THEORETICAL SIMPLE POWER ANALYSIS OF THE GRAIN STREAM CIPHER

A. A. Zadeh and Howard M. Heys

Electrical and Computer Engineering
Faculty of Engineering and Applied Science
Memorial University of Newfoundland

ABSTRACT

Power analysis has come to be an important category of cryptanalytic attacks. Although such attacks have been extensively applied to block ciphers, only limited research has been done to analyze their effectiveness on stream cipher hardware implementations. In this paper, we consider the application of simple power analysis (SPA) to the Grain stream cipher. The applicability of SPA is considered under idealized assumptions of the Hamming distance power model and the complexity of the attack is analyzed. The resulting analysis implies that the Grain cipher is susceptible to power analysis attacks where there is strong correlation between the power measurements and changes in the cipher's state registers.

Index Terms— stream ciphers, cryptanalysis, simple power analysis, Grain stream cipher

1. INTRODUCTION

Power analysis attacks belong to the general category of cryptographic side channel attacks. Such attacks make use of measurements of implementation characteristics of ciphers that can be related to cipher data and thereby used to derive the cryptographic key for the system. Power attacks, based on analyzing power trace measurements made on an operating cryptographic device, were first proposed by Kocher, et al., [1] in 1999 and have since become an important and effective category of attacks on cryptographic systems. Most notably such attacks have been applied to symmetric key cryptographic systems based on block ciphers such as the Advanced Encryption Standard (AES). (See, for example, [2].) However, little research has been undertaken applying these attacks to stream ciphers.

Stream ciphers typically operate on one bit of data at a time. For example, to encrypt, an unpredictable, pseudorandom sequence of data, referred to as the keystream, is generated using a keystream generator and XORed bit-by-bit with the sequence of plaintext bits to produce the ciphertext bit sequence. To decrypt, the identical keystream is generated and XORed with the ciphertext to reproduce the plaintext bit stream. In this paper we consider the stream cipher Grain [3], which was selected for the ECRYPT eSTREAM portfolio for a hardware-oriented stream cipher [4]. Grain is a keystream generator designed for efficient hardware implementations, based on the nonlinear mixing of data from an 80-bit linear feedback shift register (LFSR) and an 80-bit nonlinear feedback shift register (NLFSR).

The general principle behind power analysis attacks is the following. Since the dynamic power dissipation is the major consumed power in CMOS circuits, sampling the consumed power gives an idea of the number of switching transistors in a circuit. This information then can be used to identify characteristics of the data within the device and in the appropriate circumstances reveal bit values of the registers of a cipher implemented within the device. In a power analysis attack, it is assumed the attacker has the ability to measure the power consumed by the cipher. 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.

In this paper, we apply the concept of power analysis, in particular, simple power analysis (SPA), to the Grain stream cipher. In doing so, we assume an ideal model which can accurately map power trace measurements to the number of changes in bits stored in the cipher's LFSR and NLFSR. This analysis builds on the concepts first presented in [5], applied to nonlinear filter generator type stream ciphers (based on one LSFSR), and then extended in [6] to apply to nonlinear combination generator type stream ciphers comprised of multiple LFSRs.

2. BACKGROUND

In order to present the outcomes of our work, we must first review the Grain stream cipher and the concepts associated with simple power analysis.

This work is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

2.1. Grain Stream Cipher

The original version of Grain (now referred to as Grain version 0 or Grain V0) was submitted to the ECRYPT stream cipher project (eSTREAM) [4] in 2005 and designed primarily for hardware implementation with an 80-bit key. In order to address some security concerns, a slightly modified version (with small changes to the output function and the nonlinear feedback function), referred to as Grain version 1 or Grain V1 [3], has been selected for the hardware portfolio by the eSTREAM project. (In addition, a version with a 128-bit key, called Grain-128, has also been defined [3].) The Grain V1 architecture consists of one 80-bit LFSR and one 80-bit NLFSR. The output is a nonlinear combination of LFSR and NLFSR bits. Let S_t and B_t denote the 80-bit LFSR and NLFSR states, respectively, and $s_t(i)$ and $b_t(i)$ ($0 \leq i < 80$), represent the values of bit i in the states at time t. In this paper, we consider the 80-bit version of Grain V1 and Fig. 1 shows the overall architecture. The output (that is, the keystream) at time t, z_t, is determined using a nonlinear combination of state bits and the LFSR state S_t and the NLFSR state B_t are determined using linear and nonlinear feedback relations, respectively. The details of these operations are described in [3].

In addition to the 80-bit key, Grain V1 has a 64-bit initialization vector (IV). For details on how to setup the key and resynchronize Grain with a new IV, refer to [3]. An exhaustive key search on Grain V1 would take on the order of 2^{80} and this gives an idea of the relative benchmark to consider when analyzing the security of other attacks on Grain V1. Alternatively, since determining the 80-bit states of the LFSR and the NLFSR would allow the determination of all subsequent keystream bits, a successful attack of Grain should reveal all 160 bits of the FSRs of Grain. Although some analyses of Grain have been published, with attacks in particular targeted to the 128-bit version Grain-128 [7], the 80-bit version Grain V1 is still considered secure and would be a good selection for implementation in a CMOS-based ASIC for a stream cipher application.

2.2. Power Analysis Attacks

In the approach taken in former research considering power analysis (such as [5, 6] for example, in addition to many others), the measured power consumption at the rising edge of the clock is taken as proportional to the number of register bits changed in the system at that point in time. This is referred to as the *Hamming distance power model.* By taking samples of power data at the triggering clock edges of synchronous digital hardware, this can reveal information about data stored in the registers during particular operations of the cipher.

As summarized in [8], the two basic methods that exist to exploit power measurement are differential power analysis and simple power analysis. DPA makes use of a number of power traces to which statistical methods are applied to determine data-dependent correlations. SPA examines the information from a power trace and directly attempts to determine information about the cipher data and key. In [9], a differential power analysis (DPA) attack has been applied to Grain. The attack is able to recover the key with a small number of power samples. However, the attack makes use of resynchronizations where the initialization vectors are chosen to be specific values. These conditions constrain the application of the attack to very specific circumstances.

3. THEORETICAL APPLICATION OF SPA TO STREAM CIPHERS

In [5] and [6], theoretical simple power analysis methods are offered to analyze LFSR cryptographic cores under the assumption of the ideal application of the Hamming distance power model. That is, it is assumed that power measurements can be exactly related to the Hamming distance of data in the registers before and after the triggering edge of the clock with no noise or inaccuracies in the mapping between power information and cipher data. The objective of the attacks is to directly determine the cipher state (that is, the bits of the registers) of the cipher. Knowing the cipher state, it is possible to determine the subsequent keystream bits. We summarize the results for application of SPA to LFSR-based stream ciphers in this section.

3.1. General Concepts

In our discussion, we refer to L bit values of the LFSR as the state. At clock cycle t, the current state is represented as S_t. The Hamming distance between S_t and S_{t-1} is given as HD_t and is calculated from

$$HD_t = \sum_{i=0}^{L-1} \left(s_t(i) \oplus s_{t-1}(i) \right), \tag{1}$$

where $s_t(i)$ represents the value of bit i of S_t with $s_t(0)$ being the rightmost bit of the LFSR and $\oplus$ representing XOR. It is assumed that the shift register shifts right with the leftmost bit, $s_t(L-1)$ updated by a linear combination of state bits S_{t-1}.

Between two successive clock cycles it can be shown that the difference between the Hamming distances must be one of the three values: $HD_{t+1} - HD_t \in \{-1, 0, +1\}$. Based on the Hamming distance power model, defining the theoretical power difference to be PD_t given by

$$PD_t = HD_{t+1} - HD_t, \tag{2}$$

it can be seen that PD_t is proportional to the difference of the measured dynamic power consumption at two consecutive clock cycles at times t and $t+1$, which is an analog variable in watts denoted as MPD_t. Simply, $PD_t \propto MPD_t$.

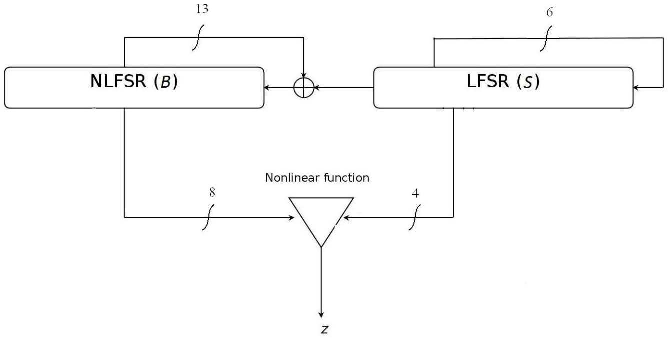

Fig. 1. Architecture of Grain Stream Cipher

Substituting (2) into (1) results in

$$PD_t = [s_{t+1}(L-1) \oplus s_t(L-1)] - [s_t(0) \oplus s_{t-1}(0)], \quad (3)$$

where the new bit value for state $t+1$, $s_{t+1}(L-1)$, will be the new value of bit $L-1$ based on the values of S_t.

3.2. Attacking an LFSR-based Stream Cipher

As described in [5] to attack a stream cipher based on one LFSR and a nonlinear filtering function, considering operations over $GF(2)$, we can write

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

where we now denote $s_{t+1}(L-1)$ as $s_t(L)$ and $s_t(L-1)$ as $s_{t-1}(L)$. (In general, we can write $s_{t+j}(i) = s_t(i+j)$ with $s_t(i+j)$ representing the $(i+j)$-th bit following bit $s_t(0)$ in the FSR sequence.)

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, $MPD_t \approx 0$), then we can conclude $PD_t = 0$ and write $s_t(L) \oplus s_{t-1}(L) \oplus s_t(0) \oplus s_{t-1}(0) = 0$ and, if the measured dynamic power consumption at time t and $t+1$ are not equal (that is $MPD_t \neq 0$), we can conclude $PD_t \neq 0$ and write $s_t(L) \oplus s_{t-1}(L) \oplus s_t(0) \oplus s_{t-1}(0) = 1$. For an LFSR, collecting enough MPD_t values and using the linear feedback relation, we can set up a linear system of equations of the S_t bits, $\{s_t(i)\}$, where $0 \leq i < L$, and determine the keystream sequence.

3.3. Attacking Stream Ciphers Based on Multiple LFSRs

In [6], the proposed method in [5] is extended to be applicable to stream ciphers with multiple LFSRs by assuming the measured power difference of the circuit is the summation of individual LFSRs. For example, if the stream cipher has two LFSRs, the total measured MPD of the circuit is $MPD^{total} = MPD^1 + MPD^2$ where MPD^i is proportional to the theoretical power difference of the i-th LFSR, PD^i, where $i \in \{1,2\}$ and $PD^{total} = PD^1 + PD^2$. Then, when MPD^{total} is a large positive level, indicating that $PD^{total} = +2$, we know that PD values for both LFSRs are equal to +1. After collecting enough power samples, we can set up a system of equations for each LFSR independently and obtain the bit values. This can be extended to be applied to any number of LFSRs that are combined to form a stream cipher.

4. APPLYING SPA TO NLFSRS

An NLFSR has a similar structure to an LFSR, except the feedback function is nonlinear. In order to make stream ciphers more secure, particularly against algebraic attack, NLFSRs are widely used in stream ciphers with Grain being an example. Since in an NLFSR, the feedback is nonlinear, using the abovementioned method results a system of nonlinear equations which are difficult to solve.

We now review a simple power analysis method, outlined in [10], that can be used to determine the bits of an NLFSR given appropriate power measurements. As with the previously described attacks, the objective of the approach is to directly determine the register bit values, thereby determining precisely the cipher state. Again, we assume that the measured power consumption resulting in the measured power difference at time t, MPD_t, can be perfectly converted to the theoretical power difference, PD_t.

Consider a consecutive values of PD_t for an NLFSR with the length of L bits and denote the i-th bit of the NLFSR at time t as $b_t(i)$. In order to calculate NLFSR bit values, we should modify the former equations proposed to analyze an LFSR. Similar to equation (3), we can write:

$$PD_t = [b_t(L) \oplus b_{t-1}(L)] - [b_t(0) \oplus b_{t-1}(0)]. \qquad (5)$$

Then, when $PD_t = +1$, we conclude

$$\begin{array}{c} b_t(L) \oplus b_{t-1}(L) = 1 \\ b_t(0) \oplus b_{t-1}(0) = 0 \end{array} \qquad (6)$$

and, when $PD_t = -1$, we can write

$$\begin{array}{l} b_t(L) \oplus b_{t-1}(L) = 0 \\ b_t(0) \oplus b_{t-1}(0) = 1. \end{array} \tag{7}$$

When $PD_t = 0$, the two bracketed XOR results of equation (5) are both equal to either 0 or 1 and we can write

$$b_t(L) \oplus b_{t-1}(L) = b_t(0) \oplus b_{t-1}(0). \tag{8}$$

As long as $PD_t \neq 0$, we can find a relation between two consecutive values of the NLFSR bits, using equation (6) or (7).

To analyze the NLFSR, we must obtain L consecutive bits of the NLFSR. Equations (6) and (7) could determine the relation between two bits of the NLFSR when $PD_t = +1$ or $PD_t = -1$. However, when $PD_t = 0$, we cannot use equation (6) and (7) directly. Instead, we make use of an equation similar to (4) for PD_t and PD_{t+L} to obtain

$$\begin{array}{rcl} |PD_t| \oplus |PD_{t+L}| & = & b_t(L) \oplus b_{t-1}(L) \oplus b_t(0) \\ & & \oplus b_{t-1}(0) \oplus b_{t+L}(L) \\ & & \oplus b_{t+L-1}(L) \oplus b_{t+L}(0) \\ & & \oplus b_{t+L-1}(0) \end{array} \tag{9}$$

resulting in

$$\begin{array}{rcl} |PD_t| \oplus |PD_{t+L}| & = & b_t(0) \oplus b_{t-1}(0) \oplus b_t(2L) \\ & & \oplus b_{t-1}(2L) \end{array} \tag{10}$$

where we have made use of the fact that $b_{t+j}(i) = b_t(i+j)$. As well, it can be shown that

$$PD_t + PD_{t+L} = [b_t(2L) \oplus b_{t-1}(2L)] - [b_t(0) \oplus b_{t-1}(0)]. \tag{11}$$

The value of PD_{t+i} must be +1, 0 or -1 implying that $|PD_{t+i}|$ is 0 or 1. Since $|PD_t| \oplus |PD_{t+L}|$ will be either 1 or 0, if $PD_t = 0$, then we can write equation (6) or (7) for PD_{t+L} if $|PD_{t+L}|$ is 1 and using equation (10) find the relation between $b_t(0)$ and $b_{t-1}(0)$. For example, let us assume $PD_t = 0$. If $PD_{t+L} = +1$ or -1, then $b_t(2L) \oplus b_{t-1}(2L)$ and $b_t(L) \oplus b_{t-1}(L)$ are known from either equation (6) or (7) (with t replaced with $t + L$) and since the left side of equation (10) is known from power measurements then $b_t(0) \oplus b_{t-1}(0)$ can be inferred. If $PD_{t+L} = 0$, then power differences from cycle $t + 2L$ must be considered.

Now using equations (6) or (7) and (10), if necessary, the relationships between L pairs of consecutive bits are known. Although the relations between consecutive pairs of bits are known, the actual values are not. However, there are only two possibilities and both can be tested to determine which results in the correct state of the NLFSR. Since for this method, the feedback relation is not used, we can use the approach for both an NLFSR and LFSR, with no need to solve a system of equations.

From equation (5), it is easy to see that the probability of PD_t equal to zero is $\frac{1}{2}$. Hence, we need to obtain PD_{t+L} for, on average, $\frac{1}{2}$ of L consecutive PD_t values. On average, $\frac{1}{2}$ of the values of PD_{t+L} are equal to the zero and we need to collect PD_{t+2L} values. In other words, on average for $\frac{1}{2}$ of L consecutive bits we are targeting, we need to collect PD_{t+L} values; for $\frac{1}{4}$ of the L consecutive bits, we need to collect PD_{t+2L} values, etc.

In practical applications to analyze the sequence of an NLFSR, it is sufficient to find any consecutive L bits of the NLFSR. Hence, the analysis initially collects a number of consecutive power samples and then analyzes the values. In order to estimate the probability of a successful analysis, we assume $n \times L$ consecutive power difference values have been collected. The probability of all PD_{t+iL} values being zero for $0 \leq i < n$ and a fixed value of t (and therefore not being usable to determine bits in the register) is 2^{-n}. If we assume the occurrence of $PD_t = 0$ for different values of t are independent, then, given $n \times L$ power difference values, the probability that this is enough samples to analyze the NLFSR is $[1 - 2^{-n}]^L$. For $L \ll 2^n$, this probability is approximately $1 - 2^{-n}L$.

5. A NEW THEORETICAL SPA ATTACK OF GRAIN

Since Grain uses two feedback shift registers (one LFSR and one NLFSR), we need to consider the methods presented in [6] and summarized in Section 3.3 which describe a theoretical attack on stream ciphers with multiple LFSRs, where it is assumed that the attack takes place in circumstances where measured power traces perfectly map to the correct PD_t values. However, the proposed attack can not be applied directly on NLFSR based ciphers, such as Grain, since it relies on constructing and solving a system of linear equations.

To extend the attack to Grain, we can use the proposed method discussed in [10] and summarized in Section 4 which is applied to an NLFSR assuming perfect mapping from power measurements to the correct PD_t values. Since for the Hamming distance power model, we know that the overall power consumption of Grain is approximated by the summation of power consumption of the LFSR and the NLFSR (and it is assumed power consumed in other parts of the circuit is negligible), measuring the power at the triggering edge of the clock, embodies the power consumption of the D flip-flops of both the LFSR and NLFSR. If we assume the power consumption of the circuit at time t (at the triggering edge) is the summation of the power consumption of LFSR and NLFSR (which is also proportional to the Hamming distance of their consecutive states), then we can conclude the overall dynamic power dissipation of the circuit at the triggering edge of the clock is proportional to $HD_t^{LFSR} + HD_t^{NLFSR}$. Hence, we can define the power difference of the circuit as

$$\begin{array}{rcl} PD_t^{Grain} & = & [HD_{t+1}^{LFSR} + HD_{t+1}^{NLFSR}] \\ & & -[HD_t^{LFSR} + HD_t^{NLFSR}] \\ & = & PD_t^{LFSR} + PD_t^{NLFSR}. \end{array} \tag{12}$$

As shown in Section 3, PD_t^{LFSR} and PD_t^{NLFSR} values can be -1, 0 or $+1$, and, hence, $-2 \leq PD_t^{Grain} \leq +2$. As described in [6], if $PD_t^{Grain} = +2$ or -2, then we can conclude $(PD_t^{LFSR}, PD_t^{NLFSR}) = (+1, +1)$ or $(-1, -1)$, respectively. Hence, we can use the proposed method in [5] and set up a system of linear equations to get the bit values of the LFSR. To complete the attack and get the bit values of the NLFSR, we use the proposed method described in Section 4.

To calculate the bit values of the NLFSR, we should have 80 consecutive PD_t^{NLFSR} values. To obtain 80 consecutive PD_t^{NLFSR} values we should at first collect enough power samples so that we have several hundred values of $PD_t^{Grain} = +2$ or -2 and we can find 80 power differences that lead to independent linear equations [6]. Using these, we can calculate LFSR bit values. After calculating LFSR bit values, we should calculate PD_t^{LFSR} values for a few hundred consecutive clocks. Finally, deducting calculated PD_t^{LFSR} from the measured PD_t^{Grain}, we have a few hundred of PD_t^{NLFSR} values. Using the proposed method in Section 4, we can calculate the bit values of the NLFSR.

The probability of $PD_t^{Grain} = +2$ or -2 is 1/8. As discussed in [6], when considering the 80-bit LFSR of Grain, to solve the system of 80 linear equations, somewhat more than 80 power difference values are required to ensure that we can obtain 80 linearly independent equations. Based on the analysis in the appendix of [6], from 120 random linear equations, the probability that at least 80 equations will be linearly independent is greater than 99.99%. To obtain 120 equations, on average, 960 power samples should be collected. Using 1200 power difference values, as calculated in [6], the probability of 120 usable power difference values is greater than 98.99%. Making use of the analysis method in Section 4, the probability of a successful attack on an 80-bit NLFSR when 1200 power samples have been collected is $(1 - 2^{-15})^{80} \approx 99.8\%$. Hence, we can conclude that with 1200 power samples, Grain is theoretically susceptible to an SPA attack with very high probability. This represents an attack on Grain that is substantially less complex than exhaustive key search, which requires as much as the analysis of 2^{80} values for the 80-bit key of Grain.

6. CONCLUSION

In this paper, we have discussed the application of a simple power analysis attack applied to Grain in an ideal environment where the Hamming distance model can be applied perfectly to relate power measurements directly to changes in the cipher's state registers. Under these conditions, Grain would be susceptible to power analysis with only a few hundred power samples. However, this is an idealized result and difficulties would exist in mounting a practical attack which can not assume that measured power differences can be perfectly related to register data. Nevertheless, the results presented here do illustrate the potential vulnerability of stream ciphers based on LFSRs and NLFSRs to power analysis attacks and suggest that care must be taken to design implementations which do not leak power consumption information.

7. REFERENCES

[1] P.C. Kocher, J. Jaffe, and B. Jun, ‘Differential Power Analysis’, Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO ’99), Lecture Notes in Computer Science, vol. 1666, Springer, pp. 388–397, 1999.

[2] S.B. Ors, F. Gurkaynak E. Oswald, and B. Preneel, ‘Power Analysis attacks on an ASIC AES Implementation’, Proceedings of Information Technology: Coding and Computing (ITCC 2004), Las Vegas, Nevada, vol. 2, IEEE, pp. 546–552, 2004.

[3] M. Hell, T. Johansson, A. Maximov, and W. Meier, ‘The Grain Family of Stream Ciphers’, New Stream Cipher Designs, Lecture Notes in Computer Science, vol. 4986, Springer, pp. 179–190, 2008.

[4] Homepage for ‘eSTREAM: the ECRYPT Stream Cipher Project’, www.ecrypt.eu.org/stream.

[5] S. Burman, D. Mukhopadhyay, and K. Veezhinathan, ‘LFSR Based Stream Ciphers are Vulnerable to Power Attacks’, INDOCRYPT 2007, Lecture Notes in Computer Science, vol. 4859, Springer, pp. 384–392, 2007.

[6] A.A. Zadeh and H.M. Heys, ‘Applicability of Simple Power Analysis to Stream Ciphers Using Multiple LFSRs’, Proceedings of Canadian Conference on Electrical and Computer Engineering (CCECE 2012), Montreal, May 2012.

[7] C. Berbain, H. Gilbert, and A. Maximov, ‘Cryptanalysis of Grain’, Proceedings of Fast Software Encryption (FSE2006), Lecture Notes in Computer Science, vol. 4047, Springer, pp. 15–29, 2006.

[8] P.C. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, ‘Introduction to Differential Power Analysis’, Journal of Cryptographic Engineering, vol. 1, no. 1, Springer, pp. 5–27, 2011.

[9] W. Fischer, B.M. Gammel, O. Kniffler, and J. Velten, ‘Differential Power Analysis of Stream Ciphers’, Proceedings of the 7th Cryptographers’ track at the RSA Conference (CT-RSA 2007), Lecture Notes in Computer Science, vol. 4377, Springer, pp. 257–270, 2007.

[10] A.A. Zadeh and H.M. Heys, ‘Simple Power Analysis Applied to Nonlinear Feedback Shift Registers’, submitted for review.