PACE Conclave 2024
iCEST 2024 INTERNATIONAL CONCLAVE ON ENGINEERING SCIENCES & TECHNOLOGY
SEMI-COMM TECH SUMMIT INTERNATIONAL CONFERENCE ON EMERGING TRENDS IN ELECTRONICS & COMMUNICATION

ICEST_EC_021

ENERGY-EFFICIENT LFSR DESIGN USING ADVANCED CLOCK GATING TECHNIQUES

Mohammed Raihan Ahad[1], Mohammad Tufail Ahamed[1], Ameenuddin P.[1],
Mohammed Zakir B.[1*]

[1]Department of Electronics and Communication, P. A. College of Engineering, Mangalore, Karnataka.

Email: mohammedraihanahad11@gmail.com

Abstract:

Linear Feedback Shift Registers (LFSRs) represent a fundamental component in numerous digital systems, facilitating operations ranging from sequence generation to error detection and correction. However, the pervasive use of LFSRs comes with the inherent challenge of high-power consumption, particularly in battery-powered devices and energy-constrained environments. Our approach distinguishes itself from conventional gated clock strategies by focusing on two key aspects: an optimized logic gate implementation and strategic reduction of XOR gates within the feedback network. By carefully selecting and designing logic gates tailored to minimize power consumption, coupled with judicious XOR gate reduction, we achieve remarkable power savings without compromising performance or functionality. To rigorously evaluate the effectiveness of our proposed method, we conducted extensive transistor-level simulations using standard cells in a 45nm technology node. These simulations provide detailed insights into the power characteristics and performance metrics of our approach compared to conventional implementations. The simulation results demonstrate a notable reduction in power consumption, validating the efficacy of our approach in enhancing energy efficiency in LFSRs. Furthermore, comparative analysis against existing gated clock strategies showcases superior power savings, affirming the significance of our method in practical implementations.

Key Words: Linear Feedback Shift Registers (LFSRs), transistor-level simulations in a 45nm technology.

1. Introduction

Today, linear feedback shift registers (LFSR), find extensive application in electronics equipment demanding rapid creating a sequence of pseudo-random , notably in digital circuit built-in tests. In these contexts, optimizing area, power consumption, and delay stands as paramount objectives [1].

LFSRs serve as foundational components in stream ciphers for secure communication systems like GSM and LTE applications , as well as in lightweight stream ciphers tailored for embedded systems . The advent of word-based LFSRs optimizes their compatibility with modern processors structured around words. These specialized LFSRs find application across various stream ciphers, prominently featured in the SNOW series and utilized in image encryption applications [2].

LFSRs are additionally employed in producing a simulated version of white noise for tasks such as parameter estimation and system identification. They also feature in the Global Positioning System (GPS), where an LFSR facilitates the swift transmission of a sequence indicating high-precision relative time offsets. LFSRs are also mostly used in direct sequence spread spectrum (DSSS) systems, and error detection and correction by implementing BCH (Bose, Chaudhuri ,Hocquenghem) and CRC (cyclic redundancy codes) encoder and decoder circuits. Recently LFSR have been also exploited to build strong physical unclonable functions (PUFs) for cryptographic applications [3].

2. Problem statement

The continuous toggling of flip-flops in conventional Linear Feedback Shift Registers (LFSRs) leads to significant power dissipation, posing a challenge for low-power design. This research aims to develop a novel clock gating approach for LFSRs, optimizing power savings without compromising performance or introducing significant overhead. The proposed method will be evaluated for power reduction, area overhead, and overall performance, offering a solution to enhance energy efficiency in digital circuits [4].

3. Literature survey

Reducing power consumption in digital systems is paramount due to its direct impact on energy efficiency, battery life, and environmental sustainability. As modern devices become increasingly ubiquitous and reliant on battery power, minimizing power usage becomes imperative to extend operational lifetimes and reduce the frequency of recharging or replacing batteries. Moreover, in large-scale computing systems and data centers, reducing power consumption translates directly to lower operational costs and environmental footprint.

The survey reviews various methodologies and architectures designed to reduce power consumption in Linear Feedback Shift Registers (LFSRs), a crucial component in applications such as Built-In Self-Test (BIST), cryptography, and error correction. The paper by C. P. de Souza et al. [1] addresses the issue of error masking in BIST techniques by utilizing the Berlekamp-Massey algorithm (BMA). Traditional BIST methods compress test responses, leading to potential aliasing issues. The proposed BMA-based architecture crafts an efficient LFSR for generating fault-free test responses, ensuring thorough testing by comparing these sequences against responses from the Circuit Under Test (CUT), thus avoiding aliasing and maintaining minimal LFSR length. R. Oommen et al. [2] and M. Mohan et al. [3] explore different LFSR architectures and their power efficiencies. The studies compare CMOS, Gate Diffusion Input (GDI), modified GDI (mGDI), and Multi-Threshold CMOS (MTCMOS) techniques. Both papers conclude that LFSR designs using mGDI configuration achieve superior power efficiency, high performance, and reduced area utilization compared to other methods. G. Hu et al. [4] introduce an improved state-space transformation technique for high-speed parallel LFSRs, focusing on BCH and CRC encoding. The novel transformation matrix construction and efficient search algorithm enhance throughput and reduce complexity. X. Zhang [5] proposes an alternative method to shift the complexity in matrix multiplication, achieving significant power reduction without increasing critical path delay or total gate count. W. Aloisi and R. Mita [6] present a gated-clock design methodology aimed at reducing power consumption in LFSRs. The technique relies on controlling the clock signal to minimize dynamic power usage, contingent on the technological attributes of the gates. While the gated-clock design can substantially save power, it requires additional silicon area for the gating circuit. C. Manifavas et al. [7] provide a survey on lightweight stream ciphers for embedded systems, highlighting the importance of efficient cryptographic mechanisms for resource-constrained devices. Stream ciphers like AES-CTR, Salsa20, and WG-8 are evaluated for their speed [8] and low-power implementations [9], relevant to ubiquitous computing applications where power efficiency is critical. F. M. Mwaniki and H. J. Vermeulen [10] introduce a bipolar pseudo-random impulse sequence (PRIS) for system identification applications, demonstrating its efficacy in generating wideband perturbation signals. The PRIS approach is efficient in high-power applications, providing accurate frequency spectrum estimation with reduced power

ISBN-978-81-19905-39-3

losses compared to traditional methods. The surveyed papers converge on the necessity for innovative low-power LFSR designs to meet the growing demands of modern digital systems. Techniques such as the Berlekamp-Massey algorithm for alias-free BIST, GDI-based architectures for power efficiency, state-space transformations for high-speed operations, and gated-clock designs for dynamic power reduction represent significant advancements. These methodologies collectively push the boundaries of power-efficient digital design, ensuring robust performance and minimal energy consumption [11].

4. Proposed Work

Reducing the power dissipation in general can be accomplished by reducing the power consumption of the term PXORNAND. This can be done by means of the power-aware solution, which combines the benefits of the complementary pass transistor logic (CPL-XOR/XNOR) with the transmission gate approach (TG-MUX) . It's important to highlight that complementary signals required by the CPL-XOR/XNOR section are easily available as output signals of many FF standard cells. Moreover, the complementary outputs of the CPL-XOR/XNOR section are perfectly tailored to drive the TG-MUX section since they guarantee a full voltage swing at the output node of the XORAND gate without any additional level restoring transistors

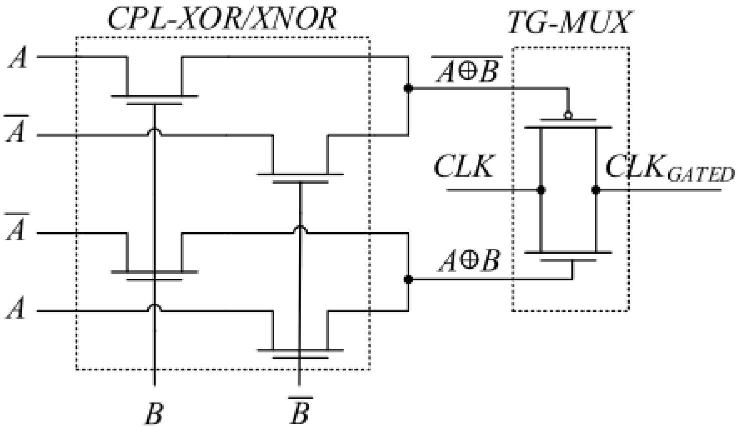

Fig 1: Power-aware XORAND for gated clock implementation

The power usage of a gated clock LFSR implemented using the XORAND circuit in fig. can be modeled as

$$P_{CPT\_TG} \approx n\alpha P''_{FF} + n_t\alpha P_{XOR}$$

where the power usage of the gated circuit, $P_{XORNAND}$, is virtually eliminated and the FFs power consumption, P_{FF}’’, accounts for the smaller capacitive effects due to both CPL and TG circuits.

4.1 Reduced XOR Number

To further cut down the LFSR power consumption, we propose an additional strategy to reduce the number of XOR gates in the feedback path, nt, by taking advantage of the CPL-XOR/XNOR section. Indeed, at the output of this CPL gate we have a binomial $x^{i+1} \oplus x^{i}$, with index i from 0 to n − 2, which can be used to save XORs in the feedback path.

For example, considering the polynomial, $x^7 + x^3 + x^2 + x + 1,$ instead of using three XORs in the feedback path to implement $x^3 \oplus (x^2 \oplus (x \oplus 1)),$ we can simply do the XOR of the binomials $x^3 \oplus x^2$ and $x \oplus 1$available at the outputs of the CPL gates. Moreover, in case of non-adjacent taps, we can exploit the property $x^i \oplus x^i = 0.$

Thus, to achieve a further reduction on the number of XOR 198 gates, we can efficiently use together the outputs of the CPL-XOR/XNOR sections, and the terms x^i at the outputs of the FFs.

Thus, a further reduction on the number of XOR gates in the feedback path is achieved, since it results equal to,

$$n_t'' = n_t - m_c$$

where m_c is the number of adjacent taps couples, but considering each tap in only one couple.

For example, in the polynomial $x^{10} + x^4 + x^3 + x + 1$ the couples of adjacent taps, m_c, are 2, that is, the couples $(x^4 + x^3)$ and $(x + 1)$.

Finally, the gated clock LFSR schematic will be as shown:

ISBN-978-81-19905-39-3

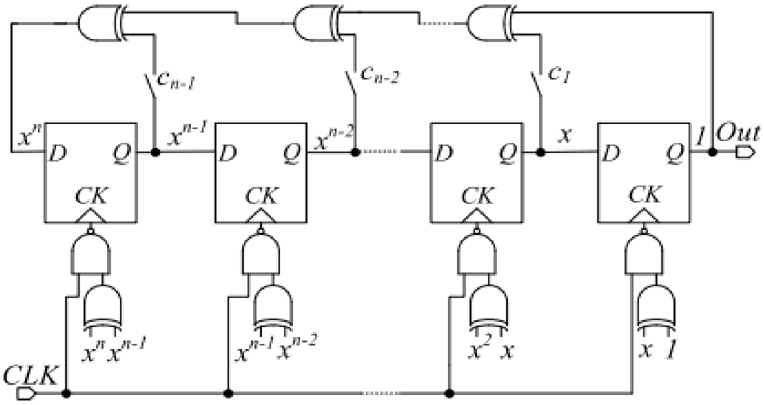

Fig 2: Gated Clock LFSR

For the digital blocks, we used the master-slave positive edge triggered D-type Flip-Flop depicted in Fig.

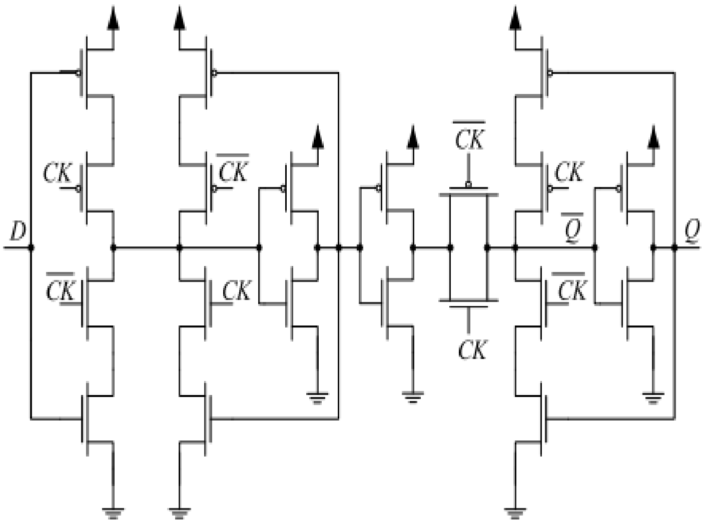

Fig 2: Schematic of Flip Flop

The two- input speed-optimized XOR gate is shown in Fig.3

ISBN-978-81-19905-39-3

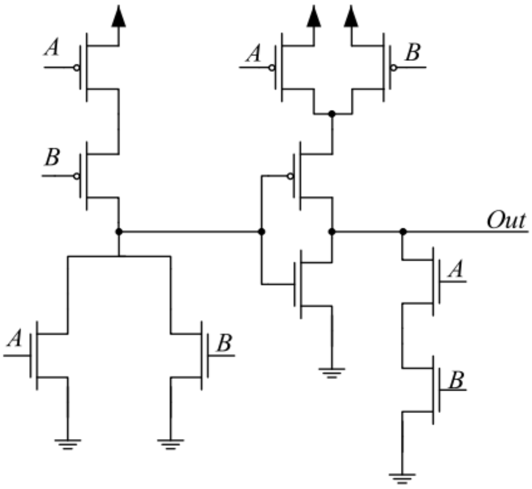

Fig 3: Simplified schematic of the speed-optimized XOR gate included in the STM standard-cell library.

5.Application

- **Pattern generators:** Novel clock gating optimizes power use, enhancing efficiency and longevity for pattern generation in LFSRs.
- **Counters:** selectively activating the clock signal, making it ideal for counters and where energy efficiency is crucial, ensuring functionality while minimizing power consumption.
- **Built in self-test (BIST)**: enhancing capabilities by reducing energy usage during test operations, thereby improving overall test efficiency and reliability.
- **Encryption:** optimizing their operation for encryption algorithms by dynamically activating clock signals only when needed, reducing energy expenditure without compromising security.
- **Compression:** dynamically controls clock signals in linear feedback shift registers, reducing power consumption compression optimizes energy efficiency in data processing, enhancing performance for low-power devices
- **Error correction:** By efficiently controlling clock signals, it can mitigate errors, enhancing error correction capabilities in data transmission systems.
- **Pseudo Random Bit Sequence**: optimizes power usage in linear feedback shift registers, enhancing efficiency for generating pseudo-random bit sequences.

5.1Advantages

- **Reduced Power Consumption**: Clock gating helps in reducing the power consumed by the circuit by gating the clock signal when it's not needed, thus minimizing unnecessary switching activity.
- **Improved Energy Efficiency**: By selectively enabling the clock signal only when necessary, energy wastage due to unnecessary clock toggling is minimized, leading to improved energy efficiency.
- **Lower Heat Dissipation**: Since power consumption is reduced, there's less heat generated by the circuit, which can help in reducing thermal issues and enhancing the reliability of the system.
- **Extended Battery Life**: In applications powered by batteries, such as portable devices, lower power consumption translates to extended battery life, which is highly desirable for users.
- **Maintained Functionality**: Despite reducing power consumption, the functionality of the LFSR is maintained. The clock gating approach ensures that the required clock pulses are delivered to the register when needed, preserving its functionality.
- **Compatibility**: This novel approach may be compatible with existing design methodologies and tools, making it easier to integrate into existing design flows without requiring significant changes.
- **Flexibility**: Depending on the design requirements, the clock gating approach can be tailored to optimize power savings while meeting performance criteria, providing flexibility in power management strategies.
- **Scalability**: The approach may be scalable, allowing it to be applied to different sizes and configurations of LFSRs, making it suitable for a wide range of applications and design scenarios.
- **Cost-Effectiveness**: By reducing power consumption without sacrificing functionality, the overall cost of the system may be reduced, particularly in terms of operating expenses related to power consumption.
- **Compliance with Power Constraints**: In systems with strict power constraints, such as IoT devices or wearable electronics, the novel clock gating approach can help ensure compliance with these constraints without compromising performance.

6. Conclusion

A proficient strategy for diminishing the power usage of the commonly used linear feedback shift register (LFSR) is introduced and thoroughly examined. The methodology incorporates the utilization of the Complementary Pass-Transistor Logic (CPL) design style in specific sections and leverages the gated clock for implementing the feedback network, thereby reducing the count of XOR gates. Through simulations conducted in a 45 nm CMOS technology, the proposed design approach has been validated. In contrast to conventional implementations, it demonstrates a notable power reduction, all without increasing the area or critical path delay.

Reference

[1]. C. P. de Souza, F. M. de Assis, and R. C. S. Freire, ‘‘A new architecture of test response analyzer based on the Berlekamp–Massey algorithm for BIST,’’ IEEE Trans. Instrum. Meas., vol. 59, no. 12, pp. 3168–3173, 312 Dec. 2010.

[2]. R. Oommen, M. K. George, and S. Joseph, ‘‘Study and analysis of various LFSR architectures,’’ in Proc. Int. Conf. Circuits Syst. Digit. Enterprise Technol. (ICCSDET), Dec. 2018, pp. 1–6.

[3]. M. Mohan and S. S. Pillai, ‘‘Review on LFSR for low power BIST,’’ in Proc. 3rd Int. Conf. Comput. Methodologies Commun. (ICCMC), Mar. 2019, pp. 873–876.

[4]. K.-J. Lee, Z.-Y. Lu, and S.-C. Yeh, ‘‘A secure JTAG wrapper for SoC testing and debugging,’’ IEEE Access, vol. 10, pp. 37603–37612, 321 2022.

[5]. 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.

[6]. D. Rupprecht, K. Kohls, T. Holz, and C. Popper, ‘‘Breaking LTE on layer two,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2019, pp. 1121–1136.

[7]. C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Y. Papaefstathiou, ‘‘A survey of lightweight stream ciphers for embedded systems,’’ Secur. Commun. Netw., vol. 9, no. 10, pp. 1226–1246, Jul. 2016.

[8]. S. Nandi, S. Krishnaswamy, B. Zolfaghari, and P. Mitra, ‘‘Key-dependent feedback configuration matrix of primitive σ–LFSR and resistance to some known plaintext attacks,’’ IEEE Access, vol. 10, pp. 44840–44854, 2022.

[9]. 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.

[10]. F. M. Mwaniki and H. J. Vermeulen, ‘‘Characterization and application of a pseudorandom impulse sequence for parameter estimation applications,’’ IEEE Trans. Instrum. Meas., vol. 69, no. 6, pp. 3917–3927, Jun. 2020

[11]. F. Zanier, G. Bacci, and M. Luise, ‘‘Criteria to improve time-delay esti- mation of spread spectrum signals in satellite positioning,’’ IEEE J. Sel. Topics Signal Process., vol. 3, no. 5, pp. 748–763, Oct. 2009.