Design of Feedback Shift Register of Against Power Analysis Attack

Yongbin Zhao¹,* , XuYang¹ and RanranLi¹

Abstract: Stream ciphers based on linear feedback shift register (LFSR) are suitable for constrained environments, such as satellite communications, radio frequency identification devices tag, sensor networks and Internet of Things, due to its simple hardware structures, high speed encryption and lower power consumption. LFSR, as a cryptographic primitive, has been used to generate a maximum period sequence. Because the switching of the status bits is regular, the power consumption of the LFSR is correlated in a linear way. As a result, the power consumption characteristics of stream cipher based on LFSR are vulnerable to leaking initialization vectors under the power attacks. In this paper, a new design of LFSR against power attacks is proposed. The power consumption characteristics of LFSR can be masked by using an additional LFSR and confused by adding a new filter Boolean function and a flip-flop. The design method has been implemented easily by circuits in this new design in comparison with the others.

Keywords: Stream cipher, feedback shift register, power analysis, Boolean function.

1 Introduction

On account of its simple hardware structures, high speed encryption and lower power consumption, stream ciphers based on LFSR are well suitable for constrained environments, such as satellite communications, radio frequency identification devices tag, sensor networks and Internet of Things. For example, ZUC [ETSI/SAGE Specification (2010)] formed the core of the 3GPP mobile standards 128-EEA3 and 128-EIA3. However, the security of stream ciphers is serious threaten by correlation attacks [Meier (2011)], algebraic attacks [Courtois (2002); Rønjom (2017)], differential cryptanalysis [Siegenthaler (1984); Banik (2016)], cube attack [Aumasson, Dinur and Meier (2009), Rahimi, Barmsbory and Mansouri (2016)] and side channel attack etc. Side channel attacks, which include power attacks [Kocher, Jaffe and Jun (1999)], timing attacks [Kocher (1996)], electromagnetic attacks [Quisquater and Samyde (2001)] and differential fault analysis [Shamir and Biham (1998)], are effective methods to gain information from the physical implementation of a cryptosystem. Power attack has been considered as the most dangerous attack to the security of cryptographic embedded systems.

CMOS logic and application specific details cause the power characteristics of logic

¹ School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, China.
* Corresponding Author: Yongbin Zhao. Email: zhaoyungbin@163.com.
operations dependency on the input data. Power attack tries to find the relationship between initialization vectors (IV) and power consumption by using the measurement of the power consumption variation in every cycle. Differential power analysis was proposed by Kocher, Jaffe and Jun in 1999. Lano et al. [Lano, Mentens and Preneel (2004)] adapted differential power analysis methods to theoretically attack stream cipher algorithms A5/1 and E0. After Fischer et al. [Fischer, Gammel and Kniffel (2006)] have mounted a successful differential power attack against Trivium and Grain ciphers, which are candidate stream ciphers in ECRYPT (European Network of Excellence in Cryptology). The power analysis method has been widely applied in stream cryptanalysis [Tena-Sánchez and Acosta (2015); Gupta, Mishra and Suri (2016)]. A few designs [Kocher, Jaffe and Jun (1999), Burman, Mukhopadhyay and Veezhinathan (2007), Sharif Mansouri (2014)], which protect stream ciphers from leaking information, have been proposed. In this paper, a new design of LFSR against power attacks for stream cipher based on LFSR is proposed. The implementation is simpler and easier by using this design in comparison to the others. In addition, the better synchronization performance is achieved.

2 Preliminaries
2.1 Boolean function

Let be the finite field with two elements, \( F_2^n = \{(x_1, ..., x_n) : x_i \in F_2, i = 1, ..., n\} \) denote the \( n \)-dimensional vector space. A Boolean function \( f \) in \( n \) variables is a mapping from \( F_2^n \) into \( F_2 \), and the set of all Boolean functions in \( n \) variables is denoted by \( B_n \). Alternatively, the Boolean function \( f(x) \in B_n \) can also be represented as the Algebraic Normal Form (ANF), i.e.,

\[
f(x_1, ..., x_n) = \bigoplus_{u \in F_2^n} a_u \left( \prod_{i=1}^{n} x_i^{u_i} \right)
\]

for \( a_u \in F_2 \), \( u = (u_1, ..., u_n) \), where \( \oplus \) denotes the sum over \( F_2 \). The Walsh transform \( S_f(\omega) \) of \( f \in B_n \) is a real-valued function and is defined as \( S_f(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) + x \cdot \omega} \),

where \( \omega \in F_2^n \), and \( x \cdot \omega = x_1 \omega_1 \oplus x_2 \omega_2 \oplus \cdots \oplus x_n \omega_n \).

Many properties of Boolean functions can be described by the Walsh spectrum, such as nonlinearity, denoted by \( N_f = 2^{n-1} - \frac{1}{2} \max_{\omega} |S_f(\omega)| \), balancedness, denoted by \( S_f(0) = 0 \), mth order correlation immunity(\( m \)-CI), denoted by \( S_f(\omega) = 0 \), where \( 0 < \text{wt}(\omega) \leq m \). The balanced \( m \)-CI function is said to be \( m \)-resilient.

In stream cipher, Boolean functions are provided high nonlinearity and satisfy certain criteria. Cryptographic properties of Boolean function, such as balancedness, nonlinearity and correlation immunity, etc. are also important indicator for the security of steam ciphers. Boolean functions with good cryptographic properties must be balanced, high level nonlinearity, CI is no less than 1 for filter functions and less than the number of LFSRs for combination functions.
2.2 LFSR

As a cryptographic primitive, LFSR composed of XOR gates and flip-flops has been used to generate a maximal period sequence. It has two implementation, Galois implementation and Fibonacci implementation. The Fibonacci implementation (see Fig. 1) is simply copy each bit to its neighbor on the right. In this paper, the Fibonacci representation LFSRs was adapted (see more details in [Goresky M and Klapper A M (2002)]). The initial state of the LFSR is called the IV. For example, IV = LS(0) = (s(0), s(1), ..., s(n−1)) , s(i) ∈ {0,1} in Fig. 1. After i clock cycle, the state of LFSR is LS(i) = (s(i), s(i+1), ..., s(i+n−1)) , and the leftmost bit is

\[ s(i+n) = \sum_{j=0}^{n-1} c_j s(i+n-j) \]

at the next clock cycle.

![Figure 1: Fibonacci representation of LFSR with length n](image)

The combination of taps and their location is often referred to as a connection polynomial, and expressed \( f(x) = 1 + c_1 x + c_2 x^2 + ... + c_n x^n \). When \( f(x) \) is a primitive polynomial, the output sequence of LFSR is a periodic sequence of span \( 2^n - 1 \) (called maximum length sequence or m-sequence).

3 Design of LFSR

Based on the power model of LFSR, the new design of LFSR can effectively mask the power consumption characteristics of the LFSR. By adding a filter function and a flip-flop, the power consumption characteristics of the LFSR can be confused.

3.1 Power model of LFSR

In stream cryptosystems based on LFSR, the power consumption is mainly divided into three parts: the power consumption of the LFSR, the power consumption of the filter function, and other power consumption (caused by measurement errors, noise, electromagnetic radiation, etc.). These three parts are separately denoted by \( P_{LFSR} \), \( P_{h(i)} \) and \( \Omega \) respectively. The power consumption of the LFSR is composed of XOR gates \( (P_f) \) and flip-flops \( (P_{FF}) \), that is \( P_{LFSR} = P_{FF} + P_f \). At \( i^{th} \) clock cycle, the power consumed is expressed as:

\[ PD_i = P_{LFSR} + P_h + \Omega_i = P_{FF_i} + P_{h_i} + \Omega_i \]  \hspace{1cm} (1)
Among other power consumptions $\Omega$, most of the consumptions are random measurement errors. It is generally considered that the errors can be reduced by multiple measurements in the same clock cycle. The mathematical expectation measurements of $\Omega$ is a constant ($E(\Omega) = c_1, c_1 \in R$). Considered that the feedback function and filter function are realized by XOR gate, the power consumption is a const, that is $P_h + P_f = c_2, c_2 \in R$. So it can be gotten that $P_h + P_f + \Omega = c, c \in R$.

Power consumption of 0.18 $\mu m$ CMOS standard cells had been given by Kumar et al. [Kumar, Lemke and Paar (2004)] (see Tab. 1), obviously $P_{FF} \gg P_f, P_h$.

**Table 1: Power consumption of 0.18 $\mu m$ CMOS standard cells**

<table>
<thead>
<tr>
<th>Heading level</th>
<th>Normalized Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-input NAND</td>
<td>1</td>
</tr>
<tr>
<td>2-input AND</td>
<td>2.14</td>
</tr>
<tr>
<td>2-input XOR</td>
<td>3.36</td>
</tr>
<tr>
<td>D Flip Flop</td>
<td>22.55</td>
</tr>
</tbody>
</table>

**Remark:** Some results on 90 nm ASIC technology had been given by Sharif Mansouri [Sharif Mansouri (2014)].

In order to suit for CMOS-implemented power consumption, Fischer et al. [Fischer, Gammel and Kniffler (2006)] used Hamming distance based on power model to describe the power consumptions and give an approximate estimation

$$P_{FF}(0,0) \approx 0 \approx P_{FF}(1,1) \ll P_{FF}(1,0) \approx P_{FF}(0,1) \quad (2)$$

Where $P_{FF}(a, b), a, b \in \{0,1\}$ is the power consumption of flip-flop whose state is from $b$ to $a$. For simplifying the question, $P_{FF}(0,0)$ equals $P_{FF}(1,1)$ and $P_{FF}(0,1)$ equals $P_{FF}(1,0)$ was assumed. By Eqs. (1) and (2), the power consumption at $i^{th}$ clock cycle be expressed as:

$$PD_i = P_{LFSR} + c = P_{FF}(0,1) \times \text{CountZtO}_i + P_{FF}(0,0) \times \text{CountZtZ}_i + c \quad (3)$$

where $\text{CountZtO}_i$ is the count of flip-flops whose state is from 0 to 1 or from 1 to 0, and $\text{CountZtZ}_i$ is the count of flip-flops whose state is from 0 to 0 or from 1 to 1. It is clear that power consumption is determined by the state change of flip-flops in adjacent two clock cycles from the Eqs. (2) and (3).

### 3.2 Analysis of flip-flop state changes in LFSR

Because LFSR has been used to generate a maximal period sequence, the connection
Design of Feedback Shift Register of Against Power Analysis Attack

Polynomial of LFSR is selected by a primitive polynomial. For simplicity, the length of the LFSR in cipher stream is 8-(8-stages) was assumed. Example 1. The feedback polynomial (primitive polynomial) [Lidl and Niederreiter (1994)] was chosen.

\[ f(x) = x^8 + x^6 + x^5 + x^5 + 1 \] (4)

Obviously, the linear recurrence relation of Eq. (4) is

\[ s(i+8) = s(i+4) \oplus s(i+3) \oplus s(i+2) \oplus s(i) \] (5)

The period of output sequence is 255. Let IV = (01010100), the following output sequence was gotten:

0010101011011101011001100011010100111011010101001101010011010111110 01010001011111111100101110100000011100110010111100000011100011001 00100111011001000010111011001000111111110111111111110110010010000 110110001111110011110011110111101111011110111111111101110010010000 254 1 4 3 0 1 7

255 1 3 4 0 1 7

The statistical results are shown in Tab. 2, Fig. 2 and Fig. 3.

Table 2: Statistical results of the LFSR

<table>
<thead>
<tr>
<th>( i^{th} ) clock cycle</th>
<th>( P(0,0) )</th>
<th>( P(1,0) )</th>
<th>( P(0,1) )</th>
<th>( P(1,1) )</th>
<th>CoutZtO</th>
<th>CoutZtZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>254</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>255</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

Remark: \( P(a, b), a, b \in \{0,1\} \) is the count of flip-flops, if state from \( b \) to \( a \).
3.3 A new design of LFSR

Definition 1: Let $S$ be a output sequence of LFSR, then $S'$ is a power reversible sequence when $S_i \oplus S_{i+1} = 1$ and $S'_i \oplus S'_{i+1} = 0$ or $S_i \oplus S_{i+1} = 0$ and $S'_i \oplus S'_{i+1} = 1$, where $S_i$ is the output of LFSR at $i^{th}$ clock cycle.

From example 1, the following power reversible sequence was gotten

10000001110111011001100010101111001100101011111011001011101011100001001011101110010110010111000011101110111110111001011101111110011011111011111011110111010
From sequence (2), the connection polynomial by BM algorithm [Massey (1969)] was gained:

\[ f(x) = x^{10} + x^7 + x^5 + x^4 + x^2 + 1 \]  

(6)

And the linear recurrence relation of equation is

\[ s(i+10) = s(i+8) \oplus s(i+6) \oplus s(i+5) \oplus s(i+3) \oplus s(i) \]

Therefore, the new design of LFSR against the power attack was proposed. In the design, adding two additional flip-flop and a new LFSR with length \( n+2 \) was required (see Fig. 4).

**Figure 4:** The new design of LFSR against the power attack

The statistical results using the new design to implement LFSR with length 8 are shown in Tab. 3, Fig. 5 and Fig. 6.

**Figure 5:** Statistical figure of the new design LFSR with state changes
Figure 6: Statistical figure of the new design with \(CoutZtO\) and the difference of \(CoutZtO\)

Table 3: Statistical results of the new design

<table>
<thead>
<tr>
<th>(i^{th}) colck cycle</th>
<th>(P(0,0))</th>
<th>(P(1,0))</th>
<th>(P(0,1))</th>
<th>(P(1,1))</th>
<th>(CoutZtO)</th>
<th>(CoutZtZ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>1023</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>1024</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

3.4 Improvement of the design

In the design, the power consumption was masked. For confusing the power consumption, the improvement design with an additional filter function \(g(x)\), whose inputs are taps of LFSRs, to control the power consumption of the leftmost flip-flop was proposed (see Fig. 7).
**Figure 7:** The improvement design of LFSR (only the upper half) with additional filter function

For example, the Boolean function \( g(x) \) was selected,

\[
g(x) = x_1 + x_4 + x_0x_3 + x_2x_1 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4
\]

(6)

where the variables \( x_0, x_1, x_2, x_3 \) and \( x_4 \) correspond to the tap positions \( s_{t+2}, s_{t+7}, s_{t+9} \) and \( s'_{t+4}, s'_{t+6} \), and \( g(x) \) is 1-resilient, nonlinear \( N_g = 12 \) is maximum. The power trace has been disordered (see Fig. 8).

**Figure 8:** Statistical figure of the improvement design with \( CoutZtO \) and the difference of \( CoutZtO \)
4 Conclusions
Stream ciphers based on LFSR have received frequent usage in the wide range of constrained environments. The power attack is one of the serious threaten for the security of stream ciphers. The new design of LFSR basing on power model of LFSR was proposed by using the mask method. The capability of LFSR against the power attack has been improved due to the power trace has been masked and confused. The new design can be carried out easily by circuits. Since only XOR gates and flip-flops are adapted, the better synchronization performance has been achieved, which made the new LFSR suitable for wider usage in different situations.

Acknowledgement: This work is supported by Colleges and universities in Hebei province science and technology research project (Grant No. ZD2016020).

References


