LFSR Based Stream Ciphers Are Vulnerable to Power Attacks

Sanjay Burman[1], Debdeep Mukhopadhyay[2], and Kamakoti Veezhinathan[3]

[1] PhD Student, Department of Computer Science and Engg., Indian Institute of Technology, Madras, India
sanjayburman@gmail.com
[2] Assistant Professor, Department of Computer Science and Engg., Indian Institute of Technology, Madras, India
debdeep@cse.iitm.ernet.in
[3] Associate Professor, Department of Computer Science and Engg., Indian Institute of Technology, Madras, India
kama@cs.iitm.ernet.in

Abstract. Linear Feedback Shift Registers (LFSRs) are used as building blocks for many stream ciphers, wherein, an n-degree primitive connection polynomial is used as a feedback function to realize an n-bit LFSR. This paper shows that such LFSRs are susceptible to power analysis based Side Channel Attacks (SCA). The major contribution of this paper is the observation that the state of an n-bit LFSR can be determined by making $O(n)$ power measurements. Interestingly, *neither the primitive polynomial nor the value of n be known to the adversary launching the proposed attack*. The paper also proposes a simple countermeasure for the SCA that uses n additional flipflops.

Keywords: Linear Feed Back Shift Registers, Side Channel Attacks, Power Analysis, Hamming Distance, Dynamic Power Dissipation.

1 Introduction

Encryption algorithms are used to protect information from unauthorized access or disclosure and are constructed using key controlled cryptographic primitives. The security robustness of cryptographic primitives have traditionally been measured under three mathematical models, namely, (1) when an adversary is assumed to have unlimited computational power (*unconditional security*); (2) when it can be proved that if an adversary is successful in breaking the cryptographic primitive under attack then, the adversary can also solve another mathematical problem that is believed to be hard to solve (*provable security*); and, (3) when the effort required to break a cryptographic primitive is so large that the cryptographic primitive can be considered to be unbreakable (*computational security*). However, it has been established in the recent past that even if a cryptographic primitive is robust against attacks under the three mathematical models mentioned above, there exist a class of attacks *against the real life implementations*

K. Srinathan, C. Pandu Rangan, M. Yung (Eds.): Indocrypt 2007, LNCS 4859, pp. 384–392, 2007.

that must be considered to ensure the security robustness of a system implementing the cryptographic primitives. These are referred to as *Side Channel Attacks* (SCA) [1]. This class of attacks against implementations are rather powerful and lead to system breaks with little effort. The adversary in this case exploits the information leaked unintentionally from the system executing the cryptographic primitive, into the environment, to attack the cryptographic system, often leading to catastrophic failure of security. This is possible even on a system whose *theoretical robustness has been established under the mathematical models mentioned above.*

Stream ciphers are an important class of symmetric ciphers used extensively for encryption by hardware-based cryptographic systems. They are popular because of their simplicity, efficiency and performance. The secure realization of stream ciphers is crucial to guard against the SCAs. Some guidelines in this direction are suggested in [2]. An overview on SCAs on stream ciphers and countermeasures is provided in [3]. LFSRs are used as building blocks for many stream ciphers because of their well defined structure and remarkable properties like long period, ideal autocorrelation and statistical properties. The leakage of information and vulnerability of stream ciphers based on Galois LFSRs is investigated in [4].

Though side channel attacks have reportedly been successfully mounted for many years [5], the publication of [6] by Kocher et.al. is a watershed in this area. This spurred a flurry of research and development in the exploitation of and safeguards against information leaked though side channels with an intention to attack the cryptographic mechanisms built into various security systems. There are several types of side channels through which information leaks inadvertently into the environment. The most prominent of them includes the measurement of the time taken or power consumed to perform a cryptographic function, the argument(s) to the function being the secret cryptographic key/data. A number of successful attacks using the above idea have been reported. These attacks can be mounted by using some very standard test and measuring equipment that are widely available. Typically power attacks can be mounted by measuring the electrical current that flows through a small resistor (10 Ω to 50 Ω) placed in series with the pin through which power is fed into a device performing a cryptographic computation. If the current being drawn is a function of the cryptographic key/data then the measurements of current during the cryptographic computation will be correlated with the cryptographic key/data. This correlation can then be analyzed to either directly mount the attack to reveal the key/data or be used in conjunction with a brute force attack to reduce the search space. Similar power attacks can also be mounted by measuring the electromagnetic radiations in the vicinity of the device performing the cryptographic computation.

This paper presents a power analysis based SCA technique to precisely determine the state of an n-bit LFSR by measuring the power consumed by the LFSR in each cycle over consecutive cycles linear in n.

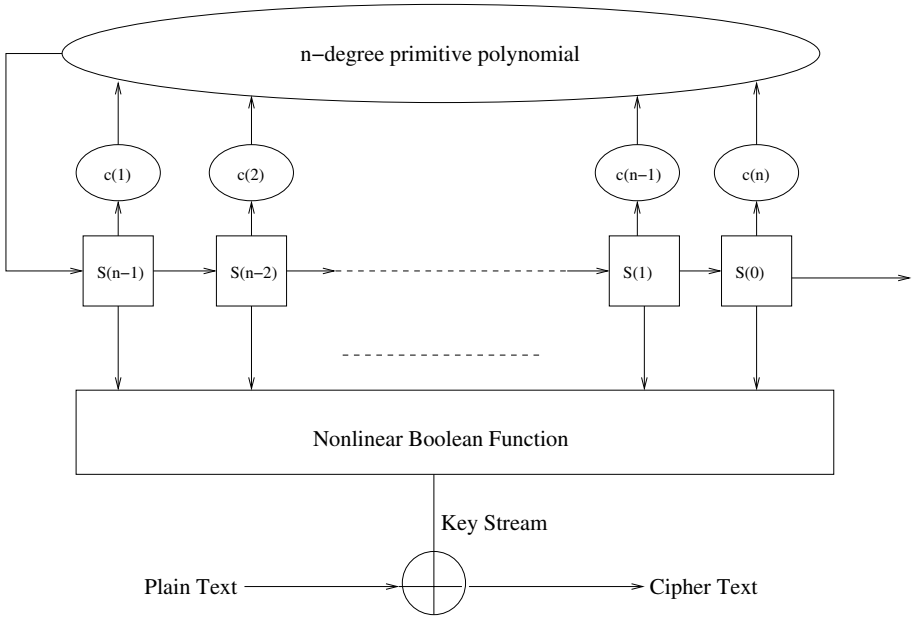

Fig. 1. An n-stage LFSR with a Non-linear filter

2 Preliminaries

2.1 LFSRs

LFSRs are used as primitives in building blocks in many stream ciphers because of their simple structure, guaranteed period and near ideal statistical properties. A general LFSR structure is shown in Figure 1.

The LFSR is a finite state machine that operates over some finite field F_q, where q is a prime or positive power of a prime. For the purposes of this paper we assume that $q = 2^r$, and $r = 1$, i.e. we consider only *binary LFSRs*. An n-stage binary LFSR consists of n consecutive storage elements, called stages. Each stage is a flipflop that stores $S(i)$, such that, $S(i) \in \{0, 1\}$, $\forall i$, $1 \leq i \leq n$. The content of the n-stages of the LFSR at time t is referred to as the *state of the LFSR* at time t and denoted by ST_t. The state at time $t + 1$ is computed by rightshifting the LFSR by one bit. The value shifted into the first (leftmost) stage, denoted by $S(n)$, is a linear combination of the contents of the n-stages as defined by the feedback polynomial used to realize the LFSR. Therefore, if $ST_t = (S(n-1), \cdots, S(0))$ then, $ST_{t+1} = (S(n), S(n-1), S(n-2), \cdots, S(1))$, where,

$$S(n) = c(1)S(n-1) \oplus c(2)S(n-2) \oplus \cdots \oplus c(n)S(0),\ c(i) \in \{0, 1\},\ \forall i,\ 1 \leq i \leq n.$$

For more information and background on the LFSRs, the reader is referred to [7]. We shall now present some new and interesting properties of LFSRs.

Theorem 1. *Let HD_t be the* Hamming Distance *between the n-bit vectors, ST_t and ST_{t+1}. Let $PD_t = (HD_t - HD_{t+1})$. Then, $PD_t \in \{-1, 0, 1\}$.*

Proof. Let $ST_t = (S(n-1), \cdots, S(1), S(0))$. Then, $ST_{t+1} = (S(n), S(n-1), \cdots, S(1))$ and $ST_{t+2} = (S(n+1), S(n), S(n-1), \cdots, S(2))$. Let $HW(V)$ denote the Hamming Weight (number of ones) of a bit-vector V. It is straightforward to see the following:

$$HD_t = HW((S(n) \oplus S(n-1)), (S(n-1) \oplus S(n-2)), \cdots, (S(1) \oplus S(0))) \quad (1)$$

$$HD_{t+1} = HW((S(n+1) \oplus S(n)), (S(n) \oplus S(n-1)), \cdots, (S(2) \oplus S(1))) \quad (2)$$

Equations 1 and 2 imply the following:

$$\begin{aligned} PD_t &= HD_t - HD_{t+1} && (3)\\ &= HW((S(0) \oplus S(1)) - HW((S(n+1) \oplus S(n))) && (4)\\ &= \{0, 1\} - \{0, 1\} && (5)\\ &= \{-1, 0, 1\} && (6) \end{aligned}$$

Hence, the Theorem. ◇

Corollary 1. *Let PD'_t be defined as follows: It is equal to* 0 *when, $HD_t = HD_{t+1}$, else it is* 1*. Given $S(n+1)$, $S(n)$, $S(1)$ and $S(0)$ as defined in Theorem 1,*

$$PD'_t = S(n+1) \oplus S(n) \oplus S(1) \oplus S(0).$$

Proof. The definition of PD'_t and equation 4 imply the corollary. ◇

2.2 Dynamic Power Consumption of an LFSR

The dynamic power consumed by a digital circuit is directly proportional to the switching activity (number of components in the circuit that has a state-transition from 0 to 1 or vice-versa) [9]. In the case of LFSRs the dynamic power consumed during the transition in cycle t, that is, from time period t to time period $t+1$, is proportional to HD_t (refer Theorem 1), as the computed Hamming Distance is a measure of the total number of toggles in the state of the LFSR during the time interval t to $t+1$. This implies that the *difference in power consumed by the LFSR* between cycle t and cycle $t+1$ is proportional to PD_t (as defined in Theorem 1). This paper assumes the following:

Assumption 1. *If the number of toggles in the state of an LFSR in cycle t is different than that in cycle $t+1$ (in other words $HD_t \neq HD_{t+1}$), then the power consumed by the LFSR in the two cycles are also different, else they are the same. Therefore, by measuring the power consumption at every cycle, the value of PD'_t as defined in corollary 1, can be computed.* ◇

3 The Proposed SCA Model

We explain our attack approach for the case where the stream cipher is built using an LFSR with a primitive feedback function and a nonlinear feed forward function as shown in Figure 1. These generators have been widely studied and often used as primitive building blocks in a number of stream ciphers [8]. The n-stage LFSR is initialized with a nonzero state which is the cryptographic key. Every time it is clocked a new key stream bit is generated by filtering the state using a nonlinear Boolean function. The key stream bit is added `mod 2` to the plain text to produce the cipher text. The *only* assumption of the proposed SCA model is that the adversary,

– can compute the values of PD'_t by measuring the power consumed by the LFSR, as stated in Assumption 1 above.

It is worthwhile to note that as stated in Assumption 1, the measurement of the power consumed is used *not to compute the number of toggles during any cycle* but *to just indicate whether the number of toggles between any two consecutive cycles is same or different*. Before proceeding further, the following properties of sequences generated by LFSR with primitive connection polynomials are presented. Such sequences are called M-sequences in the literature.

Theorem 2. *[10] The* linear complexity *of an infinite binary sequence s, denoted by $L(s)$, is defined as follows:*

1. *if s is the* zero sequence $s = 0, 0, 0, \ldots$, *then $L(s) = 0$;*
2. *if no LFSR generates s, then $L(s) = \infty$;*
3. *otherwise, $L(s)$ is the length of the shortest LFSR that generates s.*

Let t be a (finite) subsequence of s of length at least $2L(s)$. Then, the Berlekamp-Massey algorithm on input t determines an LFSR of length $L(s)$ which generates s.

Theorem 3. *[11] Given an n-bit LFSR F generating an M-sequence S, a linear combination of the stages of F yields a delayed version (phase) of S. For every delay d, $1 \leq d \leq 2^n - 1$, there exists a linear combination of the stages that yields a version of S that is delayed by d.* ◇

Let $(S(n-1), S(n-2), \cdots, S(0))$ be the initial unknown state of the given LFSR at time instant 0. Let $S(n+k)$ denote the bit shifted into the LFSR in the k^{th} cycle, $0 \leq k \leq n$. From corollary 1, if the adversary obtains the values of PD'_k, they can be related to the sequence generated by the LFSR as follows:

$$S(n+1) \oplus S(n) \oplus S(1) \oplus S(0) = PD'_0 \tag{7}$$

$$S(n+2) \oplus S(n+1) \oplus S(2) \oplus S(1) = PD'_1 \tag{8}$$

$$\cdots \quad \cdots \quad \cdots \tag{9}$$

$$S(n+k+1) \oplus S(n+k) \oplus S(k+1) \oplus S(k) = PD'_k \tag{10}$$

$$\cdots \quad \cdots \quad \cdots \tag{11}$$

The next theorem shows that the PD'_k values computed are a delayed M-sequence generated by the LFSR.

Theorem 4. *The sequence $PD'_0, PD'_1, \cdot$ is a delayed sequence of the M-sequence generated by the given LFSR with initial state $(S(n-1), S(n-2), \cdots, S(0))$.*

Proof. Note that by the definition of the LFSR, $S(n)$ is a linear combination of the bits currently stored in the LFSR. Let $S(n) = f_0(S(n-1), S(n-2), \cdots, S(0))$. Now, $S(n+1) = f_0(S(n), S(n-1), \cdots, S(1))$. Since $S(n)$ is a linear combination of $(S(n-1), S(n-2), \cdots, S(0))$, $S(n+1)$ can also be represented as a linear combination of $(S(n-1), S(n-2), \cdots, S(0))$ denoted by $f_1(S(n-1), S(n-2), \cdots, S(0))$.

From equation 7 we see that

$$PD_0 = f_1(S(n-1), \cdots, S(0)) \oplus f_0(S(n-1), \cdots, S(0)) \oplus S(1) \oplus S(0).$$

Hence, PD'_0 is a *linear combination LC* of the bits stored in the LFSR at time instant 0.

From equation 10 we see that

$$PD_k = f_1(S(n+k-1), \cdots, S(k)) \oplus f_0(S(n+k-1), \cdots, S(k)) \oplus S(k+1) \oplus S(k).$$

Note that PD'_k is the *same linear combination*, *LC*, (as in the case of PD'_0 mentioned above) of the bits stored in the LFSR at time instant k. This and theorem 3 proves this theorem. ◇

Theorem 5. *Given the length of the LFSR, the primitive connection polynomial and the delayed sequence $PD'_0, PD'_1, \cdots, PD'_{n-1}$, the initial state of the LFSR can be determined.*

Proof. As mentioned earlier, let $S(n+k)$ denote the bit shifted into the LFSR in the k^{th} cycle, $0 \leq k \leq n$. Note that by the definition of the LFSR, $S(n)$ is a linear combination of the bits currently stored in the LFSR. Let $S(n) = f_0(S(n-1), S(n-2), \cdots, S(0))$. As the primitive polynomial and the length of the LFSR, n, is known to the adversary imply that the function $f_0()$ is known to the adversary. As mentioned earlier, $S(n+1) = f_0(S(n), S(n-1), \cdots, S(1))$. Since $S(n)$ is a linear combination of $(S(n-1), S(n-2), \cdots, S(0))$, $S(n+1)$ can be represented as the function $f_1(S(n-1), S(n-2), \cdots, S(0))$. In a similar fashion, $S(n+k) = f_k(S(n-1), S(n-2), \cdots, S(0))$. As the primitive polynomial is known to the adversary, all the functions $f_k(S(n-1), S(n-2), \cdots, S(0))$, $0 \leq k \leq n$ are known to the adversary.

Substituting $S(n+k)$ by $f_k(S(n-1), \cdots, S(0))$, $0 \leq k \leq n$, in the equations 7 8 10, we get

$$\begin{gathered}
f_1(S(n-1), \cdots, S(0)) \oplus f_0(S(n-1), \cdots, S(0)) \oplus S(1) \oplus S(0) = PD'_0 \\
f_2(S(n-1), \cdots, S(0)) \oplus f_1(S(n-1), \cdots, S(0)) \oplus S(2) \oplus S(1) = PD'_1 \\
\cdots \qquad \cdots \qquad \cdots \\
f_n(S(n-1), \cdots, S(0)) \oplus f_{n-1}(S(n-1), \cdots, S(0)) \oplus f_0(S(n-1), \cdots, S(0)) \oplus \\
S(n-1) = PD'_{n-1}
\end{gathered}$$

Given that PD'_k, $0 \leq k < n$ is known, the above forms a set of n simultaneous equations with n unknowns, namely, $S(n-1), S(n-2), \cdots, S(0)$. Solving the above shall yield the values of $S(n-1), S(n-2), \cdots, S(0)$. Substituting these values in $f_k(S(n-1), S(n-2), \cdots, S(0))$, $0 \leq k \leq n$, gives the values of $S(2n), S(2n-1), \cdots, S(n+1)$.

The fact that the sequence generated by the LFSR is an M-sequence and Theorem 4 imply that the above set of simultaneous equations does have *an unique solution*. This is true from the observation that there should exist states $(S(n-1), S(n-2), \cdots, S(0))$ which is at an unique *delay distance* from the sequence $(PD'_0, PD'_1, \cdots)$; and, there can be only one (state of the LFSR) solution to $(S(n-1), S(n-2), \cdots, S(0))$. If there are more than one solution, it essentially implies that the delayed sequence $(PD'_0, PD'_1, \cdots)$ can be arrived at from two different initial states of the LFSR, with the same amount of delay, which contradicts the fact that the LFSR generates an M-sequence. ◇

3.1 The Proposed Attack

Let $POW(k)$ denote the dynamic power consumed by the nonlinear filter generator at time instant k.

1. Measure $POW(0)$, for time instant 0;
2. **for** each time instant k, $k \geq 1$ **do**
   (a) Measure the dynamic power, $POW(k)$.
   (b) $PD'_{k-1} = 1$ **if** $POW(k-1) \neq POW(k)$, **else** it is 0.
   (c) Input PD'_{k-1} into the Berlekamp-Massey (BM) Algorithm. **If** BM terminates then **exit this for loop**; **else** repeat Step 2;
3. **Result**
   (a) Berlekamp-Massey algorithm outputs the *length* n of the LFSR F and the connection polynomial realized by F; (as inferred from theorems 2 and 4).
   (b) Now that the length of the LFSR and the connection polynomial realized by the LFSR are known, compute the initial state of the LFSR at the time of launch of the attack using Theorem 5.

4 Countermeasure to the SCA

Figure 2 shows the countermeasure for the SCA. In the circuit, for each flipflop F in the LFSR, there is a corresponding toggle flipflop F' that toggles, if F does not toggle; and, does not toggle, if F toggles. Note that the clock input to F' is the $XNOR$ of the input and output of F AND-ed with the system clock. If the input and output of F is same, that is F does not toggle in the next cycle, the clock is fed into F' essentially toggling it. On the other hand, if the input and output of F are different, that is F toggles in the next cycle, the clock is not fed into F' preventing it from toggling. In this circuit, at each stage there shall be uniformly n toggles, thereby countering the power attack. To avoid clock skews between the LFSR flipflops and their toggle counterparts, the clock path

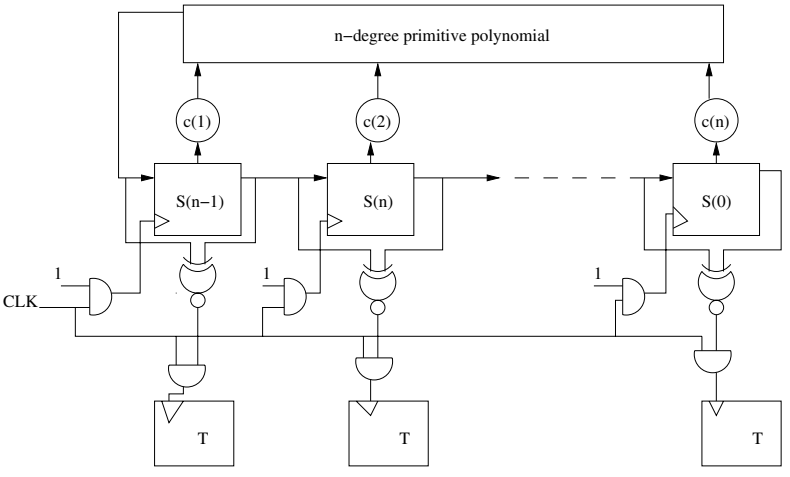

Fig. 2. The Countermeasure to the SCA

to both are balanced by introducing a dummy gate in the clock path driving the flipflops of the LFSR. The drawbacks of this approach are that it needs double the number of flipflops and consumes more dynamic power.

5 Conclusions

We have shown an interesting property of LFSRs with respect to the hamming distance between the state transitions of an LFSR with primitive feedback polynomial. We exploit this property to determine the state of the LFSR by making $O(n)$ power measurements. In this paper, we have made an ideal assumption that the power consumed by the LFSR in each of any two consecutive cycles shall remain the same if the number of toggles in the state of the LFSR are also equal in the two cycles under consideration. A more practical assumption would be that if the *difference in power consumed across two cycles is less than a threshold* then the toggles are equal across the cycles, else they are different. Such type of *thresholds* can be determined by simulating the model of the LFSR, using circuit simulators like SPICE. The paper also presents a simple countermeasure for the attack.

References

1. Kocher, P., Lee, R., McGraw, G., Raghunathan, A., Ravi, S.: Security as a New Dimension in Embedded System Design. In: Proc. of IEEE Design Automation Conference - DAC 2004, pp. 753–761. IEEE Computer Society Press, Los Alamitos (2004)
2. Kumar, S., Lemke, K., Paar, C.: Some Thoughts about Implementation Properties of Stream Ciphers. In: Proc. of State of the Art of Stream Ciphers Workshop - SASC 2004, Brugge, Belgium (2004)

3. Rechberger, C., Oswald, E.: Stream Ciphers and Side-Channel Analysis. In: Proc. of State of the Art of Stream Ciphers Workshop - SASC 2004, Brugge, Belgium (2004)
4. Delaunay, P., Joux, A.: Galois LFSR, Embedded Devices and Side Channel Weaknesses. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 436–451. Springer, Heidelberg (2006)
5. Shamir, A.: A Top View of Side Channel Attacks. In: Proc. of L-SEC/CALIT IT Security Congress (October 19-20, 2006)
6. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
7. Golomb, S.: Shift Register Sequences. Aegean Park Press, Laguna Hills, CA (1981)
8. Bedi, S.S., Pillai, N.R.: Cryptanalysis Of The Nonlinear Feedforward Generator. In: Roy, B., Okamoto, E. (eds.) INDOCRYPT 2000. LNCS, vol. 1977, pp. 188–194. Springer, Heidelberg (2000)
9. Hsiao, M.S.: Peak Power Estimation using Genetic Spot Optimization for large VLSI circuits. In: DATE 1999. Proc. of Intl. Conf. on Design Automation and Test in Europe, pp. 175–179 (1999)
10. Menezes, A., van Oorschot, P., Van stone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton, USA (1996)
11. Davies, A.C.: Delayed versions of maximal-length linear binary sequences. Electronic Letters 1, 61 (1965)