function	Algebraic degree	Nonlinearity	Correlation immunity
$F1$	3	12	1
$F2$	3	24	0
$F3$	4	56	2

Table 1: Characteristics of the Boolean functions

LFSR	F1		F2		F3	
	T1	T2	T1	T2	T1	T2
L1 & L2	0,1,4,8,12	0,1,3,7,12	0,1,2,5,9,12	0,2,5,7,10,12	0,1,3,5,19,11,12	0,2,3,5,8,10,12
L3 & L4	0,1,4,9,14	0,4,6,13,14	0,1,4,8,10,14	0,2,3,10,13,14	0,1,4,5,10,13,14	0,2,3,7,9,11,14
L5 & L6	0,1,3,11,15	0,1,5,11,15	0,1,4,8,13,15	0,3,7,8,11,15	0,1,3,6,10,12,15	0,2,3,7,10,13,15
L7 & L8	0,3,8,13,17	0,2,5,9,17	0,2,3,8,15,17	0,1,4,10,12,17	0,1,3,9,11,14,17	0,2,8,9,12,15,17
L9 & L10	0,1,3,7,19	0,2,7,9,19	0,1,3,7,12,19	0,1,4,11,13,19	0,1,3,8,11,17,19	0,3,5,9,10,14,19

Table 2: Tap settings used in our experiments

m-tuple	Expected occurrences	Observed occurrences	Standard Deviation	Proportion of all 3-tuples	Standard deviation of all 3-tuples	Goodness-of-fit value
000	4095	2815		0.023438		
001	4096	4352		0.132818		
010	4096	4864		0.132818		
011	4096	4352	768.208	0.132818	0.023445	1152.098
100	4096	4352		0.132818		
101	4096	4864		0.132818		
110	4096	4352		0.132818		
111	4096	2816		0.085940		

Table 3: 3-tuple distribution of a NLFG sequence

For each LFSR, nonlinear filter function and tap setting combination, the NLFG was run to generate a sequence $2^L + m - 1$ in length. The frequency distribution of m-tuples was calculated for $m = 2$ to 13. From this, the m-tuple which occurs least and most frequently for m-tuples of sizes 2 to 13 were noted. The standard deviation is a useful summary measure for the m-tuple distribution of a sequence. The smaller the standard deviation, the closer the m-tuple distribution of the sequence is to a uniform distribution. To enable comparisons where different size LFSR are used, the proportions of all m-tuples which have a specific value is calculated and the standard deviation of the proportion is also calculated. Recall the m-tuple distribution for the maximal length sequence produced by a LFSR is almost uniform. For example, the 3-tuple distribution for a 15-bit LFSR $L3$ with the nonlinear filter function $F1$ is given in Table 3.

Clearly, from this table, the distribution is far from uniform. This is shown by the large standard deviation and chi-square value.

3 Experimental results

Our experiments involved 90 NLFGs, comprising of different LFSRs, Boolean functions and tap settings. A sequence of length $2^L + m - 1$ bits for each NLFG was generated and the output sequence was examined for m-tuples for values of m ranging from 2 to 13 bits. We make a number of observations based on the results of our experiment. The factors which could impact on the m-tuple distribution include the positions of the inputs to the filter functions, the number of inputs to the filter function, and the length and feedback function of the LFSR. Detailed results from the experiments can be found in Appendix A.

Observation 3.1: The m-tuple distribution of NLFG output sequences is generally non-uniform. Note that our observation supports the earlier findings by Anderson. We also note that the degree of non-uniformity varies depending on the combination of LFSR feedback function, the nonlinear filter functions and positions of input taps to the filter function. There are a few cases when the m-tuple output of the NLFG was uniform for smaller m-tuple values. For example, the 3-tuple distribution for a NLFG using the $L5$, $F1$ and T1 combination had the m-tuple distribution expected of a maximal length sequence. However, as m increased, the distribution became less uniform. Close to uniform distribution were more frequent when $m < 4$ and when uneven tap settings were used. With the exception of one case when $m = 5$, all m-tuple distributions when $m > 4$ were not uniform for NLFGs which used uneven tap settings. The almost uniform m-tuple distribution never occurred for consecutive tap settings for all m-tuples tested.

Observation 3.2: The m-tuple distribution is less uniform when tap settings are consecutive. When comparing the m-tuple distribution for the output sequences obtained from NLFGs with the same LFSR and filter function but with different positions in the LFSR selected for inputs to the filter function, the distributions when the tap settings are consecutive are more varied than when the tap settings are uneven. For example, in the case for a 3-tuple distribution of a NLFG using the feedback function $L3$ with consecutive tap settings and the $F1$ as the nonlinear filter, the least frequent 3-tuple occurred 2815 times and the most frequent 3-tuple occurred 4864 times. The standard deviation obtained was 320.057. When the same feedback function and filter function was used in a NLFG with uneven tap setting T1, the least frequent 3-tuple occurred 3520 times and the most frequent 3-tuple occurred 4672 times. The standard deviation obtained 133.982. For the same LFSR and nonlinear filter with the uneven tap setting T2, the minimum obtained was 4095 and the maximum obtained was 4096 and the standard deviation obtained 0.331. This trend was apparent for every NLFG sequence examined.

Observation 3.3: For some NLFGs with balanced Boolean functions, some m-tuples do not occur. It is possible that particular m-tuples may not appear in a NLFG output sequence. In our experiments, we noted that this can occur when the nonlinear Boolean functions are balanced. The number of different m-tuples which do not appear in the output sequence is higher for NLFGs using consecutive tap settings than when uneven tap settings are used. For example, a NLFG using the feedback function $L1$, $F2$ Boolean function and the consecutive tap settings has 20 non-occurring 10-bit tuples. In contrast, a NLFG using the same feedback function and Boolean function with the T1 tap setting has only three non-occurring 10-bit tuples. As the m-tuple size increases, the number of non-occurring m-tuples also increases for uneven tap settings. We also noted from our experiments that, for a given choice of filter function and tap setting, as the size of the LFSR increased, the number of m-tuples which do not appear in the output sequence remained constant once a certain size was reached for the LFSRs we tested. For example, there were 17 non-occurring 10-bit m-tuples for a 6-input Boolean function when $L \geq 15 \ldots 20$.

Observation 3.4: Distribution of m-tuples for NLFGs using consecutive tap settings are similar regardless of the size of the LFSR. The distributions of the proportions of m-tuples for NLFGs using consecutive tap settings were similar regardless of the size of the LFSR. However, this was not the case for uneven tap settings. For NLFGs using uneven tap settings, the standard deviation of the m-tuples in terms of proportions are different for different LFSR lengths, tap settings and Boolean functions.

4 Discussion

In this section, we consider the potential impact of biased m-tuple distributions in the output sequences from NLFGs. These sequences are used keystream for stream ciphers, in initialisation functions and as building blocks for message authentication codes (MAC).

Some stream ciphers use the output of NLFGs as keystream to encrypt messages. There is a potential major flaw in this design choice if the NLFG has a highly biased m-tuple distribution. Firstly, there is a possibility of mounting a distinguishing attack on the keystream. If an attacker were to perform a statistical analysis on the m-tuple outputs, they might be able to mount a distinguishing attack based on the frequency of the various m-tuples in the keystream. Another possible attack is a ciphertext-only attack on the stream cipher. Biased m-tuple distribution combined with the redundancy of the plaintext may provide leakage of information to allow an attack to partially decrypt ciphertext messages without initial knowledge of the secret key. An example of a ciphertext-only attack which exploits biased eight-tuple distributions in RC4 is the ciphertext-only attack by Mantin and Shamir [6].

Modern stream ciphers use a secret key and a publicly known initialisation vector (IV) as input to an initialisation function to generate the initial state of the keystream generator. This initialisation function should be nonlinear. A potential problem with using the output of a nonlinear filter for initialisation is that if m-tuples occur more often than others, then it is possible that some initial states will occur more often than others, resulting in biased keystream distribution. In the case where some m-tuples do not occur at all, this means some initial states might not occur at all for any key-iv pair, reducing the effective key space of the stream cipher.

In recent years, stream cipher designers have proposed ciphers which aim to provide simultaneous confidentiality and integrity protection. These are commonly called authenticated encryption (AE) stream ciphers. Some AE stream ciphers use nonlinear filter generators in components used to compute the Message Authentication Code (MAC) tag. One example of such a cipher is Sfinks [2]. For MAC algorithms which make use of nonlinear filters, the distribution of MAC tags for messages may not be uniform. An attacker may be able to exploit this in a MAC collision attack.

5 Conclusion and Future Work

In this paper, we examined the output of various NLFGs and analysed the distribution of m-tuples in the output sequence for $m = \{2, 3, \ldots 13\}$. We show that the m-tuple distributions of NLFGs are biased, regardless of tap settings used, although the bias is generally greater when the tap settings to the filter function are consecutive. In some cases, there are some m-tuples which do not occur at all in the outputs. This happens for small m-values if the NLFGs use consecutive tap settings rather than uneven tap settings. The experiments also show that the frequency distributions of m-tuples for NLFGs using consecutive tap settings are similar regardless of the size of the LFSR.

The findings in this experiment may have cryptanalytic applications. The significant m-tuple bias in the output sequence may be exploited in attacks ranging from distinguishing attacks to ciphertext-alone attacks. If a NLFG is to be used in a cryptographic application, we recommend against consecutive tap settings.

A limitation of the work is the use of only three Boolean functions of input sizes 5, 6 and 7 bits. This makes it difficult to draw conclusions about the effect of the Boolean function itself on the m-tuple distributions of NLFG output sequences. Further experiments investigating the m-tuple distribution of NLFG sequences formed using Boolean functions with the same number of inputs but with different nonlinearity or algebraic degree remains future work.

References

1. Anderson, R.: Searching for the Optimum Correlation Attack. In Preneel, B., ed.: Fast Software Encryption (FSE 94). Volume 1008 of Lecture Notes in Computer Science., Springer (1995) 137–143
2. Braeken, A., Lano, J., Mentens, N., Preneel, B., Verbauwhede, I.: SFINKS : A Synchronous Stream Cipher for Restricted Hardware Environments. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/026 (2005) Available from `http://www.ecrypt.eu.org/stream/ciphers/sfinks/sfinks.ps`.
3. Faugère, Jean-Charles and Ars, Gwénolé: An Algebraic Cryptanalysis of Nonlinear Filter Generators using Gröbner bases. Technical report, Institut National De Recherche En Informatique Et En Automatique (2003) Available from `http://hal.inria.fr/docs/00/07/18/48/PDF/RR-4739.pdf`.
4. Hell, M., Johansson, T., Meier, W.: Grain – A Stream Cipher for Constrained Environments. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/010 (2005) Available from `http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf`.

5. Jansen, C.J., Helleseth, T., Kholosha, A.: Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher (Version 2). eSTREAM, ECRYPT Stream Cipher Project, Report 2006/006 (2006) Available from `http://www.ecrypt.eu.org/stream/papersdir/2006/006.pdf`.
6. Mantin, I., Shamir, A.: A Practical Attack on Broadcast RC4. In Matsui, M., ed.: Fast Software Encryption (FSE 2002). Volume 2355 of Lecture Notes in Computer Science., Springer (2002) 152–164
7. Simpson, L.: Divide and Conquer Attacks on Shift Register Based Stream Ciphers. PhD thesis, Queensland University of Technology (January 2000)

A Experimental Results

Appendix A lists the results from the analysis of the m-tuple distribution, for $m = \{2, 3, \ldots 13\}$, for Boolean functions $F1$, $F2$ and $F3$.

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	2	1791	2304	0	256.250	0.031284	2047	2048	0	0.433	0.000053	2047	2048	0	0.433	0.000053
	3	703	1216	0	192.209	0.023466	1008	1040	0	15.878	0.001938	1008	1040	0	15.878	0.001938
	4	255	640	0	128.125	0.015642	496	528	0	11.228	0.001371	494	530	0	11.393	0.001391
L2	2	1791	2304	0	256.250	0.031284	2047	2048	0	0.433	0.000053	2047	2048	0	0.433	0.000053
	3	703	1216	0	192.209	0.023466	1023	1024	0	0.331	0.000040	1023	1024	0	0.331	0.000040
	4	255	640	0	128.125	0.015642	511	512	0	0.242	0.000030	509	514	0	2.076	0.000253
L3	2	7167	9216	0	1024.250	0.031259	7969	8704	0	512.250	0.015633	8191	8192	0	0.433	0.000013
	3	2815	4864	0	768.208	0.023445	3520	4672	0	367.804	0.011225	4095	4096	0	0.331	0.000010
	4	1023	2560	0	512.125	0.015629	1632	2464	0	228.622	0.006977	2047	2048	0	0.242	0.000007
L4	2	7167	9216	0	1024.250	0.031259	8191	8192	0	0.433	0.000013	8191	8192	0	0.433	0.000013
	3	2815	4864	0	768.208	0.023445	4095	4096	0	0.331	0.000010	4095	4096	0	0.331	0.000010
	4	1023	2560	0	512.125	0.015629	2040	2056	0	7.941	0.000242	2047	2048	0	0.242	0.000007
L5	2	14335	18432	0	2048.250	0.031254	16383	16384	0	0.433	0.000007	16383	16384	0	0.433	0.000007
	3	5631	9728	0	1536.208	0.023441	8191	8192	0	0.331	0.000005	8191	8192	0	0.331	0.000005
	4	2047	5120	0	1024.125	0.015627	4080	4112	0	15.939	0.000243	4080	4112	0	15.939	0.000243
L6	2	14335	18432	0	2048.250	0.031254	16383	16384	0	0.433	0.000007	16383	16384	0	0.433	0.000007
	3	5631	9728	0	1536.208	0.023441	8191	8192	0	0.331	0.000005	8191	8192	0	0.331	0.000005
	4	2047	5120	0	1024.125	0.015627	4095	4096	0	0.242	0.000004	4095	4096	0	0.242	0.000004
L7	2	57343	73728	0	8192.250	0.031251	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	22527	38912	0	6144.208	0.023438	32767	32768	0	0.331	0.000001	32767	32768	0	0.331	0.000001
	4	8191	20480	0	4096.125	0.015626	16383	16384	0	0.242	0.000001	16383	16384	0	0.242	0.000001
L8	2	57343	73728	0	8192.250	0.031251	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	22527	38912	0	6144.208	0.023438	32767	32768	0	0.331	0.000001	32767	32768	0	0.331	0.000001
	4	8191	20480	0	4096.125	0.015626	16383	16384	0	0.242	0.000001	16383	16384	0	0.242	0.000001
L9	2	229375	294912	0	32768.250	0.031250	262143	262144	0	0.433	0	262143	262144	0	0.433	0
	3	90111	155648	0	24576.209	0.023438	131071	131072	0	0.331	0	129024	133120	0	2047.875	0.001953
	4	32767	81920	0	16384.125	0.015625	65535	65536	0	0.242	0	63488	67584	0	1448.066	0.001381
L10	2	229375	294912	0	32768.250	0.031250	262143	262144	0	0.433	0	262143	262144	0	0.433	0
	3	90111	155648	0	24576.209	0.023438	131071	131072	0	0.331	0	131071	131072	0	0.331	0.000000
	4	32767	81920	0	16384.125	0.015625	65535	65536	0	0.433	0	65535	65536	0	0.433	0

Table A1: Distribution table for *F1* (2,3,4 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	5	80	416	0	80.056	0.009774	230	290	0	17.833	0.002177	242	270	0	7.300	0.000891
	6	16	256	0	48.606	0.005934	103	154	0	12.619	0.001541	114	146	0	7.977	0.000974
	7	4	128	0	28.873	0.003525	44	87	0	8.925	0.001090	47	78	0	6.863	0.000838
L2	5	80	416	0	80.056	0.009774	236	276	0	16.333	0.001994	242	272	0	7.860	0.000960
	6	16	256	0	48.606	0.005934	101	153	0	12.560	0.001533	111	145	0	7.719	0.000942
	7	4	148	0	28.873	0.003525	44	84	0	9.089	0.001110	45	84	0	6.732	0.000822
L3	5	320	1664	0	320.057	0.009768	731	1315	0	133.982	0.004089	1005	1043	0	10.263	0.000313
	6	64	1024	0	194.345	0.005931	347	700	0	78.005	0.002381	496	530	0	8.300	0.000253
	7	16	592	0	115.458	0.003524	166	380	0	44.269	0.001351	235	277	0	9.466	0.000289
L4	5	320	1664	0	320.057	0.009768	1007	1040	0	7.998	0.000244	980	1068	0	26.226	0.000800
	6	64	1024	0	194.345	0.005931	484	544	0	17.361	0.000530	464	562	0	22.664	0.000692
	7	16	592	0	115.458	0.003524	224	293	0	15.493	0.000473	213	297	0	16.530	0.000504
L5	5	640	3328	0	640.056	0.009767	2016	2096	0	22.628	0.000345	2012	2084	0	19.957	0.000305
	6	128	2048	0	388.664	0.005931	962	1086	0	26.131	0.000399	984	1056	0	15.796	0.000241
	7	32	1184	0	230.905	0.003523	462	561	0	19.939	0.000304	461	559	0	18.176	0.000277
L6	5	640	3328	0	640.056	0.009767	2029	2066	0	11.540	0.000176	2038	2058	0	8.271	0.000126
	6	128	2048	0	388.664	0.005931	1005	1049	0	9.765	0.000149	985	1065	0	18.788	0.000287
	7	32	1184	0	230.905	0.003523	483	538	0	10.089	0.000154	460	560	0	18.699	0.000285
L7	5	2560	13312	0	2560.056	0.009766	8184	8200	0	7.971	0.000030	8112	8272	0	65.932	0.000252
	6	512	8192	0	1554.580	0.005930	3985	4215	0	58.325	0.000222	3924	4268	0	66.576	0.000254
	7	128	4736	0	923.586	0.003523	1853	2258	0	88.290	0.000337	1922	2178	0	44.703	0.000171
L8	5	2560	13312	0	2560.056	0.009766	8128	8256	0	63.970	0.000244	8175	8208	0	16.032	0.000061
	6	512	8192	0	1554.580	0.005930	3900	4284	0	87.166	0.000333	4058	4134	0	20.095	0.000077
	7	128	4736	0	923.586	0.003523	1882	2189	0	64.085	0.000244	2002	2107	0	20.461	0.000078
L9	5	10240	53248	0	10240.057	0.009766	32255	33280	0	512.031	0.000488	30944	34592	0	923.516	0.000881
	6	2048	32768	0	6218.244	0.005930	15808	16960	0	367.671	0.000351	15056	17583	0	544.201	0.000519
	7	512	18944	0	3694.313	0.003523	7648	8768	0	273.423	0.000261	7448	8983	0	310.541	0.000296
L10	5	10240	53248	0	10240.057	0.009766	32608	32928	0	131.962	0.000126	32767	32768	0	0.174	0.000000
	6	2048	32768	0	6218.244	0.005930	16208	16560	0	94.671	0	16000	16768	0	383.984	0.000366
	7	512	18944	0	3694.313	0.003523	8058	8338	0	60.767	0.000058	7770	8614	0	272.083	0.000259

Table A2: Distribution table for *F1* (5,6,7 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	8	0	86	1	16.772	0.002048	19	51	0	5.985	0.000731	17	45	0	5.389	0.000658
	9	0	51	6	9.571	0.001168	6	30	0	4.157	0.000507	6	27	0	3.966	0.000484
	10	0	31	32	5.467	0.000667	1	18	0	2.885	0.000352	1	18	0	2.834	0.000346
L2	8	0	86	1	16.772	0.002048	17	50	0	6.148	0.000751	20	47	0	5.203	0.000635
	9	0	51	6	9.571	0.001168	5	29	0	4.222	0.000515	6	30	0	3.722	0.000454
	10	0	31	31	5.464	0.000667	0	20	1	2.695	0.000360	1	19	0	2.952	0.000329
L3	8	0	344	1	67.072	0.002047	72	209	0	25.263	0.000771	109	149	0	8.101	0.000247
	9	0	204	6	38.277	0.001168	22	120	0	15.297	0.000467	46	80	0	6.257	0.000191
	10	0	122	23	21.493	0.000656	6	70	0	9.221	0.000281	16	50	0	5.078	0.000155
L4	8	0	344	1	67.072	0.002047	103	157	0	10.895	0.000333	94	167	0	12.401	0.000378
	9	0	204	6	38.277	0.001168	42	90	0	8.225	0.000251	43	90	0	8.257	0.000252
	10	0	122	23	21.493	0.000656	14	55	0	5.815	0.000177	16	53	0	5.998	0.000183
L5	8	0	688	1	134.139	0.002047	214	301	0	15.502	0.000237	213	297	0	16.060	0.000245
	9	0	408	6	76.553	0.001168	94	163	0	11.628	0.000177	92	161	0	11.864	0.000181
	10	0	244	23	42.985	0.000656	41	89	0	8.370	0.000128	40	90	0	8.376	0.000128
L6	8	0	688	1	134.139	0.002407	226	294	0	11.147	0.000170	210	301	0	13.686	0.000209
	9	0	408	6	76.553	0.001168	105	163	0	9.271	0.000141	99	158	0	9.626	0.000147
	10	0	244	23	42.985	0.000656	44	88	0	7.254	0.000111	42	85	0	6.893	0.000107
L7	8	0	2752	1	536.542	0.002047	883	1192	0	64.860	0.000247	955	1105	0	27.813	0.000106
	9	0	1632	6	306.205	0.001168	385	650	0	43.728	0.000167	461	580	0	20.653	0.000079
	10	0	976	23	171.937	0.000656	167	373	0	29.149	0.000111	214	319	0	16.127	0.000062
L8	8	0	2752	1	536.542	0.002047	891	1130	0	42.693	0.000163	975	1066	0	17.374	0.000066
	9	0	1632	6	306.205	0.001168	423	600	0	28.488	0.000109	469	555	0	15.926	0.000061
	10	0	976	23	171.937	0.000656	203	320	0	19.132	0.000073	203	298	0	13.616	0.000052
L9	8	0	11008	1	2146.153	0.002047	3600	4784	0	210.909	0.000201	3572	4616	0	176.886	0.000169
	9	0	6528	6	1224.812	0.001168	1616	2584	0	136.766	0.000130	1740	2333	0	101.051	0.000096
	10	0	3904	23	687.745	0.000656	780	1352	0	83.062	0.000079	829	1204	0	59.001	0.000056
L10	8	0	11008	1	2146.153	0.002047	3894	4292	0	81.768	0.000078	3707	4512	0	175.030	0.000167
	9	0	6528	6	1224.812	0.001168	1886	2227	0	60.558	0.000058	1737	2381	0	106.320	0.000101
	10	0	3904	23	687.745	0.000656	918	1136	0	1562.605	0.000038	802	1263	0	65.158	0.000062

Table A3: Distribution table for *F1* (8,9,10 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	11	0	19	204	3.230	0.000394	0	12	41	2.007	0.000245	0	11	42	1.977	0.000241
	12	0	16	1011	2.004	0.000245	0	9	550	1.421	0.000173	0	9	530	1.392	0.000170
	13	0	10	3718	1.266	0.000155	0	7	3018	1.002	0.000122	0	7	2972	0.991	0.000121
L2	11	0	19	209	3.173	0.000387	0	13	45	2.070	0.000253	0	13	36	1.928	0.000235
	12	0	13	984	1.909	0.000233	0	9	586	1.459	0.000178	0	8	507	1.359	0.000166
	13	0	8	3597	1.203	0.000147	0	7	3087	1.028	0.000125	0	6	2913	0.973	0.000119
L3	11	0	73	79	11.812	0.000363	1	41	0	5.719	0.000176	5	29	0	3.817	0.000117
	12	0	48	300	6.544	0.000201	0	26	11	3.626	0.000111	0	19	1	2.752	0.000085
	13	0	28	1248	3.692	0.000113	0	18	248	2.307	0.000071	0	13	161	1.978	0.000061
L4	11	0	74	79	11.831	0.000363	2	35	0	4.372	0.000134	3	31	0	4.285	0.000132
	12	0	48	296	6.565	0.000202	0	22	6	3.042	0.000093	0	22	2	2.974	0.000091
	13	0	27	1224	3.751	0.000115	0	15	184	2.077	0.000064	0	14	158	2.046	0.000063
L5	11	0	148	79	23.817	0.000363	14	54	0	5.881	0.000090	14	55	0	5.894	0.000090
	12	0	94	240	13.068	0.000199	4	35	0	4.110	0.000063	4	37	0	4.217	0.000064
	13	0	53	751	7.152	0.000109	0	21	3	2.858	0.000044	0	23	6	2.932	0.000045
L6	11	0	148	79	23.817	0.000363	14	54	0	5.323	0.000081	16	51	0	5.192	0.000079
	12	0	94	240	13.068	0.000199	3	35	0	3.908	0.000060	4	30	0	3.824	0.000058
	13	0	59	777	7.189	0.000110	0	21	1	2.798	0.000043	0	20	1	2.772	0.000042
L7	11	0	592	79	95.266	0.000363	76	217	0	18.892	0.000072	89	177	0	11.747	0.000045
	12	0	376	240	52.273	0.000199	29	127	0	12.076	0.000046	37	94	0	8.260	0.000032
	13	0	222	668	28.458	0.000109	8	75	0	7.688	0.000029	12	54	0	5.753	0.000022
L8	11	0	592	79	95.266	0.000363	98	165	0	10.644	0.000041	98	169	0	10.031	0.000038
	12	0	376	240	52.273	0.000199	41	98	0	7.646	0.000029	39	98	0	7.439	0.000028
	13	0	222	668	28.458	0.000109	13	54	0	5.505	0.000021	13	55	0	5.337	0.000020
L9	11	0	2368	79	381.062	0.000363	344	716	0	48.442	0.000046	392	637	0	36.032	0.000034
	12	0	1504	240	209.091	0.000199	164	380	0	27.685	0.000026	182	343	0	22.633	0.000022
	13	0	888	668	113.832	0.000109	69	208	0	17.958	0.000017	81	185	0	14.614	0.000014
L10	11	0	2368	79	381.062	0.000363	435	603	0	25.343	0.000024	382	654	0	40.131	0.000038
	12	0	1504	240	209.091	0.000199	203	321	0	16.594	0.000016	180	353	0	24.896	0.000024
	13	0	888	668	113.832	0.000109	85	170	0	11.699	0.000011	78	205	0	15.543	0.000015

Table A4: Distribution table for *F1* (11, 12, 13 bit tuple)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	2	1920	2176	0	127.750	0.015596	2047	2048	0	0.433	0.000053	2047	2048	0	0.433	0.000053
	3	864	1183	0	95.792	0.011695	1023	1024	0	0.331	0.000040	984	1064	0	32.835	0.004009
	4	368	655	0	76.616	0.009354	480	544	0	19.597	0.002393	476	555	0	23.549	0.002875
L2	2	1920	2176	0	127.750	0.015596	2047	2048	0	0.433	0.000053	2047	2048	0	0.433	0.000053
	3	864	1183	0	95.792	0.011695	1007	1040	0	16.128	0.001969	992	1056	0	31.876	0.003892
	4	368	655	0	76.616	0.009354	492	548	0	19.989	0.002440	484	548	0	22.881	0.002793
L3	2	7680	8704	0	511.750	0.015618	8191	8192	0	0.433	0.000013	8191	8192	0	0.433	0.000013
	3	3456	4735	0	383.792	0.011713	3936	4256	0	131.788	0.004022	4095	4096	0	0.331	0.000010
	4	1472	2623	0	306.816	0.009364	1888	2239	0	98.509	0.003006	2047	2048	0	0.242	0.000007
L4	2	7680	8704	0	511.750	0.015618	8191	8192	0	0.433	0.000013	8191	8192	0	0.433	0.000013
	3	3456	4735	0	383.792	0.011713	3936	4256	0	131.788	0.004022	4095	4096	0	0.331	0.000010
	4	1472	2623	0	306.816	0.009364	1824	2240	0	113.084	0.003451	2015	2080	0	32.063	0.000979
L5	2	15360	17408	0	1023.750	0.015621	16383	16384	0	0.433	0.000007	16383	16384	0	0.433	0.000007
	3	6912	9471	0	767.792	0.011716	7969	8704	0	512.215	0.007815	8191	8192	0	0.331	0.000005
	4	2944	5247	0	613.749	0.009365	3520	4672	0	367.728	0.005611	3936	4256	0	129.923	0.001983
L6	2	15360	17408	0	1023.750	0.015621	16383	16384	0	0.433	0.000007	16383	16384	0	0.433	0.000007
	3	6912	9471	0	767.792	0.011716	8191	8192	0	0.331	0.000005	8160	8224	0	31.876	0.000486
	4	2944	5247	0	613.749	0.009365	4063	4128	0	32.063	0.000489	3920	4304	0	134.752	0.002056
L7	2	61440	69632	0	4095.750	0.015624	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	27648	37887	0	3071.792	0.011718	32767	32768	0	0.331	0.000001	30976	34560	0	1279.825	0.004882
	4	11776	20991	0	2455.348	0.009366	16383	16384	0	0.242	0.000001	14400	17983	0	942.673	0.003596
L8	2	61440	69632	0	4095.750	0.015624	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	27648	37887	0	3071.792	0.011718	32767	32768	0	0.331	0.000001	31488	34048	0	1055.364	0.004026
	4	11776	20991	0	2455.348	0.009366	16383	16384	0	0.242	0.000001	14944	17632	0	771.235	0.002942
L9	2	245760	278528	0	16383.75	0.015625	262143	262144	0	0.433	0	262143	262144	0	0.433	0
	3	110592	151551	0	12287.792	0.011719	131071	131072	0	0.331	0	125952	136192	0	4221.909	0.004026
	4	47104	83967	0	9821.746	0.009367	64256	66816	0	1055.561	0.001007	59904	70144	0	3028.938	0.002889
L10	2	245760	278528	0	16383.75	0.015625	262143	262144	0	0.433	0	262143	262144	0	0.433	0
	3	110592	151551	0	12287.792	0.011719	131071	131072	0	0.331	0	125952	136192	0	4221.909	0.004026
	4	47104	83967	0	9821.746	0.009367	65535	65536	0	0.242	0	59904	70144	0	3028.938	0.002889

Table A5: Distribution table for *F2* (2,3,4 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	5	176	356	0	42.977	0.005247	199	304	0	19.773	0.002414	217	287	0	17.793	0.002172
	6	44	204	0	36.315	0.004434	89	175	0	18.874	0.002304	91	155	0	13.881	0.001695
	7	16	122	0	22.242	0.002715	35	98	0	12.718	0.001553	43	86	0	9.168	0.001119
L2	5	176	356	0	42.977	0.005247	222	311	0	19.819	0.002420	225	302	0	18.612	0.002272
	6	44	204	0	36.315	0.004434	88	175	0	18.347	0.002240	104	151	0	13.106	0.001600
	7	16	122	0	22.242	0.002715	35	97	0	12.104	0.001478	43	87	0	8.851	0.001081
L3	5	704	1424	0	172.081	0.005252	982	1081	0	25.816	0.000788	981	1076	0	26.990	0.000824
	6	176	816	0	145.310	0.004435	451	690	0	44.625	0.001362	456	558	0	21.471	0.000655
	7	64	488	0	88.987	0.002716	189	389	0	29.324	0.000895	201	303	0	18.231	0.000556
L4	5	704	1424	0	172.081	0.005252	911	1093	0	53.792	0.001642	989	1062	0	21.262	0.000649
	6	176	816	0	145.310	0.004435	410	634	0	51.776	0.001580	352	800	0	76.536	0.002336
	7	64	488	0	88.987	0.002716	181	345	0	33.495	0.001022	158	474	0	49.283	0.001504
L5	5	1408	2848	0	344.221	0.005252	1926	2203	0	62.643	0.000956	1946	2166	0	55.637	0.000849
	6	352	1632	0	290.637	0.004435	592	1520	0	166.378	0.002539	856	1220	0	83.546	0.001275
	7	128	976	0	177.982	0.002716	237	803	0	100.244	0.001530	396	638	0	54.050	0.000825
L6	5	1408	2848	0	344.221	0.005252	1908	2143	0	59.277	0.000905	1922	2207	0	69.420	0.001059
	6	352	1632	0	290.637	0.004435	926	1150	0	49.829	0.000760	841	1117	0	83.802	0.001279
	7	128	976	0	177.982	0.002716	423	581	0	33.979	0.000518	398	645	0	54.112	0.000826
L7	5	5632	11392	0	1377.058	0.005253	8111	8285	0	47.568	0.000181	8063	8340	0	65.300	0.000249
	6	1408	6528	0	1162.601	0.004435	3832	4280	0	81.971	0.000313	3392	4752	0	355.949	0.001358
	7	512	3904	0	711.948	0.002716	1840	2304	0	94.994	0.000362	1514	2501	0	210.097	0.000801
L8	5	5632	11392	0	1377.058	0.005253	8122	8262	0	40.403	0.000154	7965	8415	0	108.488	0.000414
	6	1408	6528	0	1162.601	0.004435	4064	4144	0	19.609	0.000075	3480	4688	0	287.135	0.001095
	7	512	3904	0	711.948	0.002716	1930	2166	0	69.253	0.000264	1706	2467	0	166.347	0.000635
L9	5	22528	45568	0	5508.406	0.005253	29947	35580	0	1517.746	0.001447	30783	34896	0	1027.430	0.000980
	6	5632	26112	0	4650.454	0.004435	14336	17728	0	806.993	0.000770	13984	18847	0	1105.934	0.001055
	7	2048	15616	0	2847.813	0.002716	6928	9744	0	628.072	0.000599	6688	9919	0	633.344	0.000604
L10	5	22528	45568	0	5508.406	0.005253	32489	33063	0	123.809	0.000118	32665	32887	0	54.749	0.000052
	6	5632	26112	0	4650.454	0.004435	15432	17287	0	552.438	0.000527	14072	18631	0	1091.873	0.001041
	7	2048	15616	0	2847.813	0.002716	7338	9365	0	470.134	0.000448	6654	9781	0	619.964	0.000591

Table A6: Distribution table for *F2* (5,6,7 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	8	4	65	0	13.144	0.001605	13	55	0	8.235	0.001005	16	47	0	6.130	0.000748
	9	0	41	3	7.612	0.000929	4	34	0	5.257	0.000642	4	28	0	4.315	0.000527
	10	0	23	20	4.453	0.000544	0	21	3	3.433	0.000419	0	17	3	2.954	0.000361
L2	8	4	65	0	13.144	0.001605	13	50	0	7.712	0.000942	18	48	0	5.916	0.000722
	9	0	43	3	7.600	0.000928	4	34	0	5.176	0.000632	5	32	0	4.295	0.000524
	10	0	23	26	4.406	0.000544	0	19	1	3.389	0.000414	1	17	0	3.017	0.000368
L3	8	16	260	0	52.585	0.001605	84	228	0	19.052	0.000581	78	165	0	12.980	0.000396
	9	0	168	3	30.194	0.000921	32	138	0	12.019	0.000367	29	92	0	9.239	0.000282
	10	0	91	17	17.023	0.000520	13	85	0	7.845	0.000239	10	52	0	6.377	0.000195
L4	8	16	260	0	52.585	0.001605	77	199	0	21.110	0.000644	61	274	0	30.385	0.000927
	9	0	168	3	30.194	0.000921	181	345	0	33.495	0.001022	22	172	0	18.407	0.000562
	10	0	91	17	17.023	0.000520	10	64	0	8.375	0.000256	10	93	0	10.923	0.000333
L5	8	32	520	0	105.173	0.001605	82	438	0	58.361	0.000891	181	359	0	33.627	0.000513
	9	0	336	3	60.389	0.000921	33	234	0	33.437	0.000510	73	199	0	20.893	0.000319
	10	0	182	17	34.047	0.000520	12	142	0	19.703	0.000301	26	104	0	13.012	0.000977
L6	8	32	520	0	105.173	0.001605	197	317	0	22.883	0.000349	169	348	0	33.154	0.000506
	9	0	336	3	60.389	0.000921	92	182	0	15.111	0.000231	73	183	0	20.214	0.000308
	10	0	182	17	34.047	0.000520	37	102	0	10.328	0.000158	25	100	0	12.342	0.000188
L7	8	128	2080	0	420.701	0.001605	785	1257	0	83.011	0.000317	705	1349	0	123.493	0.000471
	9	0	1344	3	241.560	0.000921	351	691	0	56.403	0.000215	332	796	0	74.321	0.000284
	10	0	728	17	136.191	0.000520	154	382	0	35.718	0.000136	113	435	0	45.149	0.000172
L8	8	128	2080	0	420.701	0.001605	883	1195	0	62.774	0.000239	800	1266	0	95.444	0.000364
	9	0	1344	3	241.560	0.000921	420	627	0	42.630	0.000163	348	662	0	56.295	0.000215
	10	0	728	17	136.191	0.000520	184	340	0	26.877	0.000103	162	361	0	33.831	0.000129
L9	8	512	8320	0	1682.814	0.001605	3080	5415	0	412.356	0.000393	3218	5161	0	357.407	0.000341
	9	0	5376	3	966.245	0.000921	1370	3013	0	252.397	0.000241	1443	2666	0	203.722	0.000194
	10	0	2912	17	544.764	0.000520	577	1638	0	155.132	0.000148	636	1390	0	118.380	0.000113
L10	8	512	8320	0	1682.814	0.001605	3367	5138	0	314.488	0.000300	3221	5096	0	344.841	0.000329
	9	0	5376	3	966.245	0.000921	1502	2811	0	191.075	0.000182	1520	2640	0	190.614	0.000182
	10	0	2912	17	544.764	0.000520	647	1487	0	115.196	0.000110	711	1395	0	107.391	0.000102

Table A7: Distribution table for *F2* (8,9,10 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	11	0	16	161	2.657	0.000324	0	14	74	2.299	0.000281	0	12	56	2.057	0.000251
	12	0	10	843	1.644	0.000201	0	10	668	1.556	0.000190	0	9	601	1.436	0.000175
	13	0	7	3346	1.086	0.000133	0	7	3161	1.057	0.000129	0	6	3040	1.002	0.000122
L2	11	0	14	162	2.647	0.000323	0	12	61	2.242	0.000274	0	14	44	2.088	0.000255
	12	0	10	806	1.643	0.000201	0	10	650	1.526	0.000186	0	10	580	1.456	0.000178
	13	0	6	3324	1.084	0.000132	0	8	3158	1.050	0.000128	0	7	3075	1.022	0.000125
L3	11	0	51	68	9.453	0.000288	4	51	0	5.123	0.000156	2	34	0	4.425	0.000135
	12	0	31	242	5.257	0.000160	0	31	8	3.339	0.000102	0	21	4	3.076	0.000094
	13	0	18	980	3.028	0.000092	0	18	244	2.230	0.000068	0	15	219	2.130	0.000065
L4	11	0	52	68	9.461	0.000289	2	41	0	5.502	0.000168	0	53	1	6.564	0.000200
	12	0	32	234	5.239	0.000160	0	26	7	3.619	0.000110	0	34	24	4.085	0.000125
	13	0	20	936	3.078	0.000094	0	17	260	2.387	0.000073	0	23	354	2.270	0.000078
L5	11	0	103	66	18.882	0.000288	1	86	0	11.499	0.000175	9	64	0	8.110	0.000124
	12	0	63	207	10.410	0.000159	0	49	1	6.835	0.000104	3	38	0	5.169	0.000079
	13	0	35	682	5.775	0.000088	0	33	53	4.211	0.000064	0	24	11	3.360	0.000051
L6	11	0	103	66	18.882	0.000288	7	73	0	10.204	0.000156	9	57	0	7.598	0.000116
	12	0	59	209	10.471	0.000160	1	44	0	6.208	0.000095	2	38	0	4.847	0.000074
	13	0	37	724	5.838	0.000089	0	25	39	3.911	0.000060	0	23	6	3.221	0.000049
L7	11	0	412	66	75.528	0.000288	66	209	0	21.949	0.000084	41	234	0	27.148	0.000104
	12	0	240	205	41.456	0.000158	21	122	0	13.541	0.000052	18	134	0	17.138	0.000065
	13	0	146	579	22.540	0.000086	9	67	0	8.347	0.000032	3	87	0	10.604	0.000040
L8	11	0	412	66	75.528	0.000288	82	180	0	16.690	0.000064	62	206	0	20.278	0.000077
	12	0	240	205	41.456	0.000158	31	103	0	10.477	0.000040	23	123	0	13.141	0.000050
	13	0	146	579	22.540	0.000086	12	61	0	6.746	0.000026	8	78	0	8.319	0.000032
L9	11	0	1648	66	302.114	0.000288	256	882	0	91.641	0.000087	308	788	0	70.734	0.000067
	12	0	960	205	165.823	0.000158	106	483	0	56.768	0.000054	129	475	0	41.907	0.000040
	13	0	584	579	90.161	0.000086	41	284	0	34.374	0.000033	50	283	0	26.610	0.000025
L10	11	0	1648	66	302.114	0.000288	309	779	0	67.017	0.000064	314	744	0	62.724	0.000060
	12	0	960	205	165.823	0.000158	126	433	0	42.825	0.000041	142	410	0	36.351	0.000035
	13	0	584	579	90.161	0.000086	49	240	0	26.370	0.000025	64	255	0	23.290	0.000022

Table A8: Distribution table for *F2* (11, 12, 13 bit tuple)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	2	1920	2176	0	127.750	0.015596	2047	2048	0	0.433	0.000053	2047	2048	0	0.433	0.000053
	3	848	1135	0	97.181	0.011864	990	1058	0	31.947	0.003900	990	1058	0	31.931	0.003898
	4	376	615	0	67.075	0.008189	460	557	0	26.350	0.003217	471	548	0	23.546	0.002875
L2	2	1920	2176	0	127.750	0.015596	2015	2080	0	32.252	0.003937	2016	2080	0	31.752	0.003876
	3	848	1135	0	97.181	0.011864	986	1094	0	35.364	0.004317	990	1090	0	39.046	0.004767
	4	376	615	0	67.075	0.008189	464	556	0	26.843	0.003277	462	568	0	28.334	0.003459
L3	2	7680	8704	0	511.750	0.015618	8191	8192	0	0.433	0.000013	8191	8192	0	0.433	0.000013
	3	3392	4543	0	389.153	0.011876	4095	4096	0	0.331	0.000010	4087	4104	0	8.131	0.000248
	4	1504	2463	0	268.589	0.008197	2010	2086	0	26.025	0.000794	1990	2098	0	34.969	0.001067
L4	2	7680	8704	0	511.750	0.015618	8064	8320	0	127.750	0.003899	8191	8192	0	0.433	0.000013
	3	3392	4543	0	389.153	0.011876	3960	4232	0	90.698	0.002768	4088	4104	0	7.881	0.000241
	4	1504	2463	0	268.589	0.008197	1856	2168	0	74.954	0.002287	2011	2077	0	19.607	0.000598
L5	2	15360	17408	0	1023.750	0.015621	16383	16384	0	0.433	0.000007	16383	16384	0	0.433	0.000007
	3	6784	9087	0	778.450	0.011878	8191	8192	0	0.331	0.000005	8175	8208	0	16.128	0.000246
	4	3008	4927	0	537.275	0.008198	3989	4203	0	75.554	0.001153	3959	4217	0	76.380	0.001165
L6	2	15360	17408	0	1023.750	0.015621	16383	16384	0	0.433	0.000007	16128	16640	0	255.750	0.003902
	3	6784	9087	0	778.450	0.011878	8143	8240	0	48.126	0.000734	7904	8479	0	183.630	0.002802
	4	3008	4927	0	537.275	0.008198	3934	4210	0	83.065	0.001267	3899	4346	0	114.655	0.001750
L7	2	61440	69632	0	4095.750	0.015624	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	27136	36351	0	3114.230	0.011880	32767	32768	0	0.331	0.000001	32767	32768	0	0.331	0.000001
	4	12032	19711	0	2149.389	0.008199	16372	16396	0	11.940	0.000046	16267	16500	0	74.395	0.000284
L8	2	61440	69632	0	4095.750	0.015624	65535	65536	0	0.433	0.000002	65535	65536	0	0.433	0.000002
	3	27136	36351	0	3114.230	0.011880	32767	32768	0	0.331	0.000001	32576	32960	0	191.875	0.000732
	4	12032	19711	0	2149.389	0.008199	16383	16384	0	0.242	0.000001	16088	16680	0	156.879	0.000598
L9	2	245760	278528	0	16383.750	0.015625	262143	262144	0	0.433	0	258047	266240	0	4096.250	0.003906
	3	108544	145407	0	12457.354	0.011880	130816	131328	0	255.875	0.000244	126975	135168	0	2896.486	0.002762
	4	48128	78847	0	8597.845	0.008200	62368	68448	0	2136.422	0.002037	62511	68656	0	1774.376	0.001692
L10	2	245760	278528	0	16383.750	0.015625	262143	262144	0	0.433	0	262143	262144	0	0.433	0
	3	108544	145407	0	12457.354	0.011880	131071	131072	0	0.331	0	131071	131072	0	0.331	0.000000
	4	48128	78847	0	8597.845	0.008200	65312	65760	0	160.613	0.000153	65471	65600	0	64.063	0.000061

Table A9: Distribution table for *F3* (2,3,4 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	5	176	356	0	42.977	0.005247	199	304	0	19.773	0.002414	217	287	0	17.793	0.002172
	6	84	200	0	25.952	0.003168	96	165	0	13.255	0.001618	94	155	0	12.511	0.001527
	7	37	107	0	15.090	0.001842	42	94	0	9.329	0.001139	38	85	0	8.552	0.001044
L2	5	176	356	0	42.977	0.005247	222	311	0	19.819	0.002420	225	302	0	18.612	0.002272
	6	84	200	0	25.952	0.003168	99	166	0	13.349	0.001630	102	156	0	11.851	0.001447
	7	37	107	0	15.090	0.001842	48	86	0	8.013	0.000978	46	87	0	8.655	0.001057
L3	5	704	1424	0	172.081	0.005252	982	1081	0	25.816	0.000788	981	1076	0	26.990	0.000824
	6	336	800	0	103.894	0.003171	480	559	0	18.383	0.000561	478	575	0	19.895	0.000607
	7	148	428	0	60.408	0.001844	220	290	0	14.565	0.000444	228	301	0	14.887	0.000454
L4	5	704	1424	0	172.081	0.005252	911	1093	0	53.792	0.001642	989	1062	0	21.262	0.000649
	6	336	800	0	103.894	0.003171	420	569	0	37.495	0.001144	471	543	0	17.379	0.000530
	7	148	428	0	60.408	0.001844	195	316	0	24.917	0.000760	212	295	0	15.558	0.000475
L5	5	1408	2848	0	344.221	0.005252	1926	2203	0	62.643	0.000956	1946	2166	0	55.637	0.000849
	6	672	1600	0	207.817	0.003171	932	1134	0	42.299	0.000645	954	1098	0	36.066	0.000550
	7	296	856	0	120.831	0.001844	443	579	0	29.533	0.000451	442	572	0	25.480	0.000389
L6	5	1408	2848	0	344.221	0.005252	1908	2143	0	59.277	0.000905	1922	2207	0	69.420	0.001059
	6	672	1600	0	207.817	0.003171	913	1100	0	39.210	0.000598	938	1128	0	41.864	0.000639
	7	296	856	0	120.831	0.001844	442	572	0	25.577	0.000390	455	603	0	26.019	0.000397
L7	5	5632	11392	0	1377.058	0.005253	8111	8285	0	47.568	0.000181	8063	8340	0	65.300	0.000249
	6	2688	6400	0	831.356	0.003171	3965	4183	0	46.534	0.000178	3968	4273	0	50.730	0.000194
	7	1184	3424	0	483.372	0.001844	1960	2158	0	38.926	0.000152	1940	2184	0	40.198	0.000153
L8	5	5632	11392	0	1377.058	0.005253	8122	8262	0	40.403	0.000154	7965	8415	0	108.488	0.000414
	6	2688	6400	0	831.356	0.003171	3980	4176	0	40.491	0.000154	3867	4263	0	71.141	0.000271
	7	1184	3424	0	483.372	0.001844	1964	2138	0	32.524	0.000124	1897	2176	0	44.984	0.000172
L9	5	22528	45568	0	5508.406	0.005253	29947	35580	0	1517.746	0.001447	30783	34896	0	1027.430	0.000980
	6	10752	25600	0	3325.509	0.003171	14539	18756	0	943.309	0.000900	14832	18143	0	660.416	0
	7	4736	13696	0	1933.536	0.001844	6824	9730	0	555.135	0.000529	7067	9345	0	398.233	0.000380
L10	5	22528	45568	0	5508.406	0.005253	32489	33063	0	123.809	0.000118	32665	32887	0	54.749	0.000052
	6	10752	25600	0	3325.509	0.003171	16121	16620	0	105.154	0.000100	16031	16730	0	260.381	0.000248
	7	4736	13696	0	1933.536	0.001844	8025	8400	0	74.757	0.000071	7858	8566	0	189.267	0.000180

Table A10: Distribution table for *F3* function (5,6,7 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	8	14	59	0	8.926	0.001090	18	54	0	6.277	0.000766	13	49	0	5.885	0.000719
	9	5	33	0	5.347	0.000653	6	32	0	4.346	0.000531	3	28	0	4.008	0.000489
	10	1	23	0	3.389	0.000414	0	18	1	2.964	0.000362	1	17	0	2.782	0.000340
L2	8	12	63	0	8.765	0.001070	19	50	0	5.663	0.000691	18	47	0	5.793	0.000707
	9	6	37	0	5.279	0.000644	5	33	0	3.999	0.000488	5	30	0	4.027	0.000492
	10	0	23	1	3.355	0.000410	1	17	0	2.817	0.000344	1	22	0	2.846	0.000347
L3	8	55	228	0	34.430	0.001051	90	154	0	11.039	0.000337	102	167	0	10.849	0.000331
	9	22	121	0	19.253	0.000588	40	87	0	7.933	0.000242	45	92	0	7.742	0.000236
	10	7	72	0	10.811	0.000330	14	49	0	5.661	0.000173	16	52	0	5.592	0.000171
L4	8	58	228	0	34.430	0.001051	85	170	0	16.158	0.000493	95	157	0	11.646	0.000355
	9	22	121	0	19.253	0.000588	40	93	0	10.289	0.000314	45	93	0	8.344	0.000255
	10	9	75	0	10.866	0.000332	14	55	0	6.845	0.000209	16	50	0	5.865	0.000179
L5	8	116	456	0	68.868	0.001051	206	304	0	20.166	0.000308	209	298	0	17.707	0.000270
	9	44	242	0	38.510	0.000588	90	167	0	13.464	0.000205	96	162	0	12.166	0.000186
	10	17	144	0	21.282	0.000325	40	100	0	8.997	0.000137	38	88	0	8.423	0.000129
L6	8	116	456	0	68.868	0.001051	213	300	0	16.853	0.000257	202	322	0	17.163	0.000262
	9	44	242	0	38.510	0.000588	98	165	0	11.274	0.000172	92	173	0	11.676	0.000178
	10	17	144	0	21.282	0.000325	42	90	0	8.028	0.000122	41	93	0	8.068	0.000123
L7	8	464	1824	0	275.498	0.001051	943	1109	0	31.966	0.000122	950	1134	0	31.871	0.000122
	9	176	968	0	154.054	0.000588	441	586	0	25.601	0.000098	431	595	0	23.351	0.000089
	10	68	576	0	85.136	0.000325	201	318	0	18.480	0.000070	204	320	0	16.483	0.000063
L8	8	464	1824	0	275.498	0.001051	950	1139	0	28.871	0.000110	927	1105	0	32.782	0.000125
	9	176	968	0	154.054	0.000588	451	581	0	22.730	0.000087	427	588	0	23.031	0.000088
	10	68	576	0	85.136	0.000325	201	306	0	16.332	0.000062	196	308	0	16.002	0.000061
L9	8	1856	7296	0	1102.019	0.001051	3226	5052	0	315.350	0.000301	3388	4906	0	230.709	0.000220
	9	704	3872	0	616.230	0.000588	1521	2589	0	176.842	0.000169	1617	2483	0	130.778	0.000125
	10	272	2304	0	340.548	0.000325	689	1352	0	100.163	0.000096	768	1298	0	74.992	0.000072
L10	8	1856	7296	0	1102.019	0.001051	3916	5272	0	58.215	0.000056	3830	4383	0	120.261	0.000115
	9	704	3872	0	616.230	0.000588	1935	2201	0	42.025	0.000040	1841	2256	0	74.240	0.000071
	10	272	2304	0	340.548	0.000325	918	1133	0	30.240	0.000029	865	1159	0	45.913	0.000044

Table A11: Distribution table for *F3* (8,9,10 bit tuples)

LFSR feedback function	m-tuple	Consecutive Taps					Uneven Taps									
							T1					T2				
		Min	Max	No. non-occurring tuples	S.D.	S.D (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)	Min	Max	No.non-occurring tuples	S.D	S.D. (Ratio)
L1	11	0	14	37	2.206	0.000269	0	14	32	2.037	0.000249	0	11	42	1.985	0.000242
	12	0	10	581	1.504	0.000184	0	9	564	1.427	0.000174	0	8	570	1.403	0.000171
	13	0	8	3090	1.038	0.000127	0	6	3037	1.005	0.000123	0	5	3009	0.991	0.000121
L2	11	0	15	53	2.225	0.000272	0	13	41	1.991	0.000243	0	14	34	2.000	0.000244
	12	0	10	638	1.514	0.000185	0	8	564	1.407	0.000172	0	8	541	1.401	0.000171
	13	0	9	3152	1.043	0.000127	0	6	3051	1.002	0.000122	0	6	2990	0.989	0.000121
L3	11	3	41	0	6.218	0.000190	4	35	0	4.148	0.000127	4	32	0	3.976	0.000121
	12	0	28	7	3.739	0.000114	0	25	2	2.934	0.000090	0	20	2	2.785	0.000085
	13	0	16	261	2.369	0.000072	0	20	164	2.053	0.000063	0	14	144	1.974	0.000060
L4	11	2	45	0	6.295	0.000192	4	34	0	4.584	0.000140	1	31	0	4.132	0.000126
	12	0	30	6	3.788	0.000116	0	22	2	3.096	0.000094	0	19	4	2.902	0.000089
	13	0	17	244	2.375	0.000072	0	13	193	2.116	0.000065	0	14	171	2.044	0.000062
L5	11	6	83	0	11.846	0.000181	15	55	0	6.028	0.000092	13	53	0	5.863	0.000089
	12	1	51	0	6.782	0.000103	5	32	0	4.150	0.000063	3	31	0	4.087	0.000062
	13	0	32	25	4.019	0.000061	0	22	4	2.906	0.000044	0	20	0	2.868	0.000044
L6	11	6	80	0	11.876	0.000181	16	52	0	5.661	0.000086	17	54	0	5.649	0.000086
	12	0	46	2	6.770	0.000103	4	31	0	4.038	0.000062	4	32	0	3.977	0.000061
	13	0	28	31	4.038	0.000062	0	21	1	2.843	0.000043	0	21	1	2.811	0.000043
L7	11	30	320	0	46.566	0.000178	84	175	0	13.072	0.000050	88	175	0	11.632	0.000044
	12	8	188	0	25.258	0.000096	34	98	0	8.966	0.000034	34	98	0	8.213	0.000031
	13	1	114	0	13.766	0.000053	12	56	0	6.076	0.000023	12	55	0	5.753	0.000022
L8	11	30	320	0	46.566	0.000178	92	163	0	11.429	0.000044	86	166	0	11.389	0.000043
	12	8	188	0	25.258	0.000096	37	94	0	8.059	0.000031	37	96	0	8.062	0.000031
	13	3	119	0	13.766	0.000053	12	60	0	5.694	0.000022	14	57	0	5.679	0.000022
L9	11	120	1280	0	186.265	0.000178	305	733	0	57.276	0.000055	375	674	0	43.603	0.000042
	12	32	752	0	101.033	0.000096	139	411	0	33.462	0.000032	168	352	0	25.984	0.000025
	13	14	448	0	54.409	0.000052	61	239	0	19.903	0.000019	79	131	0	15.866	0.000015
L10	11	120	1280	0	186.265	0.000178	445	609	0	21.915	0.000021	408	630	0	28.819	0.000027
	12	32	752	0	101.033	0.000096	201	309	0	15.680	0.000015	193	335	0	18.564	0.000018
	13	14	448	0	54.409	0.000052	87	169	0	11.113	0.000011	90	181	0	12.372	0.000012

Table A12: Distribution table for *F3* (11, 12, 13 bit tuple)