 CMC, vol.58, no.2, pp.517-527, 2019

Design of Feedback Shift Register of Against Power Analysis Attack

Yongbin Zhao[1, *], XuYang[1] and RanranLi[1]

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, Barmshory 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 Kniffler (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, $F_2^n = \{(x_1,\ldots,x_n): x_i \in F_2, i = 1,\ldots,n\}$ 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.,

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

for $a_u \in F_2$,$u = (u_1,\ldots,u_n)$,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 $0 < wt(\omega) \le m$. 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, $IV = LS(0) = (s(0), s(1), \cdots, s(n-1))$, $s(i) \in \{0,1\}$ in Fig. 1. After i clock cycle, the state of LFSR is $LS(i) = (s(i), s(i+1), \ldots, s(i+n-1))$, and the leftmost bit is $s(i+n) = \sum_{j=0}^{n-1} c_j s(i+n-j)$ at the next clock cycle.

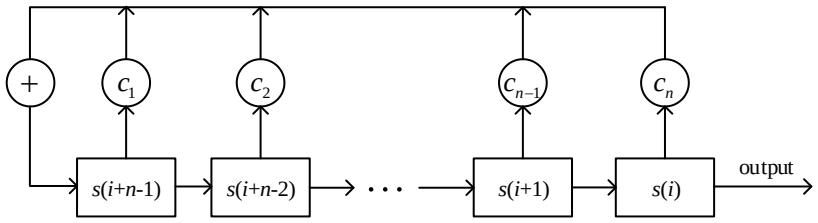

Figure 1: Fibonacci representation of LFSR with length *n*

The combination of taps and their location is often referred to as a ***connection polynomial***, and expressed $f(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_n x^n$. 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} , $P_{h(x)}$ and Ω respectively. The power consumption of the LFSR is composed of XOR gates (P_f) and filp-flops (P_{FF}), that is $P_{LFSR} = P_{FF} + P_f$. At i^{th} clock cycle, the power consumed is expressed as:

$$PD_i = P_{LFSR_i} + P_{h_i} + \Omega_i = P_{FF_i} + P_{f_i} + P_{h_i} + \Omega_i \quad (1)$$

Among other power consumptions Ω, 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 Ω 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 μm 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 μm CMOS standard cells

Heading level	Normalized Power
2-input NAND	1
2-input AND	2.14
2-input XOR	3.36
D Flip Flop	22.55

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

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

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:

$$PD_i = P_{LFSR_i} + c = P_{FF_i}(0,1) \times CountZtO_i + P_{FF_i}(0,0) \times CountZtZ_i + c \tag{3}$$

where $CountZtO_i$ is the count of flip-flops whose state is from 0 to 1 or from 1 to 0, and $CountZtZ_i$ 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

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.

$$f(x) = x^8 + x^6 + x^5 + x^5 + 1 \tag{4}$$

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

$$s(i+8) = s(\mathrm{i}+4) \oplus s(\mathrm{i}+3) \oplus s(\mathrm{i}+2) \oplus s(\mathrm{i}) \tag{5}$$

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

00101010011101110110011110111111010011001101010001100000111010101011111001010000100111111110000101111000110100000001000111000100101110000000110010010011011100100000101011011010110010110000111110110111101011101000100001101100011111001110011000101101001000101 sequence(1)

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

Table 2: Statistical results of the LFSR

i^{th} colck cycle	*P* (0,0)	*P* (1,0)	*P* (0,1)	*P* (1,1)	*CoutZtO*	*CoutZtZ*
1	2	3	3	0	2	6
2	1	4	3	0	1	7
3	1	3	3	1	2	6
4	1	3	2	2	3	5
…	…	…	…	…	…	…
254	1	4	3	0	1	7
255	1	3	4	0	1	7

Remark: *P* (*a*, *b*), $a, b \in \{0,1\}$ is the count of flip-flops, if state from *b* to *a*.

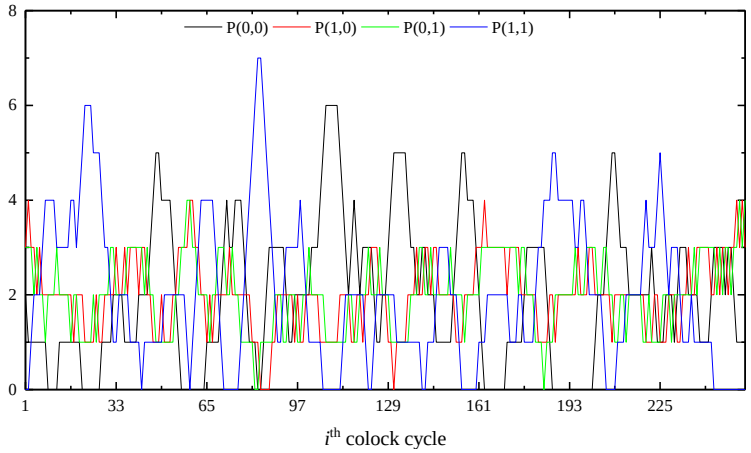

Figure 2: Statistical figure of the LFSR with state changes

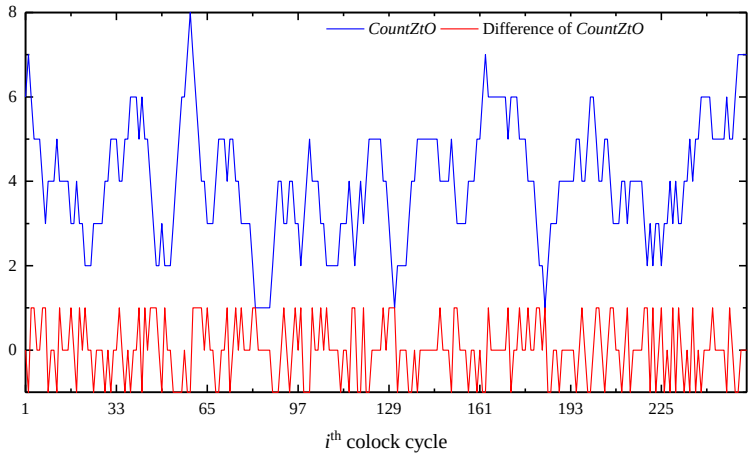

Figure 3: Statistical figure of the LFSR with *CoutZtO* and the difference of *CoutZtO*

Form Fig. 3 and Fig. 4, the power consumption of the LFSR is highly correlated in a linear way and the power consumption characteristics of stream cipher based on LFSR are vulnerable to leaking IV under the power attacks(see more details in Burman et al. [Burman, Mukhopadhyay and Veezhinathan (2007); Sharif Mansouri (2014)])

3.3 A new design of LFSR

Definition 1: Let S is 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
1000000011011101110011010001010111100110011111101100101001000000000101001111101000110101010010111101001001111010101110110110111000010010101100111000110001001110101111110001111100111100101101011100010111110111101110101

01110010010110010011001000011110001000 sequence(2)

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

$$f(x) = x^{10} + x^7 + x^5 + x^4 + x^2 + 1 \quad (6)$$

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).

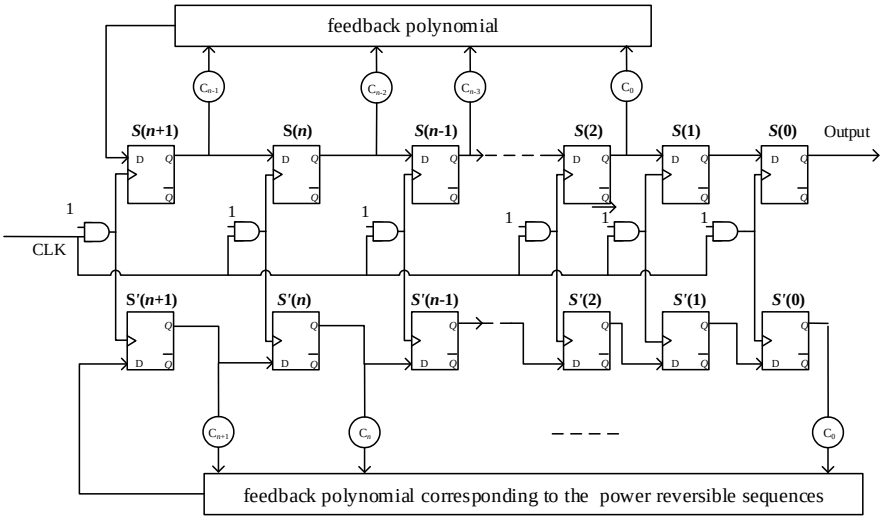

Figure 4: The new design of LFSR against the power attack

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

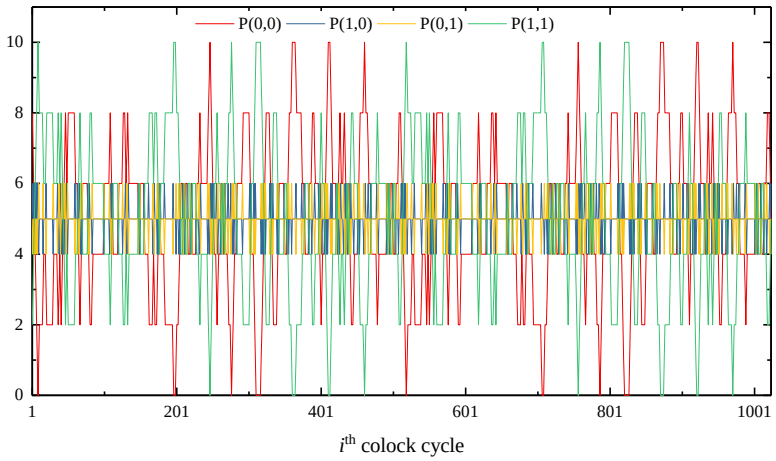

Figure 5: Statistical figure of the new design LFSR with state changes

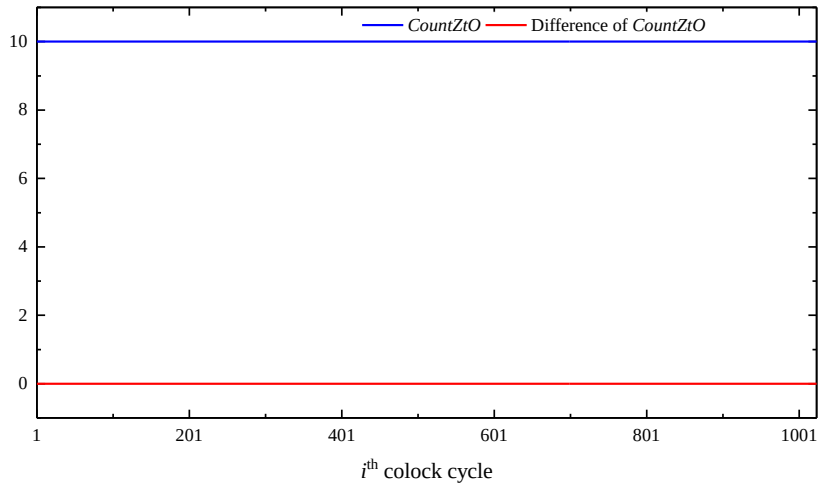

Figure 6: Statistical figure of the new design with *CoutZtO* and the difference of *CoutZtO*

Table 3: Statistical results of the new design

i^{th} colck cycle	*P* (0,0)	*P* (1,0)	*P* (0,1)	*P* (1,1)	*CoutZtO*	*CoutZtZ*
1	8	5	5	2	10	0
2	7	6	4	3	10	0
3	6	5	5	4	10	0
4	5	6	4	5	10	0
…	…	…	…	…	…	…
1023	6	5	5	4	10	0
1024	5	6	4	5	10	0

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).

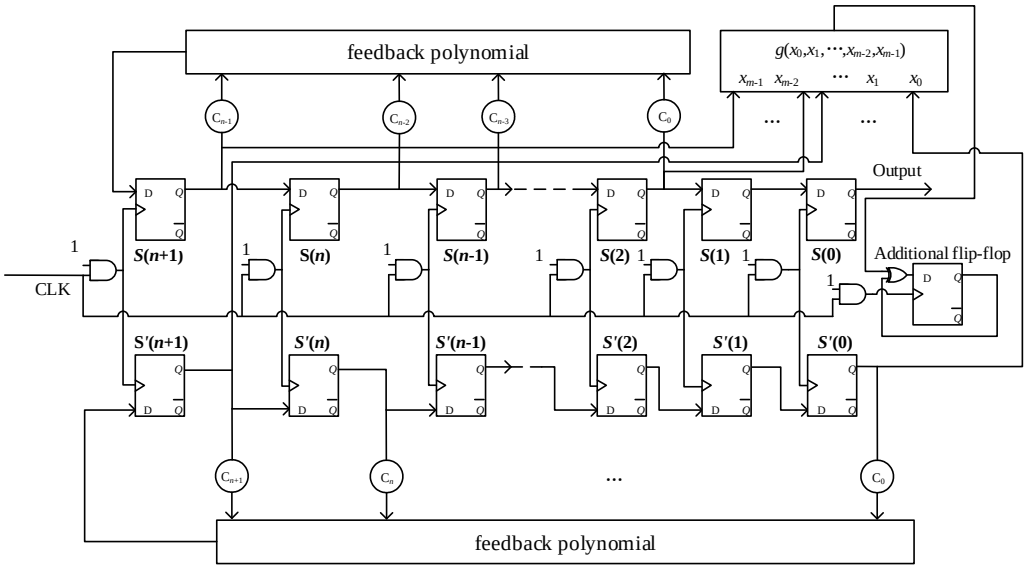

Figure 7: The improvement design of LFSR (only the upper half) with additional filter function

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

$$g(x) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4 \quad (6)$$

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).

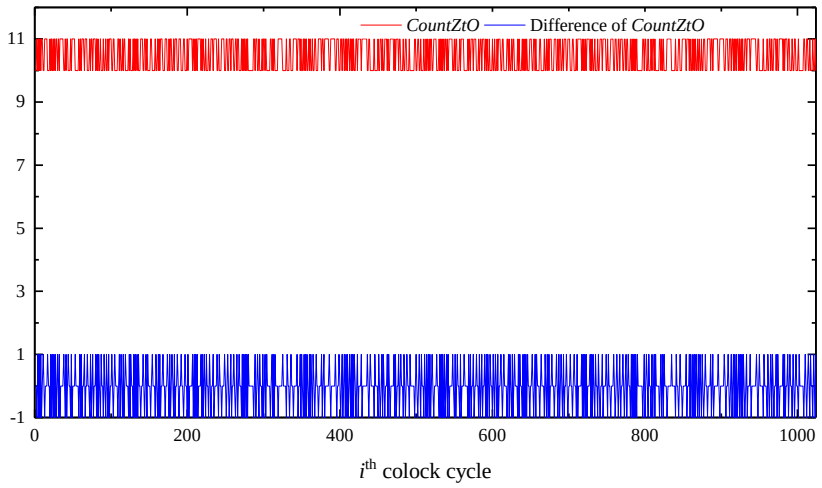

Figure 8: Statistical figure of the improvement design with *CoutZtO* and the difference of *CoutZtO*

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 carriedd 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

Aumasson, J. P.; Dinur, I.; Meier, W. (2009): Cube testers and key recovery attacks on reduced-round MD6 and trivium. *Fast Software Encryption*, pp. 1-22.

Banik, S. (2016): Conditional differential cryptanalysis of 105 round Grain v1. *Cryptography and Communications*, vol. 8, no. 1, pp. 113-137.

Burman, S.; Mukhopadhyay, D.; Veezhinathan, K. (2007): LFSR based stream ciphers are vulnerable to power attacks. *Advances in Crptology-INDOCRYPT'2007, LNCS 4859*, pp. 384-392.

Courtois, N. (2002): Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt. *International Conference on Information Security and Cryptology*, pp. 182-199.

ETSI/SAGE Specification (2010): *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*. Document 2: ZUC Specification. Version 1.4.

Fischer, W.; Gammel, B. M.; Kniffler, O. (2006): Differential power analysis of stream ciphers. *Advances in Cryptology-CT-RSA 2007, LNCS 4377*, pp. 257-270.

Goresky, M.; Klapper, A. M. (2002): Fibonacci and Galois representations of feedback-with-carry shift registers. *IEEE Transactions on Information Theory*, vol. 48, no. 11, pp. 2826-2836.

Gupta, A.; Mishra, S. P.; Suri, B. M. (2016): Differential power attack on trivium implemented on FPGA. *Proceedings of Fifth International Conference on Soft Computing for Problem Solving*, pp. 541-554.

Kocher, P. C. (1996): Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. *CRYPTO1996, LNCS 1440*, pp. 104-113.

Kocher, P.; Jaffe, J.; Jun, B. (1999): Diafferential power analysis. *Annual International Cryptology Conference*, pp. 388-397.

Kumar, S.; Lemke, K.; Paar, C. (2004): Some thoughts about implementation properties of stream ciphers. *The State of the Art of Stream Ciphers-Workshop Record 2*, pp. 311-319.

Lano, J.; Mentens, N.; Preneel, B. (2004): Power analysis of synchronous stream ciphers with resynchronization mechanism. *ECRYPT Workshop SASC-the State-of-the-Art of Stream*, pp. 327-333.

Lidl, R.; Niederreiter, H. (1994): *Introduction to Finite Fields and Their Applications*. Cambridge University Press, UK.

Massey, J. (1969): Shift-Register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, vol. IT-15, no. 1, pp. 122-127.

Meier, W. (2011): Fast correlation attacks: methods and countermeasures. *International Conference on Fast Software Encryption*, pp. 55-67.

Quisquater, J. J.; Samyde, D. (2001): Electromagnetic analysis (ema): Measures and counter-measures for smart cards. *Smart Card Programming and Security*, pp. 200-210.

Rahimi, M.; Barmshory, M.; Mansouri, M. H. (2016): Dynamic cube attack on Grain-v1. *IET Information Security*, vol. 10, no. 4, pp. 165-172.

Rønjom, S. (2017): Improving algebraic attacks on stream ciphers based on linear feedback shift register over $\mathbb{F}_{2^k}$. *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 27-41.

Shamir, A.; Biham, E. (1998): Differential fault analysis of secret key cryptosystems. *International Cryptology Conference, LNCS 1294*, pp. 513-525.

Sharif Mansouri, S. (2014): *Design and Implementation of Efficient and Secure Lightweight Cryptosystems*. KTH Royal Institute of Technology, Sweden.

Siegenthaler, T. (1984): Correlation-immunity of the combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, vol. 30, no. 5, pp. 776-780.

Tena-Sánchez, E.; Acosta, A. J. (2015): DPA vulnerability analysis on Trivium stream cipher using an optimized power model. *IEEE International Symposium on Circuits and Systems*, pp.1846-1849.

Zadeh, A. A.; Heys, H. M. (2014): Simple power analysis applied to nonlinear feedback shift registers. *IET Information Security*, vol. 8, no. 3, pp. 188-198.