IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

Low Power Linear Feedback Shift Register Using A Novel Clock Gating Technique

O. Naga Damini [1], K. Madhuri[2], S. Hussain vali[3], N. Anusha[4], K. Rohith Reddy[5]

[1]Assistant Professor, Department of ECE, Annamacharya Institute of Technology & Sciences, Tirupati, India

[2,3,4,5] Department of ECE, Annamacharya Institute of Technology & Sciences, Tirupati, India

ABSTRACT: "This method efficiently decreases the energy consumption of the widely used shift register with linear feedback by leveraging the gated clock approach. By reducing the number of XOR gates in the feedback network and implementing logic gates effectively, power consumption is significantly lowered compared to previous gated clock systems. Standard cells were used in 28-nm FD-SOI CMOS technology with a 300 MHz clock frequency to perform transistor-level simulations. Results from simulation studies demonstrate a power reduction of up to 30% compared to conventional solutions. Certain aspects of the technique employ the CPL design style, and the feedback network is executed with the advantage of gated clocks, ensuring correctness."

KEYWORDS: Complementary pass-transistor logic (CPL), gated clock, linear feedback shift register (LFSR), low-power design, transmission gate (TG)

I.INTRODUCTION

In many Electronic devices today, a lot of electronic equipment that has to quickly generate a pseudo-random sequence-like built-in tests for digital circuits uses linear feedback shift registers (LFSRs), where the most crucial merits are minimizing area, power, and time. Additionally, LFSRs are essential components of lightweight stream ciphers for embedded systems and secure communications. The purpose of word-based LFSRs is to effectively utilize the architecture of contemporary word processing systems. Several stream ciphers, including those in the SNOW series, are used in picture encode applications, use these LFSRs. An LFSR is used in the Global Positioning System to broadcast a sequence with high-precision relative time offsets fast. Moreover, To create an approximation white noise for parameter estimation and system identification, LFSRs are used.

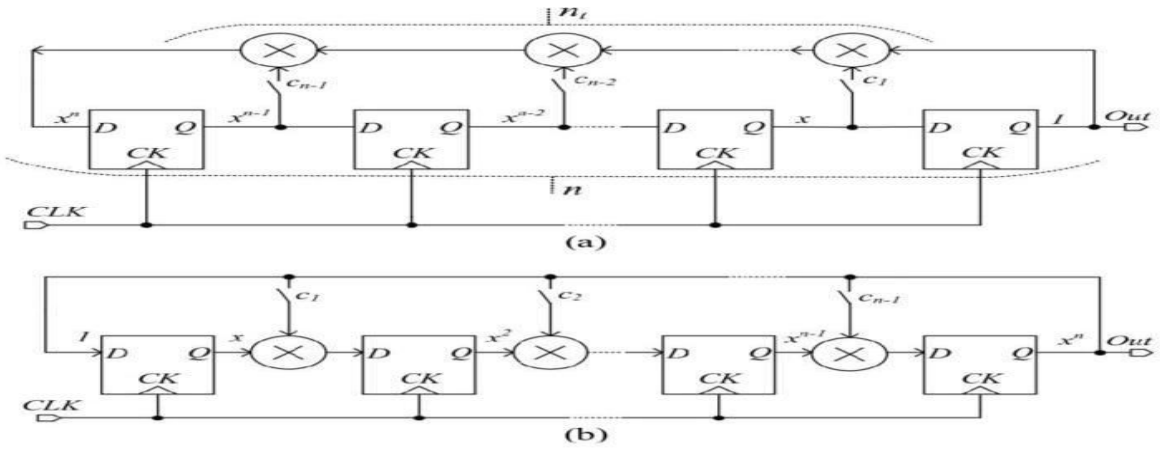

FIGURE 1. Fibonacci or standard architecture(a) and Galosis or modular architecture are two examples of generic n-bit LFSR.

Additionally, LFSRs are frequently utilized in direct sequence spread spectrum (DSSS) systems for error correction and detection through the usage of BCH (Bose, Chaudhuri, Hocquenghem) and the encoder and decoder circuits for CRC (cyclic redundancy codes). Building robust physical unclonable functions (PUFs) for cryptographic purposes has also recently made use of LFSR.

Two alternative configurations, both shown in Fig.1, can be used to provide hardware implementation of linear feedback shift registers. These configurations both produce the same output bit stream. Both the Fibonacci

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

configuration (Fig. 1a), also referred to as conventional, many-to-one, or external XOR gates, and the Galois configuration (Fig. 1b), also known as modular, one-to-many, or internal XOR gates, are the configurations mentioned. Although it is fairly easy to construct these topologies, a non-negligible amount of power is wasted since each flip-flop's clock-path toggles every clock cycle. The primary benefit of LFSRs has been obscured by the suggested solutions, which decreased energy consumption at the expense of increasing circuit complexity despite the fact that LFSR energy consumption has been extensively discussed in the literature. One of the authors has also suggested a clock gating solution to lower the power usage of the LFSRs; the analysis conducted there showed that the technological features of the gates used have a significant impact on the power reduction.

Furthermore, it was discovered in the same study that, in order to obtain a power decrease with regard to a traditional LFSR, a relationship involving technological parameters had to be satisfied. Specifically, the technique allows a maximum power saving of less than 10% with regard to a typical LFSR, even if the aforementioned relationship involving technological parameters is satisfied.

In this work, we present an improved gated clock design method for linear frequency switches (LFSRs)that significantly lowers power consumption without substantially altering the conventional basic architecture. The recommended solution allows for higher power savings over alternative gated clock systems because the clock gating network's logic gates are constructed in a power-efficient way and because the number of XOR gates in the feedback loop is properly lowered. In fact, using the recommended method has resulted in a power decrease of up to 30%.

II.BACKGROUND

A. LINEAR FEEDBACK SHIFT REGISTER

A shift register whose input bit is a linear function of its prior state is known as a linear feedback shift register (LFSR). Looking at Fig. 1's typical implementation, The cluster of flip-flops (FFs) is used to realize LFSR, and several XOR gates are used to provide linear feedback. The register operates in a deterministic manner, meaning that the stream of values it produces is entirely determined by its current state. LFSRs are based on a somewhat complicated mathematical theory, despite being quite easy to implement. Nonetheless, the nth order polynomial provides an efficient description of them.

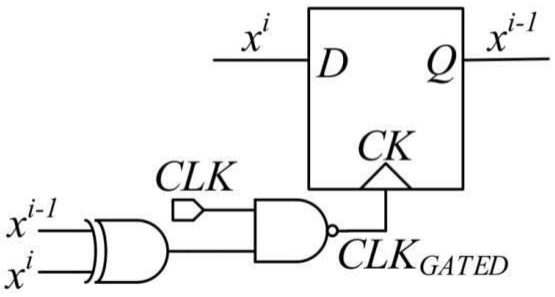

FIGURE.2: Conventional gated clock circuit

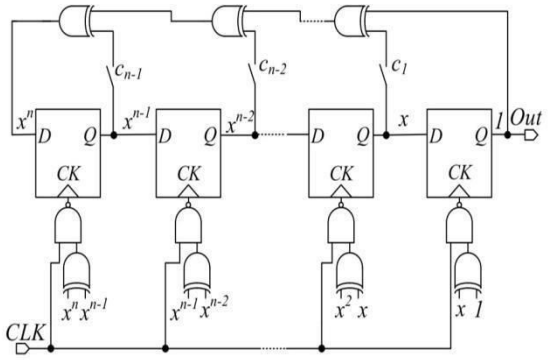

FIGURE.3: Gated clock LFSR implementation

The binary coefficients c_i (i = 1, 2, ... n-1) define the well-known characteristic polynomial (p_c) and provide information on the bit generator's various statistical features as well as the length of the pseudo-random sequence.

$$p_c = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1$$

It is possible to represent the power consumption of the standard LFSR in Fig. 1 as

$$P_{Conv} = n\, P_{FF} + n_t\, \alpha\, P_{XOR}$$

By designating P_{FF} and P_{XOR}, which correspond to the power consumption of FFs and XOR gates, respectively, and allowing α to stand for the switching activity of the inner nodes, we may assume that the maximum period in an LFSR with $n \geq 6$ is approximately equal to 0.5, indicates the register length (i.e., the generator's order), and n_t represents the number of inner taps (i.e., the number of terms of the polynomial characteristic other than x_n and 1). (2) indicates that the topologies in Fig. 1 appear to have a clock path that toggles with each clock cycle, which leads to a significant

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

power dissipation, especially at high clock rates. On the other hand, because XOR gates and the FF D-path rely on switching activity, their power consumption is 50% less than the maximum value

B. DYNAMIC POWER MANGEMENT

Digital power management (DPM), is a widely used technique for cutting down on power usage in digital systems. It entails turning off logic circuits that aren't needed for functional operations at a specific moment in time. According to the design shown in Fig. 2, this strategy, known as the "gated clock approach" at the circuit level, consists of activating flip-flops without an enable signal Fig. 3 illustrates a modified LFSR that makes use of the gated clock technique. Because more gates are needed to achieve the gated clock technique, the topology lowers flip-flop power consumption, or PFF, but at the expense of increased power consumption.

Consequently, the power consumption in (2) for the gated clock LFSR in Fig. 3 becomes only when the input signal differs from the actual output value

$P_{GC} \approx n\alpha P'_{FF} + (n + n_t)\,\alpha P_{XOR} + n\alpha P_{NAND}$

Furthermore, the term n • α • P'FF represents the dissipation of the FFs under the increased load circumstances (i.e., the additional XOR gates). An estimate of the power dissipation was made in

PGC[12] ≈ nαP'FF + ntαPXOR + nαPXORNAND

However, the benefit of the suggested topology was limited because the overall power dissipation was only 10% lower than that of a conventional (non-gated clock) LFSR.

III. IMPLEMENTED GATED CLOCK IMPLEMENTATION

A. EFFICIENT LOGIC GATE IMPLEMENTATION

Lowering the power consumption of the term PXORNAND in order to reduce the overall power dissipation. The power-aware solution shown in Fig. 4 can do this by combining the advantages of the transmission gate method (TG-MUX) and complementary pass transistor logic (CPL-XOR/XNOR).It is important to note that many FF standard cells have readily available complementary signals that are needed by the CPL-XOR/XNOR section. Furthermore, because the complete outputs of the CPL-XOR/XNOR section ensure a full voltage swing at the XORAND gate's output node without the need for additional level restoring transistors, they are ideal for driving the TG-MUX section. When a gated clock LFSR is created with the XORAND circuit shown in Figure 4, its power consumption can be represented as

PCPT _TG≈ nαP'' FF + ntαPXOR

When the FF's power consumption, PF, accommodates for the reduced capacitive effects caused by both CPL and TG circuits, and the power consumption of the gated circuit, PXORNAND, is almost completely removed.

B. REDUCED XOR NUMBER

We suggest an additional method to use the CPL-XOR/XNOR section in Fig. 4 in order to minimize the number of XOR gates in the feedback path in order to further reduce the LFSR power consumption. In fact, the binomial $x^{i+1} \oplus x^i$, with index i ranging from 0 to n − 2, at the output of this CPL gate can be utilized to store XORs in the feedback channel. Furthermore, we can take advantage of the property $x^i \oplus x^i = 0$ in the case of non-adjacent taps.

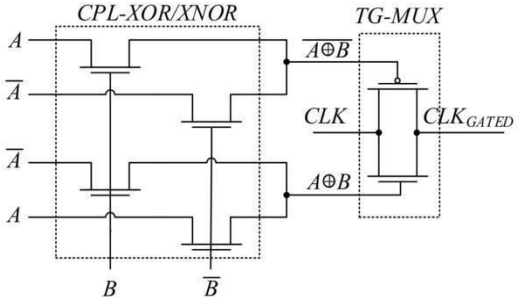

FIGURE 4. XORAND for gated clock implementation.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

Upon examining relationship (6), it becomes evident that when the characteristic polynomial has the term x and all of the taps are contiguous, the least amount of XOR operations is necessary.
The total number of XOR gates required to construct the feedback circuit for a few characteristic polynomials using both the suggested approach and the conventional topology. The quantity of inner taps, or n_t, is determined by relationship (6). It is clear that fewer XOR gates are not always needed for the recommended method. Therefore, we can effectively combine the terms x^i} at the outputs of the FFs and the outputs of the CPL-XOR/XNOR sections in order to further reduce the number of XOR gates.

Consequently, a further reduction in the number of XOR gates in the feedback loop is achieved since it equals
$n_t = n_t$ - mc (7), where mc is the number of neighbouring tap pairs but considering each tap in only one couple.
It is evident that, as a result of this approach, the total power contribution to the feedback network is reduced by an amount equal to or less than n_t, which is also the number of XOR gates needed to implement this technique.
Finally, it should be mentioned that building XOR gates with the CPL topology is not practical in the feedback network as the gates need to drive FFs instead of TGs. Yes, VDD – Vtn, or a weak logical '1', is the greatest voltage that CPL can generate. There may be a contribution from static power consumption if this value is insufficient to switch off the PMOS transistors at the input of the FFs. Therefore, CPL-XOR/XNOR gates in feedback networks are inefficient compared to the normal CMOS implementation unless extra transistors are included to facilitate level restoration.

IV. DESIGN AND SIMULATION RESULTS

The power consumption of the LFSRs created using the suggested gated clock technique, the conventional implementation, and the suggested solution have all been compared. We note that, among all LFSR architectures, the serial LFSR exhibits the lowest critical path delay. This can be achieved by reducing power consumption with the proposed approach without significantly impacting the circuit's critical path or speed.
Parallel approaches have recently been proposed, with a focus on BCH and CRC encoders. However, because of their very different architecture, it is unfair to compare the LFSR presented in this paper with these parallel approaches; for this reason, we have excluded them from the comparison.

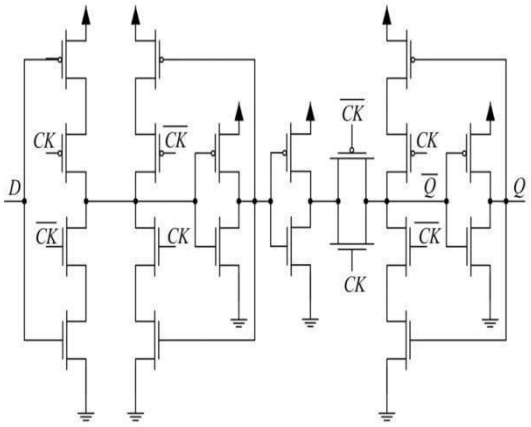

FIGURE.5: schematic of D type flipflop

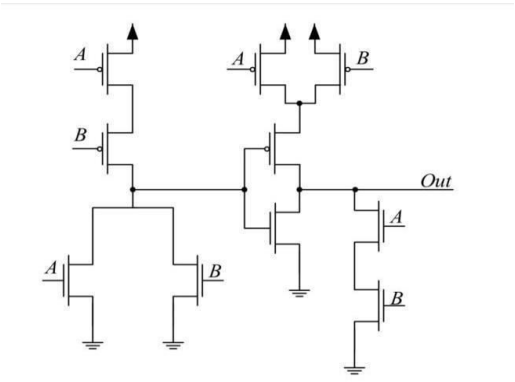

FIGURE .6 A simplified design represents the speed-optimized XOR

In addition, we used the thin oxide N-type and P-type MOSFETs from the same design kit for the circuits depicted in Figure 4. These MOSFETs have a low threshold voltage and a minimum channel length of 28 nm. Each circuit has been timed at 300 MHz and powered at 1 volt. An overview of the simulation outcomes for the LFSRs made with the different methods.

When we compare the method suggested in to the conventional implementation, we find that the clock gated design reduces the power consumption of the FFs by almost 25%; however, since additional gates are needed to implement the gated circuit, the overall power reduction is only less than 8%. Put another way, the XORNAND gates have an

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

inverse relationship with the number of taps, accounting for 12–18% of the total power usage. On the other hand, as expected, the recommended method and shown in Fig. 7 allows a significant decrease in power consumption, typically more than 20% and often exceeding 30%, especially for higher order polynomials. Finally, keep in mind that the overall power savings of the suggested gating strategy are proportionate to the number of taps, unlike the method. In fact, even while the capacitive effects of the feedback network likewise rise with the number of taps, there is an increased likelihood of finding pairs of nearby taps that reduce.

Taking into account both the conventional and the gated clock implementation, we have built the 16-bit LFSRs in VHDL and synthesised them using the Cadence Genus TM tool in order to estimate area and latency. In order to assess the area and latency of the LFSRs, we have also built the whole custom configuration of the power-aware XORAND circuit seen in Fig. 4 using the methods suggested in this work. The areas of the conventional cells and the power-aware XORAND utilised in the various 16-bit LFSR implementations have then been combined to approximate the area of the LFSRs. Every instance's feedback route determines this. The area estimates also reveal that, in addition to a significant decrease in power demand, the proposed technique results in a slight area reduction relative to the approach.

OUTPUT WAVE FORMS:

FIGURE.7: Simulated output of D- type flipflop

FIGURE 8: simulated output of XORAND for gated clock implementation.

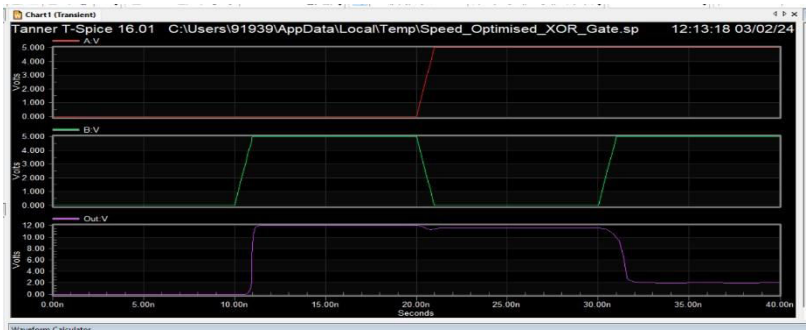

FIGURE 9: Simulated output of speed-optimized XOR gate.

V. CONCLUSION

A method for decreasing power consumption in the widely used linear feedback shift register has been thoroughly presented and analyzed. This technique combines aspects of CPL design style with the utilization of gated clocks, particularly in implementing the feedback network, thereby reducing the count of XOR gates. Through simulations conducted in a 28 nm CMOS technology, the proposed design approach has been verified.

REFERENCES

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303190|

[1] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 47, no. 5, pp. 615–621, May2000.
[2] M.Hassan Najafi, David J, "Power and area efficient sorting networks using unary processing", IEEE 35th International Conference on Computer Design, 2017
[3] R. Zimmermann and W. Fichtner, ''Lowpower logic styles: CMOS versus pass-transistor logic,'' IEEE J. Solid-State Circuits, vol. 32, no. 7,pp. 1079–1090, Jul. 1997.
[4] A. Young, "The future of cryptography: Practice and theory," IEEE IT Prof. Mag., no. 5, pp. 62–64, 2003
[5] Praveen J, Shanmukhaswamy M.N, "Power reduction technique in the LFSR uses modified control logic for VLSI circuit", International Journal of Computer Applications, Issue: 4, 2013.
[6] W. Aloisi and R. Mita, ''Gated-clock design of linear-feedback shift registers,'' IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 55, no. 6, pp. 546–550 Jun. 2008.
[7] Security Requirements for Cryptographic Modules U.S. Department of Commerce, National Institute of Standard and Technology, 2001, FIPS PUB 140-2.
[8] V. Selva Kumar, J. Mohan, "Multiple Single Input Change Test Vector for BIST Schemes",
[9] M. Goresky and A. M. Klapper, ''Fibonacci and Galois representations of feedback-with-carry shift registers,'' IEEE Trans. Inf. Theory, vol. 48, no. 11, pp. 2826–2836, Nov. 2002
[10] G. Hu, J. Sha, and Z. Wang, ''High-speed parallel LFSR architectures based on improved state-space transformations,'' IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 3, pp. 1159–1163, Mar. 2017.
[11] S. V. Murugan and B. Sathiyabhama, ''Retraction note to: Bit-swapping linear feedback shift register (LFSR) for power reduction using precharged XOR with multiplexer technique in built in self-test,'' J. Ambient Intell. Hum. Comput., pp. 6367–6373, Jul. 2021.
[12] J. Choi and N. Y. Yu, ''Secure image encryption based on compressed sensing and scrambling for internet-of-multimedia things,'' IEEE Access,vol. 10, pp. 10706–10718, 2022.
[13]L. Wang and E. J. McCluskey, "Circuits for pseudo exhaustive test pattern generation," IEEE Trans. Comput.-Aided Des., vol. 7, no. 10, pp.1068–1080, Oct. 1988.
[14] L. Benini, A. Bogliolo, and G. D. Micheli, "A survey of design tech-niques for system-level dynamic power management," IEEE Trans.Very Large Scale Integr. (VLSI) Syst., vol. 8, no. 3, pp. 299–316, Jun.2000
[15] S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based true random number generator for cryptographic application exploiting bonlinear signal processing and chaos," IEEE Trans. Signal Process.,vol. 53, no. 2, pp. 793–805, Feb. 2005.
[16] M. E. Hamid and C. H. Chen, "A note to low-power linear feedback shift register," IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 45, no. 9, pp. 1304–1307, Sep. 1998.
[17] R. Vara Prasada Rao, N. Anjaneya Varaprasad, G. Sudhakar Babu, C. Murali Mohan "Power Optimization of Linear Feedback Shift Register (LFSR) for Low Power BIST implemented in HDL", International Journal of Modern Engineering Research (IJMER),Vol. 3, Issue:3, pp-1523-1528, 2013.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details