APPLICABILITY OF SIMPLE POWER ANALYSIS TO STREAM CIPHERS CONSTRUCTED USING MULTIPLE LFSRS

Abdulah Abdulah Zadeh, H. M. Heys

Electrical and Computer Engineering
Memorial University of Newfoundland
a.zadeh@mun.ca , hheys@mun.ca

ABSTRACT

In recent years, the hardware implementation of stream ciphers has attracted the interest of many designers, mainly due to their low implementation area on a chip. However, to date, in comparison with block ciphers, side channel attacks have not been extensively analyzed for their applicability to stream cipher hardware implementations. However it has been shown that simple power analysis attacks are applicable to stream ciphers based on one linear feedback shift register. In this paper, we extend the SPA method to stream ciphers with multiple linear feedback shift registers and multiple linear feedback shift registers with irregular clocking. Then we apply the proposed method to the well-known stream ciphers E0 and LILI-128.

Index Terms— Stream cipher, Simple Power Analysis, E0, LILI-128

1. INTRODUCTION

The hardware realization of many stream ciphers is more efficient than many common block ciphers, often requiring less area on chip. Because of this advantage, stream ciphers are known as good candidates for devices in constrained environments, such as RFID tags, wireless communication devices and smart cards [1,2].

A side channel attack is based on information gained from the physical implementation of a cryptosystem, such as timing information [3] power consumption [4] or electromagnetic leaks [5,6]. Some side channel attacks have been used to attack stream ciphers. For example, the template attack [7] can be applied by acquiring a device similar to one under attack and building a template of information based on power consumption for every possible key. Then capturing a trace of information (such as power consumption over time) and comparing to the templates, the correct key can be determined as the most likely one given the outcome of comparisons. In [8], the fault attack has been used to attack different stream ciphers. A fault attack considers the information resulting from the injection of faults in the cipher hardware. In [9], a scan chain based attack has been proposed. Also in [10-11], differential power analysis attack is reviewed for its applicability to stream ciphers.

Recently, the applicability of a simple power analysis, SPA, attack on stream ciphers has been identified in [12]. The proposed method is applicable to stream ciphers with just one linear feedback shift register (LFSR). Since a number of modern stream ciphers use more than one LFSR, the direct methodology in [12] has limited applicability. In this paper, we propose a method based on simple power analysis to attack stream ciphers with multiple LFSRs such as E0 [13]. Further, we consider the applicability of the attack to irregular clocking stream ciphers by examining LILI-128 [14].

2. BACKGROUND

In this section, we introduce some of the basic background of stream cipher construction and power analysis.

2.1. Linear Feedback Shift Register

LFSRs are widely used as a component of a key stream generator in many proposed stream ciphers, due to their simple hardware structure and the good pseudo-random properties of the generated sequence. A right-shifting LFSR of length L consists of L bits and the output of each step (i.e., as the result of a clock) is the least significant bit (equal to right most bit). The bit values are shifted to the right at each step (i.e., on the rising edges of the clock, assuming positive edge-triggered register flip-flops), and the most significant bit is injected into the left most bit of the register after being produced as a linear combination of bits currently stored in the bit registers. It is well known that if the feedback is chosen as a primitive polynomial, the LFSR can make a sequence of bits with a maximal period of 2^{L-1}. Since the register bit values and resulting outputs are generated from the linear combination of the previous L bit values, the output sequence of the LFSR is easily predictable from previous outputs after L steps.

The general structure of an LFSR is shown in Fig.1, where each square represents a register bit or D-Flip-Flop.

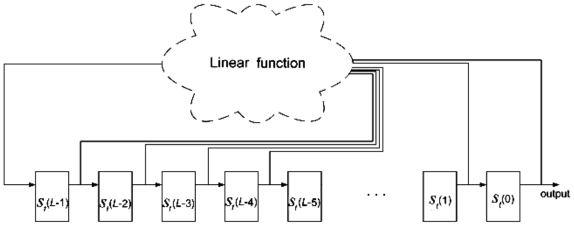

Figure 1. The overall architecture of LFSR.

2.2. Power Dissipation in Electronic Circuits

The total power dissipation of a CMOS integrated circuit is divided into two parts: static and dynamic power consumption [15]. The static power dissipation is the power which is consumed in transistors as leakage current. Dynamic power consumption is due to the current that flows only when the transistors of the device are switching from one logic state to another. This current flows to charge or discharge the peripheral capacitances, mostly gate, drain and wire capacitances. The frequency at which the device is switching (for example, the clock frequency in a synchronous sequential logic circuit), the rise and fall times of the input signal, and the length of a gate have a direct effect on the duration of the current spike and its amount. For circuits clocked at reasonably high frequencies, the leakage current of the gate is negligible compared to the switching current. In the majority of electronic devices, the dynamic supply current is dominant in CMOS circuits and most of the power is consumed in moving charges in the parasitic capacitance in the CMOS gates. Hence, for high speed devices dynamic power consumption is the most significant contributor in a hardware circuit realization in CMOS technology.

2.3. Simple Power Analysis (SPA) Attack

In a simple power analysis attack, the attacker has the ability to measure the power consumed by the cryptosystem. This can be approached by putting a small resistor in series between the power supply and power input pin (or alternatively, the ground and ground pin) of the device. Using a high speed oscilloscope, the attacker can measure over time the input (or output) current which is proportional to the overall power consumption of the device. Since the dynamic power dissipation is the major consumed power in high speed circuits, sampling the consumed power gives an idea of the number of switching transistors. This information then can be used to identify characteristics of the data within the device and in the appropriate circumstances reveal secret information (such as the key) of a cipher implemented within the device.

In the approach taken in this paper, as well as others such as [16-18], the measured power consumption at the rising edge of the clock is taken as proportional to the number of bit registers changed in the system at that point in time. This is referred to as the Hamming distance based power model. By taking samples of power data at the clock edges of synchronous digital hardware, this can reveal information about data stored in the registers during particular operations of the cipher; this information is exploited to determine the state values of the LFSRs used in the stream ciphers analyzed in this paper.

2.4. Review of SPA on LFSR-based Stream Ciphers

We first consider the attack proposed in [12] that is applicable to stream ciphers based on one LFSR and a nonlinear combining function. The key in such a system is represented by the initial state bits of the LFSR. During each clock cycle each bit value is shifted to the right. Changing the value of each bit in the register causes dynamic power consumption as mentioned above. We refer to the L-bit value of the register as the state. At clock cycle t, the current state is represented as S_t and the state for the next clock cycle is given as S_{t+1}. The Hamming distance between S_t and S_{t+1} is given as HD_t where HD_t is calculated from:

$$HD_t = \sum_{i=0}^{L-1}(s_t(i) \oplus s_{t-1}(i)) \qquad (1)$$

where $s_t(i)$ represents the value of bit i of S_t with $s_t(0)$ being the right most bit of the LFSR and $\oplus$ represents exclusive-OR.

According to the Hamming distance power model used in the attack [12], the dynamic power consumption of the cipher at clock cycle t is proportional to HD_t. Between two successive clock cycles it can be shown that the difference between the Hamming distances must be one of three values: $HD_{t+1} - HD_t \in \{-1,0,1\}$. Defining the power difference to be PD_t given by:

$$PD_t = HD_{t+1} - HD_t. \qquad (2)$$

It can be seen that PD_t is proportional to the difference of dynamic power consumption at two consecutive clock cycles or measured power difference, PD_t^m. In other word, $PD_t^m \propto PD_t$. Substituting (1) into (2) results in:

$$PD_t = [s_t(L) \oplus s_t(L-1)] - [s_t(0) \oplus s_{t-1}(0)]. \qquad (3)$$

where the new bit value for state $t+1$, $s_{t+1}(L-1)$, is also denoted as $s_t(L)$ and will be the new value of bit $L-1$ based on current bit values of state S_t. Considering operations over $GF(2)$, we can write

$$|PD_t| = s_t(L) \oplus s_t(L-1) \oplus s_t(0) \oplus s_{t-1}(0). \qquad (4)$$

If the measured dynamic power consumption of the LFSR at clock cycle t is equal to the measured dynamic power consumption at clock cycle $t+1$ (that is, $PD_t^m = 0$), then

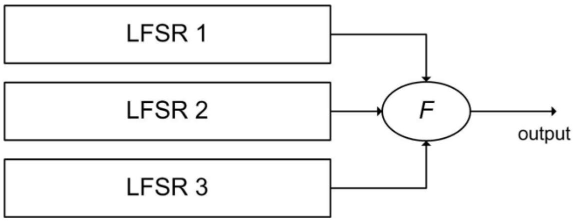

Figure 2. A stream cipher key-stream generator with three LFSRs.

we can conclude $PD_t = 0$ and write $s_t(L) \oplus s_t(L-1) \oplus s_t(0) \oplus s_{t-1}(0) = 0$ and if the measured dynamic power consumption at time t and $t+1$ are not equal (that is, $PD_t^m \neq 0$), we can conclude $PD_t \neq 0$ and write $s_t(L) \oplus s_t(L-1) \oplus s_t(0) \oplus s_{t-1}(0) = 1$.

It is known that, for any t, the bit values of $\mathrm{S_t}$ can be written as a linear function of the S_0 bits, $\{s_t(i)\}$, where $0 \leq i < L$. Hence, for a stream cipher constructed from one LFSR and a nonlinear combining function, using L power difference values, it is straightforward to find the initial L bit values of the LFSR and thereby determine the key stream sequence [1]. For this purpose, we can collect enough current samples to derive L power difference values and write L equations similar to equation (4), relating S_t through the linear expressions of the LFSR to the bits of S_0. Then we have a linear system of equations with L unknown variables and L equations, which is easily solved to determine the key, i.e. the initial state of the LFSR, S_0.

3. EXTENSION OF SPA TO CIPHERS WITH MULTIPLE LFSRS

Consider now stream ciphers constructed from multiple LFSRs and a nonlinear combining function. We now consider the novel extension of the attack in [12] to such ciphers. A system with three LFSRs is illustrated in Fig.2, where F represents a nonlinear combining function.

For simplicity in the discussion, let us assume a stream cipher with two LFSRs, $LFSR_s$ and $LFSR_R$, and bit values $s_t(i)$ and $r_t(i)$ where $0 \leq i < M$ and $0 \leq i < N$ where M and N are the sizes of the LFSRs. The overall power difference of two LFSRs, $PD_t = HD_{t+1} - HD_t$, at each clock can now be from $\{-2, -1, 0, +1, +2\}$. Since each LFSR could have a power difference of -1, 0 or $+1$, if the power difference for both LFSRs is the same and equal to -1 or $+1$, then the overall PD_t is -2 or $+2$, respectively.

Although values of $PD_t = +2$ or -2 indicate that both LFSRs must have non-zero power differences, other values of overall PD_t will not get us any useful information about the individual LFSRs. For example, if the overall $PD_t = 0$, we cannot conclude whether both LFSR power differences are equal to zero or the power difference for one LFSR is equal to -1 and for the other one is equal to +1. Also, if the overall $PD_t = \pm 1$, we cannot distinguish for which LFSR the power difference is zero and for which LFSR the power difference is nonzero. However, for each clock cycle where overall $PD_t = \pm 2$, based on equation (4), we can conclude:

$$\begin{aligned} s_{t-1}(0) \oplus s_t(0) \oplus s_{t-1}(M) \oplus s_t(M) = 1 \\ r_{t-1}(0) \oplus r_t(0) \oplus r_{t-1}(N) \oplus r_t(N) = 1 \end{aligned} \qquad (5)$$

where $s_t(i)$ and $r_t(i)$ represent the i-th bits of LFSR states at clock cycle t.

To break the stream cipher, we need to determine the $M+N$ bits of the LFSRs at a particular point in time. Hence, we require enough power difference values with $PD_t = \pm 2$ to obtain linear equations using (5) to solve for $M+N$ unknown variables. The minimum number of power difference values to set up the $M+N$ equations is M (if $M > N$) or N (if $N > M$). However, the minimum is unlikely to be achieved since usable power difference values must satisfy $PD_t = \pm 2$.

When we measure the consumed power of the circuit we should observe roughly five levels of power difference. The largest negative one should be assigned to $PD_t = -2$ and the largest positive should be assigned to $PD_t = +2$.

The probability of a particular overall $PD_t = \pm 2$ is equal to 1/8, since this occurs when the individual shift registers both have power differences of $+1$ or -1, each of which occurs with a probability of 1/4. Hence, on average, we require $8 \times max\{M, N\}$power difference values to derive $M+N$ equations. Letting $T = max\{M, N\}$, given n power difference values, it can be shown that the probability that there are enough usable power differences to form T equations is given by

$$Q_T(n) = \sum_{i=T}^{n} \binom{n}{i} \left(\frac{7}{8}\right)^{n-i} \left(\frac{1}{8}\right)^{i} \qquad (6)$$

Hence, for $T = 80$ and 800 power difference values, the probability that 80 equations can be derived is $Q_{80}(800) = 98.77\%$. Assuming that all equations derived from the power differences are linearly independent, we can solve the system for the $M+N$ initial state bits of the two LFSRs by using two systems of equations. The systems of equations are linear and can be solved using appropriate mathematical tools such as Sage [19]. However, the equations derived from the power difference values and the feedbacks are not necessarily all linearly independent. In fact, for an L-bit LFSR, given k randomly generated linear equations of the LFSR initial state bit values, from [20] the probability that all k equations are linearly independent is

$$P_L(k) = \frac{\prod_{i=0}^{L-1}(2^L - 2^i)}{k! \times \binom{2^L-1}{k}} \qquad (7)$$

for $k \leq L$. If $k = L$, then $P_L(k)$ gives the probability that L randomly selected equations is enough to solve for the LFSR initial state bits. For example, for $k = L = 80$,

$P_{80}(80) = .289$, implying that, with 80 equations, there is a 28.9% chance of being able to solve uniquely for the 80 state bits of the LFSR. Hence, in general, to ensure that we have a high probability of solving for $M + N$ bits when attacking the cipher based on two LFSRs, we should obtain somewhat more than $max\{M, N\}$ equations from the power differences.

In Appendix, we develop a method to calculate a lower bound on the probability, given k randomly generated linear equations with $k > L$, of being able to fully solve the system. For example, if $L = 80$, it can be shown that obtaining 120 random equations will give a probability of over 99.99% of being able to solve for the 80 unknowns. Hence, for the cipher based on two LFSRs, if $max\{M, N\} =$ 80 bits, then, from equation (6), 1200 power difference values will give a 98.99% probability of obtaining 120 equations, which according to the analysis of Appendix, will give a probability of 99.99% of being solvable for the LFSR initial state bit values. Hence, for ciphers based on two LFSRs of sizes 80 bits and less, 1200 power samples will give a very high probability of being able to successfully apply SPA.

4. APPLICATION OF THE ATTACK TO THE E0 STREAM CIPHER

The E0 stream cipher [13] is a well-known stream cipher, used in Bluetooth which is used in short range, high speed communications such as mobile cell phones, PCs, and computer accessories. It is based on four LFSRs ($LFSR_a$, $LFSR_b$, $LFSR_c$, $LFSR_d$) with lengths of 25, 31, 33 and 39 bits [13]. In addition to four LFSRs, four bit registers save the state of the cryptosystem as part of the nonlinear combining function. Hence, the equations used in the simple power analysis should be expanded to these four register bits. The output bit is a combination, derived from the current bit values of LFSRs and the former state or register values.

Since at each clock, four LFSRs and four register bits could be changed, the overall PD_t can be from $\{\pm 8, \pm 7, \pm 6, \pm 5, \pm 4, \pm 3, \pm 2, \pm 1, 0\}$. The useful or valid power differences are $PD_t = \pm 8$. When $PD_t = \pm 8$, we can conclude:

$$\begin{aligned}
&a_{t-1}(0) \oplus a_t(0) \oplus a_{t-1}(25) \oplus a_t(25) = 1 \\
&b_{t-1}(0) \oplus b_t(0) \oplus b_{t-1}(31) \oplus b_t(31) = 1 \\
&c_{t-1}(0) \oplus c_t(0) \oplus c_{t-1}(33) \oplus c_t(33) = 1 \\
&d_{t-1}(0) \oplus d_t(0) \oplus d_{t-1}(39) \oplus d_t(39) = 1
\end{aligned} \tag{8}$$

where a, b, c and d represent LFSR state bits. In addition, four equations can be written for the four register bits of the combiner.

Noting that the largest LFSR size is 39 bits based on the discussions in former section and Appendix, using 60 useful power difference values (i.e., $PD_t = \pm 8$), with the probability of more than 99.2%, we can find 39 linearly independent equations to solve $LFSR_d$. To find 60 useful power differences, modified equations (6) and (7) for E0, shows 160000 power difference values with the probability of 98.0% is enough. Hence, with very high probability, 160000 power samples are enough to attack E0. Once the LFSR bit values are known, the four combining function state bits can be determined by exhaustively testing each possible value.

5. APPLICABILITY TO LILI-128

So far we have described an SPA attack on stream ciphers with regular clocks. In this section, we use SPA to attack a non-regular clocking LFSR stream cipher, LILI-128 [14].

In LILI-128, two LFSRs are employed ($LFSR_c$, $LFSR_d$) to generate a random sequence. $LFSR_c$ is 39 bits in length and controls the clock of $LFSR_d$ which is 89 bits in length. The bit values of $c_t(12)$ and $c_t(20)$ in $LFSR_c$ are passed through a function with two bits output, to determine whether $LFSR_d$ should be clocked one, two, three or four times to produce key stream bits [14]. Since it is not known how many bits $LFSR_d$ is being clocked to produce each output bit, we cannot directly approach the equations for $LFSR_d$. Hence, at first we should find the bit values of $LFSR_c$.

Two different architectures have been offered for LILI-128 [14]. In the first architecture, two clocks are employed with different speeds. The first clock is used for $LFSR_c$ and the second one is for $LFSR_d$ which is four times faster. If $c_t(12) = 1$ and $c_t(20) = 1$, then $LFSR_d$is clocked four times. To use SPA and set up the equations, we should wait until $PD_t = \pm 2$ for the first clock (i.e. the clock driving $LFSR_c$). When $PD_t = \pm 2$, we can write:

$$c_t(39) \oplus c_{t-1}(39) \oplus c_t(0) \oplus c_{t-1}(0) = 1 \tag{9}$$

No information can be obtained for $LFSR_d$, because t is not known for $LFSR_d$. Hence, at this point we cannot find any equation for $LFSR_d$. More information could be obtained by considering power consumption correlated to the $LFSR_d$ clock. If power consumption could be observed for $LFSR_d$ between two consecutive clocks of $LFSR_c$indicating four shifts of $LFSR_d$ we can conclude:

$$\begin{aligned}
&c_t(12) = 1 \\
&c_t(20) = 1
\end{aligned} \tag{10}$$

Using equation (9) and (10), we can set up a system of linear equations to find the bit values of $LFSR_c$. Finding the bit values of $LFSR_c$, we can use the former power difference values to find the equations for bit values of $LFSR_d$.

In the second offered architecture for LILI-128 [14], just one clock has been used for both LFSRs. $LFSR_d$ is implemented using four copies of the feedback function and the irregular clocking is performed in one clock cycle. For this architecture, equation (10) can not be used; hence just equation (9) could be employed to realize $LFSR_c$ bit values.

Since the size of $LFSR_c$ is 39 bits, 60 equations with the probability of more than 99.2% can provide 39 linearly independent equations. In the second architecture, 600 power samples can provide 60 usable power difference values, with the probability of 97.5%. Hence, the second architecture is susceptible to SPA with 600 power samples with high probability. In the first architecture with the probability of 1/8, equation (9) can be obtained and with the probability of (1/8) ×(1/2) equation (10) can be employed in the system. After collecting 300 power samples, with the probability of more than 98.2%, 60 equations can be obtained to solve state bits of $LFSR_c$.

When bit registers of $LFSR_c$ are known, finding bit registers of $LFSR_d$ is similar to using SPA to attack one LFSR proposed in [12]. To break $LFSR_d$, if we collect 110 equations, with the probability of more than 99% we will have 89 linearly independent equations.

6. CONCLUSION

In this paper we have extended the former method of simple power analysis attack proposed for one LFSR-based stream ciphers to ciphers based on multiple LFSRs. Also, we extend the proposed method to stream ciphers with irregular clocking LFSRs.

In order to use the proposed methods, we applied them to well known stream ciphers E0 which includes four LFSRs and four bit registers and LILI-128 which includes two LFSRs, one with irregular clocking. We have shown that E0 could be broken with probability of 98%, using 16000 power samples and LILI-128 is susceptible to SPA, with the probability of 98% with 300 power samples.

7. REFERENCES

[1] Angela Barbero, Greg Horler, Alexander Kholosha, Oyvind Ytrehus, “Lightweight Cryptography for RFID Devices”, *International Conference on Wireless Mobile and Multimedia Networks 2008 IET*, pp. 294-297 (2008).

[2] Nicolas Fournel, Marine Minier, Stephane Ubeda, “Survey and Benchmark of Stream Ciphers for Wireless Sensor Networks”, *Information Security Theory and Practices, Smart Cards, Mobile and Ubiquitous Computing Systems, LNCS*, vol. 4462, pp.202-214 (2007).

[3] Paul C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, *16th Annual International Cryptology Conference (CRYPTO), LNCS*, vol.1109, pp.104-113 (1996).

[4] Paul C. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology Crypto '99, LNCS*, vol.1666, pp. 388-397 (1999).

[5] Jean-Jacques Quisquater, David Samyde, “Simple Electromagnetic Analysis for Smart Cards, New Results, Rump”, *session talk at Cyrpto* (2000).

[6] K. Gandolfi, C. Mourtel, F. Olivier, “Electromagnetic Attacks: Concrete Results”, *Cryptographic Hardware and Embedded Systems - CHES 2001, LNCS*, vol. 2162, pp. 251-261 (2001).

[7] C. Suresh, Josyula R. Rao, Pankaj Rohatgi, “Template Attacks”, *Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS*, vol.2523, pp.51—62, (2003).

[8] Jonathan Hoch, Adi Shamir, “Fault Analysis of Stream Ciphers”, *Cryptographic Hardware and Embedded Systems - CHES 2004, LNCS*, vol. 3156, pp. 1-20, (2004).

[9] Mukesh Agrawal, Sandip Karmakar, Dhiman Saha, Debdeep Mukhopadhyay, “Scan Based Side Channel Attacks on Stream Ciphers and Their Counter-Measures”, *Progress in Cryptology - INDOCRYPT 2008, LNCS*, vol. 5365, pp. 226 -235, (2008).

[10] Wieland Fischer, Berndt M. Gammel, Oliver Kniffler, Joachim Velten, “Differential Power Analysis of Stream Ciphers”, *Topics in Cryptology, CT-RSA 2007, LNCS*, vol. 4377, pp. 257-270, (2007).

[11] J. Lano, N. Mentens, B Preneel, I. Verbauwhede, “Power Analysis of Synchronous Stream Ciphers with Resynchronization Mechanism”, *The State of the Art of Stream Ciphers SASC 2004*, pp. 327-333 (2004).

[12] S. Burman, et. al., “LFSR Based Stream Ciphers are Vulnerable to Power Attacks”, *INDOCRYPT 2007, Lecture Notes in Computer Science, LNCS*, vol. 4859, pp. 384-392, (2007).

[13] Specification on the Bluetooth System, version 1.1 (2001).

[14] E. Dawson, A. Clark, J. Goli´c, W. Millan, L. Penna, L. Simpson, “The LILI-128 Keystream Generator”, *Selected Areas in Cryptography, LNCS*, vol. 2012, pp. 248-261 (2001).

[15] Amara Amara, Frederic Amiel, Thomas Ea, “FPGA vs. ASIC for Low Power Applications”, *Microelectronics Journal, Elsevier*, vol. 37, pp. 669-677 (2006).

[16] F. X. Standaert, E. Peeters, G. Rouvroy, J. J. Quisquater, “An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays”, *Proceedings of the IEEE*, vol.94, pp. 383-394, (2006).

[17] S. B.Ors, E. Oswald, B. Preneel, “Power Analysis Attacks on an FPGA-First Expeimental Results”, *Cryptographic Hardware*

and Embedded System - CHES 2003, LNCS, vol. 2279, pp. 35-50, (2003).

[18] S. B.Ors, E. Oswald, B. Preneel, “Power Analysis Attacks on an ASIC AES Implementation”, *Proceeding of ITCC 2004, IEEE*, vol. 2, pp. 546-554, (2004).

[19] Sage: Open Source Mathematics Software, available at: http://www.sagemath.org/

[20] C. L. Chen, “Linear Dependencies in Linear Feedback Shift Registers”, *IEEE Transactions on Computer*, vol.35, pp. 1086-1986 (1986).

APPENDIX

Define $\mathrm{P_L(i,k)}$ to represent the probability that, given k bits randomly selected from a sequence generated by an L-bit LFSR, it is possible to generate a set of i linearly independent equations. From [20], for $\mathrm{k \leq L}$, $\mathrm{P_L(k,k)}$ can be generated:

$$P_L(k,k) = \frac{\prod_{i=0}^{L-1}(2^L-2^i)}{k!\times\binom{2^L-1}{k}} \qquad (11)$$

We are interested in situations where $k > L$ and $i = L$. Although we will not compute the probability directly in this case, we will derive a lower bound on $P_L(L,k)$ for $k > L$.

Consider a set of $k-1$ linear equations, $k > L$, formed from bits randomly selected from the sequence of an L-bit LFSR with the unknown variables being the initial L bits of the LFSR. Assume within the set of $k-1$ linear equations, there is a subset of $i-1$ equations, $i \leq L$, that are linearly independent. Following the arguments presented in [20], the probability of randomly selecting a k-th linear equation that is linearly independent of all equations in the subset so that a subset of i linearly independent equations is formed is given by:

$$\Gamma_L(i,k) = \frac{(2^L-2^{i-1})}{(2^L-k-2)}. \qquad (12)$$

The denominator represents the total number of equations left from which the k-th equation is drawn and the numerator represents the number of equations left which are linearly independent of the equations in the subset. The denominator and numerator are formed by considering that there are a total of 2^{L-1} linear equations of L variables and there are $2^{i-1}-1$ equations that are not linearly independent of the subset of $i-1$ equations. We are specifically interested in cases where $k \ll 2^{L-1}$ and, hence, since $i \leq L$, it is easy to see that $\Gamma_L(i,k) \geq .5$ and $\Gamma_L(i,k) \cong .5$ occurs for $i = L$.

In order to calculate the lower bound on $P_L(L,k)$ for $k > L$, we can use

$$P_L(L,k) \geq \max\{P_L(j,j) \times \beta_L(j,k)\} \;\; (0 < j \leq L) \qquad (13)$$

where $P_L(j,j)$ is given by (19) and $\beta_L(j,k)$ is the probability of adding $L-j$ more linear equations to the set of linearly independent equations given $k-j$ more randomly selected equations. Since $\Gamma_L(i,k) \geq .5$, we can compute a lower bound on β_L using the binomial distribution:

$$\beta_L(j,k) \geq \sum_{i=L-j}^{k-j}\binom{k-j}{i}.5^{k-j} \qquad (14)$$

Using two equations, (13) and (14), we can estimate the lower bound on $P_L(L,k)$ for $k > L$. In Fig.3, the lower bound on $P_L(L,k)$ for different values of $k-L$ and $L = 80$ has been shown.

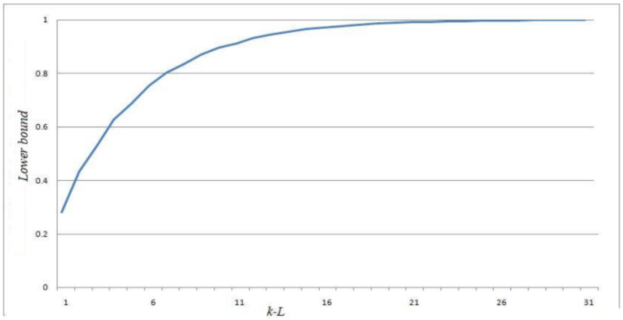

Figure 3. Lower bound on $P_L(L,k)$values for $L = 80$ and $k-L \leq 30$.