Journal of
Low Power Electronics and Applications

MDPI

Article

Design of a Power-Aware Reconfigurable and Parameterizable Pseudorandom Pattern Generator for BIST-Based Applications

Geethu Remadevi Somanathan *,†, Ujarla Harshavardhan Reddy † and Ramesh Bhakthavatchalu

Department of Electronics & Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri 690525, India; harshareddy5055@gmail.com (U.H.R.); chidanandamrita@am.amrita.edu (R.B.)
* Correspondence: geethurs@am.amrita.edu
† These authors contributed equally to this work.

Abstract

This paper presents a power-aware Reconfigurable Parameterizable Pseudorandom Pattern Generator (RP-PRPG) for a number of applications, including built in self-testing (BIST) and cryptography. Linear Feedback Shift Registers (LFSRs) are broadly utilized in pattern generation due to their efficiency and simplicity. However, the diversity of generated patterns, as well as their power consumption, improves through circuit modifications. This work explores enhancements to LFSR structures to achieve broader range of patterns with reduced power consumption for BIST-based applications. The proposed circuit constructed on the LFSR platform can be programmed to generate patterns with varying degrees of different LFSR configurations. Diverse set of patterns of any circuit arrangement can be created using any characteristic polynomial and by utilizing the reseeding capacity of the circuit. The circuit combines a double-tier linear feedback circuit with zero forcing methods, resulting in more than 70% transition reduction, thus significantly lowering power dissipation. The behaviour of the proposed circuit is assessed for characteristic polynomials with degrees ranging from 4 to 128 using various Linear Feedback Shift Register (LFSR) topologies. For reconfigurable HDL and ASIC synthesis, the power-aware RP-PRPG can be used to generate an efficient set of stream ciphers as well as applications involving the scan-for-test protocol.

Keywords: BIST; cipher text; cryptography; Fibonacci LFSR; Galois LFSR; low-power LFSR; segmented LFSR; test pattern generator; toggle reduction; zero forcing circuit

Received: 5 May 2025
Revised: 12 June 2025
Accepted: 23 June 2025
Published: 15 August 2025

Citation: Somanathan, G.R.; Reddy, U.H.; Bhakthavatchalu, R. Design of a Power-Aware Reconfigurable and Parameterizable Pseudorandom Pattern Generator for BIST-Based Applications. *J. Low Power Electron. Appl.* **2025**, *15*, 47. https://doi.org/10.3390/jlpea15030047

1. Introduction

Linear Feedback Shift Registers (LFSRs) are widely utilized in various electronic systems requiring the generation of pseudorandom binary sequences (PRBS). Common applications include built-in self-test (BIST) of digital circuits [1–11], where minimizing power, delay, and area is critical. Additionally, LFSRs serve as core components in stream ciphers for secure communications [12–16].

BIST is a Design-for-Testability (DFT) technique that embeds test logic within the chip to autonomously identify faults. It has emerged as a practical solution to VLSI testing challenges due to its advantages, such as (a) enabling at-speed and in-field testing, (b) improved testability, (c) reduced dependence on automatic test equipment (ATE), (d) enhanced flexibility and customization, and (e) support for periodic and online testing. Among various pattern generators used in BIST, LFSRs are especially favored because of their low area overhead, efficient fault coverage, scalability, and inherent randomness.

While the pseudorandom nature of LFSR-generated patterns benefits certain applications like cryptography, the low correlation between consecutive patterns results in high switching activity during test applications. This leads to increased dynamic power consumption. In scan-based testing, the impact is even more severe due to higher switching in scan chains, raising the risk of thermal stress or even permanent damage to the Circuit Under Test (CUT). Factors such as concurrent activation of internal cores and power-hungry DFT circuits further exacerbate this issue [17–22]. Thus, controlling test power is a major design consideration during LBIST implementation.

A wide range of approaches have been explored to reduce test power [11,21,23–33]. These include techniques like (i) test scheduling algorithms, (ii) low-power RAM testing, (iii) toggle suppression, (iv) LFSR tuning, (v) vector filtering BIST, (vi) circuit partitioning, and (vii) low-power test pattern generators. Among these, modifying the test pattern generator stands out due to its direct influence on power and ease of integration within existing BIST frameworks.

This paper proposes a novel low-power test pattern generator that is based on a tiered or bipartite LFSR architecture. To reduce the transition density in generated vectors, the design incorporates a zero-forcing logic. The aim is to improve correlation between test patterns, thereby lowering scan-in power.

In [34], Dual-LFSR (DL) and Quad-LFSR (QL) architectures were proposed for BRLWE-based cryptographic schemes. These parallelized hardware designs achieved 1.6× and 2.7× reductions in computational time, respectively.

Learning with Errors (LWEs) is a foundational cryptographic problem involving the solution of linear equations perturbed by small errors. Proposed by Regev in 2005, LWEs is computationally difficult due to matrix–vector operations. Its ring variant, Ring Learning with Errors (RLWEs), improves efficiency by operating in a polynomial ring, reducing key size. Binary Ring Learning with Errors (BRLWEs) further simplifies implementation by replacing Gaussian-distributed errors with binary errors, making it attractive for hardware realization. Nevertheless, the area-delay product (ADP) in BRLWE-based architectures still requires optimization.

To meet performance, area, and power targets, LFSR design strategies now emphasize advanced topological structures, high fault coverage under low-power constraints, and parallelism. Implementing LFSRs on FPGAs provides design flexibility and rapid prototyping across various polynomial degrees and feedback taps. Moreover, FPGA-based implementations support reconfigurability, making them suitable for dynamic verification and reduced time to market.

Despite their strong statistical properties, LFSRs generate output patterns that follow linear recurrences. The fixed feedback taps define the recurrence relation, which can be mathematically predicted, thus limiting the suitability of LFSRs for cryptographic functions [35].

In the context of LBIST, the pseudo-random patterns with low inter-pattern correlation exacerbate power consumption during scan shifting. This phenomenon, known as scan-in power, can be mitigated by reducing toggle rates through modifications in the Test Pattern Generator (TPG). For example, the programmable LFSR in [30] incorporates a two-stage design to reduce transition density, thus lowering dynamic power consumption.

Several studies have investigated the design of LFSR-based pseudorandom pattern generators. While some aim to maximize pattern diversity, they often do so at the cost of higher power or area. Others fail to provide sufficient flexibility or reconfigurability. This work presents an architecture that combines multiple LFSRs operating over a polynomial ring of the form

$$x^p + x^{p-1} + \cdots + 1 \quad (1)$$

where p is the degree of the polynomial. The goal is to enhance pattern diversity, reduce power consumption, and ensure hardware efficiency through structural innovations. The major contributions of this work are

- A method to increase the correlation between generated patterns by segmenting the polynomial and combining with zero forcing, which significantly contributes towards power reduction.
- Creating distinct sets of pseudorandom patterns by programming the coefficients in feedback along with the initial seed values or configurability based on the user requirements.

The rest of this paper is organized as follows: Section 2 presents the background and related work, while Section 3 discusses the proposed design. Section 4 showcases the simulation results and analysis. Section 5 provides a comparison of the results, and finally, Section 6 concludes the paper with a summary and future scope.

2. Preliminaries

Pseudo-random binary sequence (PRBS) generators are registers with input bits from a function of a prior output state. The outputs are a set of pseudorandom sequences based on an initial value known as a seed. The function of LFSR is generated by connecting the XOR function at tap points, which is decided by a characteristic polynomial. Thus, an m-bit LFSR traditionally spans using controlled D-type storage elements (DFFs) and an interconnected system of feedback routes regulated by coefficient switches represented as C_i. The D-Flip flop outputs are routed to XOR gates, as demonstrated in [34–36]. The quantity of D-Flip flop signifies the degree (m) of an LFSR, which regulates the number of patterns in the output sequence. The longest possible duration (period, L) is assigned by

$$L = 2^m - 1 \tag{2}$$

Based on the circuit structure, two fundamental circuit classifications evolved: Galois (Internal or Type 1 or Modular) feedback and Fibonacci (External or Type 2 or Standard) feedback LFSR, which are duals and are given in Figure 1 and Figure 2 respectively. Comparisons between the two structures reveal that Galois provides the leading frequency of operation required for high-performance applications, while Fibonacci offers the advantage of uniformity of the shift register [37,38].

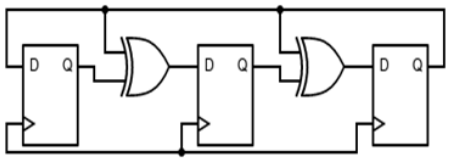

Figure 1. Galois LFSR structure.

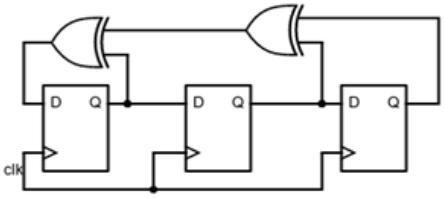

Figure 2. Fibonacci LFSR structure.

Depending on whether the characteristic polynomial is primitive or non-primitive, both Galois or Fibonacci can generate $2^m - 1$ or a lesser number of sequences, which can

be updated using extra circuitry to create all 2^m sequences where m is the degree of the polynomial. An initial seed value is required to start the sequence generation and the process of preloading these values is known as *reseeding* the LFSR. The seed loading process is made viable through integrating multiplexer modules into the circuit. The structure of an LFSR with degree m, on the other hand, may be anticipated by the feedback coefficients C_i and the output states' patterns because of its deterministic period, which is outlined by the following Equation (3) [35]:

$$S_{i+m} = \sum_{j=0}^{m-1} C_j S_{i+j} mod 2; S_j C_j \in 0, 1; i = 0, 1, 2, .. \quad (3)$$

Consider that the LFSR is primarily loaded with values S_0, S_1, ... S_{m-1}, then the next output bit S_m which forms the input to the leftmost D-FF of the LFSR, can be processed by the sum-XOR of D-FFs outputs and subsequent feedback coefficients C_i; thus, developing Equation (3):

$$\begin{aligned} S_{m+1} &= S_m C_{m-1} + ... + S_2 C_1 + S_1 C_0 mod 2 \\ S_{m+2} &= S_{m+1} C_{m-1} + ... + S_3 C_1 + S_2 C_0 mod 2 \\ &\cdots\cdots\cdots \\ S_{2m+1} &= S_{2m} C_{m-1} + ... + S_{m+1} C_1 + S_m C_0 mod 2 \end{aligned} \quad (4)$$

Thus, Equation (4) identifies m linear sets of equations involving sequences, with constant C_i values throughout all equations. If the coefficients C_is diverge with newfound states, then Equation (4) becomes void and cannot be credibly used for estimating the coefficients C_is.

2.1. Evaluation of Periodicity and Randomness

LFSRs have solid statistical attributes when the coefficients are selected effectively to achieve a possible largest length. Furthermore, for an assumed degree m, an LFSR can generate patterns of varying durations (periods) decided by the feedback coefficients as well as the starting state of the LFSR. The polynomial given in Equation (5) represents an LFSR with a feedback coefficient vector (C_0,C_1,C_2,..... C_{m-1}) [35].

$$C_0 = Cx + C_2 x^2 + C_3 x^3 + ... + C_{m-1} x^{m-1} + x^m = C(x) \quad (5)$$

To give an example, the coefficient ($C_0 = 1, C_1 = 1, C_2 = 0, C_3 = 0$) represents the primitive polynomial, $C(x) = 1 + x + x^4$. Thus, primitive polynomials can vary based on feedback coefficients and initial charging states. Proper coefficients and launching state choices allow for the deployment of maximum-length sequences with high linear complexity. The linear complexity profile measures how "random" or "structured" a sequence is. Primitive polynomials are specific forms of irreducible polynomials that are approximately equivalent to prime numbers in that they have only one factor: the polynomial itself. Primitive polynomials may be computed rather readily and consequently, maximum-length LFSRs are trivial to identify. For each given degree m, several primitive polynomials can be evolved and generally, there are many possible primitive polynomials for every given degree m. As an example, the literature [39] states that there are 69,273,666 distinct primitive polynomials for degree m = 31. Linear complexity is the primary characteristic for assessing the unpredictability of a key stream. The linear complexity test of LFSRs represented by a primitive polynomial of degree m is L/2 because an LFSR primitive polynomial stimulates an L number of sequences within its period [40]. The dynamic

behavior of the linear complexity test for the first n of generated patterns for Fibonacci with degree $m = 4$ and polynomial $C(x) = 1 + x + x^4$ with the charging state [0010] is given in Figure 3. The blue coloured graph represents the profile for the Fibonacci LFSR and orange colored graph represents that for $L \approx n/2$. This profile graph is near $L/2$ in its overall period, in which $L(2^4 - 1) = 15$. In essence, if $L \approx n/2$, the sequence has high linear complexity, and if $L \ll n/2$, the sequence has low linear complexity. Consequently, the linear complexity profile for LFSR circuits with primitive polynomials that change according to feedback coefficients and starting charge states is deemed suitable and decent for the representation of statistical pseudo-randomness.

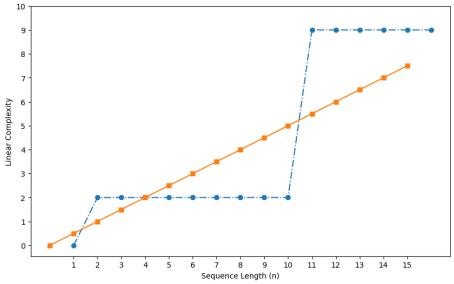

Figure 3. Linear Complexity profile generated for $C(x) = 1 + x + x^4$

2.2. Understanding Power Reduction

Compared to static power resulting from leakage currents, dynamic power is the primary source of power consumption in LFSR and is proportional to the circuit's switching activity. Equation (6) represents the dynamic power of the circuit. Mitigation of dynamic power can be achieved by techniques such as (a) reduced switching activity, (b) segmented LFSR, (c) gated clocking, and (d) low-transition designs.

$$P_d = \alpha \cdot C_L \cdot V_{dd}^2 \cdot f \tag{6}$$

where switching activity is represented by α, load capacitance is C_L, supply voltage is V_{dd}, and clock frequency is given by f. While lowering the supply voltage significantly decreases power usage, reliability and circuit speed may be impacted. The capacitance C_L is determined by the physical layout and technology utilized; therefore, reducing the value may necessitate adjustments to the design. Minimizing switching activity strategies such as (1) using low-transition LFSR designs or (2) clock gating and methods like segmentation and parallelism contribute to minimizing the activity component, α. The tradeoffs and considerations during the reduction of dynamic power are as follows: (a) Power vs. performance: reducing dynamic power frequently results in decreased performance (e.g., slower speed owing to lower frequency or voltage). Designers must strike a balance between power efficiency and performance requirements. (b) Complexity: using advanced approaches such as clock gating or dual-polynomial LFSRs might complicate the design, necessitating more sophisticated control logic and verification processes. The segmentation and parallelism method in low-power LFSR design consists of strategies to divide the LFSR into smaller segments that function independently, thereby allowing each segment to be clocked less frequently, lowering the total switching activity and dynamic power. This work investigates slicing a specific LFSR into two to reduce complexity and, consequently, hardware overhead. Because of its segmented architecture, the proposed approach can consume less power while ensuring consistency across all configurations and bit lengths.

3. Proposed Circuit

The objective is to use two consecutive low-correlated sequences to generate a highly correlated sequence, which involves injecting a new test vector between them with a significantly reduced hamming distance. Consequently, these patterns have a shorter hamming distance, which decreases the rate of toggling and, thus, the dynamic power of the circuit. Figure 4 illustrates the top-level description for the proposed RP-PRPG with input *seed* for the initial seed value and the *load_seed* input, which is used to charge these values through the application of a high value. The value at *ie* decides whether the circuit works as a Fibonacci or Galois circuit. The input *pol* chooses the set of coefficients to be tailored according to the configuration determined using *ie*, and the entire operation is wrapped up using a high value in *load_pol*. The clk signal acts as the dominant clock for the design which can be employed to regulate other sequential segments in the circuit. When enabled, the *reset* signal resets all of the output values and the *en* pin operates to activate the circuit. Outputs with reduced hamming distance are deployed using the *sequences* out pin.

Figure 5 illustrates the envisioned overall circuit architecture of the RP-PRPG using Fibonacci adopted for the convenience of description; higher degrees have identical constitutions but are more expansive in dimensions. The primary components of the proposed technique are a two-segment LFSR and a zero-forcing circuit. Clk1, Clk2, and Clk3 are split in the ratio 1:2:1, ensuring that no clocks operate simultaneously. The LFSR's partitioning is based on the MSB and LSB bits, and it is controlled by two clocks generated from the main clock. These derived clocks determine whether the first or second segment is operational at any given moment. Since only one segment is active at a given time, an extra flip-flop is required to maintain the data flow between both segments, even if it propels the area overhead. A zero-forcing circuit places zero between bits that have a difference in state value. Typically, the patterns generated are pseudorandom, with minimal pattern correlations, resulting in a higher hamming distance. Using this method, the transition between subsequent bits is significantly reduced. A larger hamming distance immediately increases power consumption during testing, which we mitigate in our design by segmenting the LFSR based on bit size. Figure 6 shows the functioning of the controller that generates control signals for the circuitry. This brings in three clock signals for the RP-PRPG as well as the tap selection. The derived clock signals dictate which segment in the RP-PRPG produces the sequences. A high value in the clock signal enables a segment, which thus generates sequences while other segment stays idle. Any of the three derived clocks can be enabled within a single cycle of the primary clock. Two of the clocks correlate to the two segments and the connection flip-flops, while the third clock relates to the zero forcing circuit.

Two-segment LFSR is a setup that involves dual segments of LFSR with a connector flip-flop. The data is separated into two layers: MSB in the first tier and LSB in the second tier, with the flip-flop serving as a link between the two. The data is subsequently sent via a zero-forcing circuit, which aids to decrease the quantity of transitions between two output patterns. If any of the bits in two consecutive patterns change, they are forced to zero. Table 1 depicts the process of reduction in transition, with a new sequence introduced between two successive sequences: seq1 and seq1. The entire number of transitions between seq1 and seq2 is divided across the new sequence s'. The total number of transitions between seq1-s' and s'-seq2 will be the same as for the conventional sequence seq1-seq2.

The clock determines whether the output is from the dual-layer LFSR or the zero-forced output. The dual-tier LFSR sends the test vector to the zero forcing circuit, where the previous and current test vectors are compared and the new vector is sent out as the next test vector, since the transitions will be fewer in number. Thus, zero forcing adds a new vector between all test vector pairs from the LFSR.

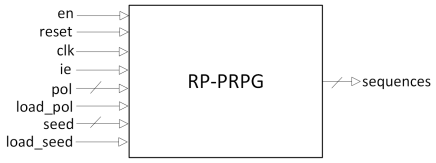

Figure 4. Top level description of RP-PRPG.

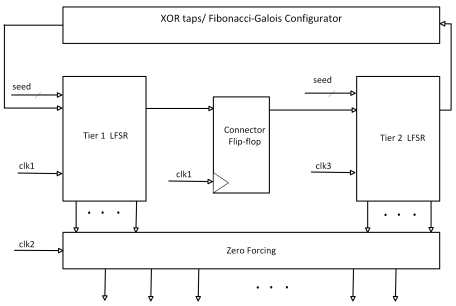

Figure 5. Hardware architecture of RP-PRPG.

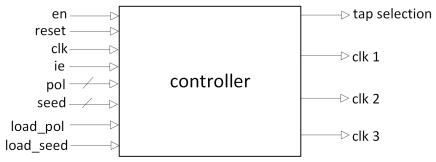

Figure 6. Operational concept.

Table 1. Illustration of zero forcing circuit.

Test Pattern	bit1	bit2	bit3	bit4	bit5	bit6	bit7	bit8
seq1	1	1	0	0	1	0	1	1
s′	1	0	0	0	0	0	1	0
seq2	1	0	1	0	0	1	1	0

4. Simulation & Performance

The RP-PRPG described in Figure 5, is built and evaluated in HDL Verilog, thus enabling quick reconfiguration and functional verification for the different bit lengths and circuit configurations. ModelSim was used for functional verification, while Xilinx VivadoSuite 2015 was used for implementation on the Artix-7 FPGA board, which was developed using 28nm high-performance, low-power (HPL) technology. This provides an excellent blend of power, efficiency and performance, making them suitable for applications including communication, automotive, and industrial equipment. This section presents the results of the circuit simulation across various bit combinations, configurations and output patterns. Figures 7 and 8 illustrates and compares the simulation wave patterns for 8-bit versions of conventional Fibonacci LFSR and the proposed design built on the primitive polynomial $x^8 + x^6 + x^5 + x^4 + 1$, whereas Figures 9 and 10 shows a similar comparison for Galois LFSR configuration of the same polynomial. The violet color in the waveform shows the pattern's transition count, while the cyan color represents the seed values utilized and the polynomial. All these circuits utilized a seed value of $(91)_{16}$ across all configurations and all these circuits generate all 256 patterns and are evaluated for several output patterns, as shown in Table 2. All the circuits are compared for 100 to 500 number of output sequences. Columns three and six correspond to the transition count of the Fibonacci and Galois configuration of the proposed design and comparing these values against the transition count of conventional circuits, it can be verified that the number of transitions is lower for the proposed circuit. The percentage reduction of transitions for

both cases is given in columns four and seven and in all cases the percentage reduction is greater than 70%.

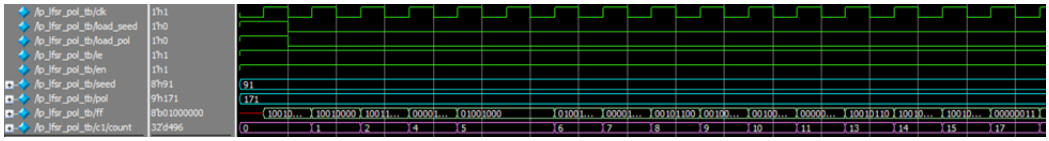

Figure 7. Simulations of the 8-bit version of the proposed circuit in Fibonacci configuration.

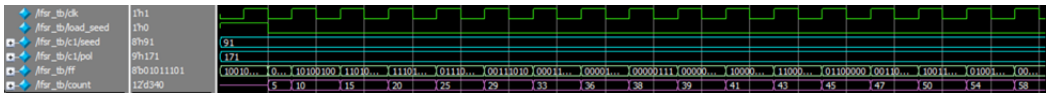

Figure 8. Simulations of 8-bit conventional Fibonacci LFSR circuit.

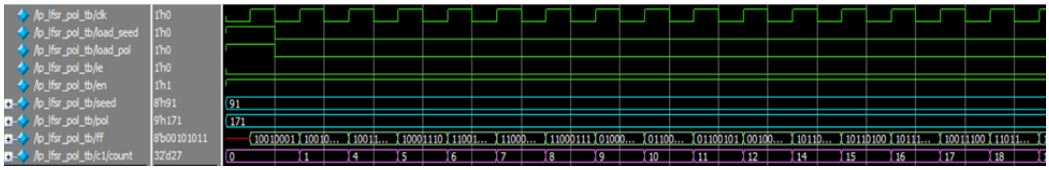

Figure 9. Simulations of the 8-bit version of the proposed circuit in Galois configuration.

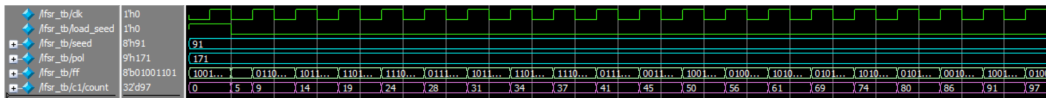

Figure 10. Simulations of 8-bit conventional Galois LFSR circuit.

Table 2. Comparison of transition reduction in 8-bit Fibonacci and Galois circuits.

# Output Sequences	Fibonacci Configuration			Galois Configuration		
	Conv.	Prop.	%Red.	Conv.	Prop.	%Red.
100	378	89	76.46	408	101	75.25
200	790	192	75.7	792	200	74.75
300	1164	319	72.59	1222	320	73.81
400	1566	429	72.61	1642	440	73.2
500	2014	532	73.58	2007	555	72.35

Output Sequences: Represents the number of output sequences under consideration; Conv.: represents conventional LFSR; Prop.: represents propsed circuit; %Red. represents percentage reduction.

The LFSR polynomial is parameterized in HDL code, since it is typically used only once before an operation, decreasing the number of primary pins required. The design was modeled for 4-, 8-, 16-, 32-, 64-, and 128-bit LFSRs with primitive polynomials, and the same number of output patterns, comparing the number of transitions between the proposed and conventional LFSR structures. For both conventional and proposed LFSR, the transition counter keeps track of the number of transitions that occur in their output. Tables 3 and 4 illustrate the simulation insights across different parameters, configurations, and output patterns. To examine and analyze the decrease in transition count between 4, 8, 16, 32, 64, and 128-bits in the proposed design and the classic LFSR, both designs were simulated for the same polynomials and for 100, 200, and 500 output patterns. The toggle reduction in both Fibonacci and Galois configurations is analyzed for an equal number of output sequences. Figure 11 shows the number of toggles obtained for both these configurations for 100 output patterns. The toggles are reduced in the proposed design in both the Fibonacci as well as the Galois configuration. Similarly, Figures 12–15 represents the reduction in the toggle for 200, 300, 400, and 500 output patterns in both configurations. The percentage reduction in the toggle is plotted for the Fibonacci configuration and is given in Figure 16. It shows that the reduction percentage increases consistently once the number of bits

crosses 60. Depending on the polynomial under consideration, this value can change. Thus, after this value, the toggle rate shows a reduction of more than 80%. Similarly, the percentage reduction of the toggle rate is calculated for the Galois configuration and is given in Figure 17. The percentage reduction in toggling is lower for 100 runs compared to 500 runs. As more patterns are considered, the toggle reduction percentage improves.

Table 3. Comparison of reduction in transition across different bits in Fibonacci configuration.

# Bits	Conventional LFSR					Proposed Design					Reduction %				
.	100	200	300	400	500	100	200	300	400	500	100	200	300	400	500
4	215	426	639	855	1066	69	140	210	281	350	67.91	67.14	67.14	67.13	67.17
8	378	790	1164	1566	2014	89	192	319	429	532	76.46	75.7	72.59	72.61	73.5
16	696	1532	2491	3143	3850	163	367	531	720	947	76.58	76.04	78.68	77.09	75.4
32	1144	2571	4359	5907	7584	232	651	976	1206	1572	79.72	74.68	77.61	79.58	79.27
64	2157	5351	8368	11,186	14,299	314	907	1689	2422	3114	85.44	83.05	79.82	78.35	78.22
128	2654	8759	15,113	21,650	28,224	332	1248	2264	3645	5217	87.49	85.75	85.02	83.16	81.52

Table 4. Comparison of reduction in transition across different bits in Galois Configuration.

# Bits	Conventional LFSR					Proposed Design					Reduction %				
.	100	200	300	400	500	100	200	300	400	500	100	200	300	400	500
4	208	421	639	848	1061	70	140	209	276	346	66.35	66.75	67.29	67.45	67.39
8	408	792	1222	1642	2007	101	200	320	440	555	75	71.59	73.65	74.54	73.84
16	712	1511	2339	3136	4015	151	364	521	727	947	78.79	75.91	77.73	76.82	76.41
32	768	2099	3662	5531	7263	156	462	832	1282	1667	79.69	77.99	77.28	76.82	77.05
64	412	1174	2208	3870	5821	99	214	400	608	849	75.97	81.77	81.88	84.29	85.41
128	297	688	1494	2766	4215	101	200	300	416	550	65.99	70.93	79.92	84.96	86.95

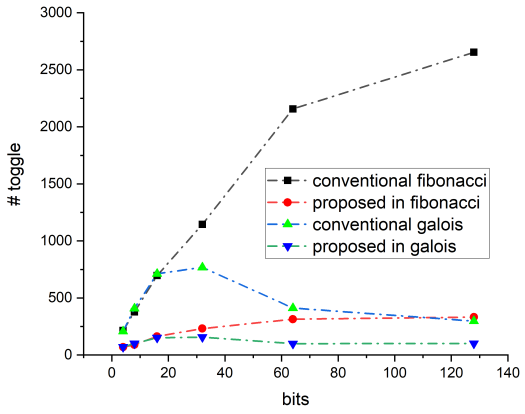

Figure 11. Toggle reduction for 100 output patterns.

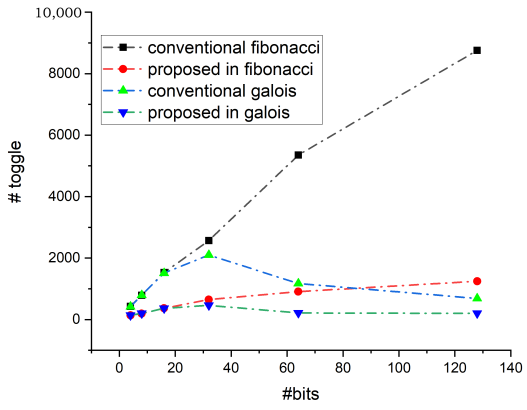

Figure 12. Toggle reduction for 200 output patterns.

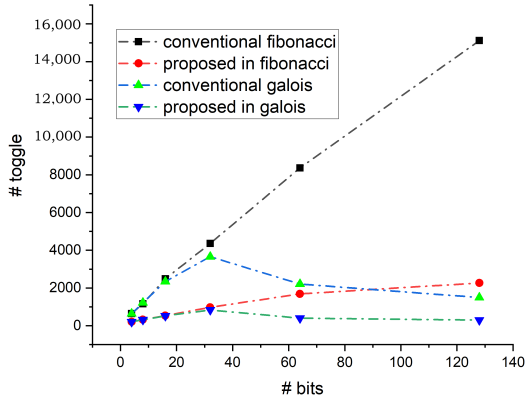

Figure 13. Toggle reduction for 300 output patterns.

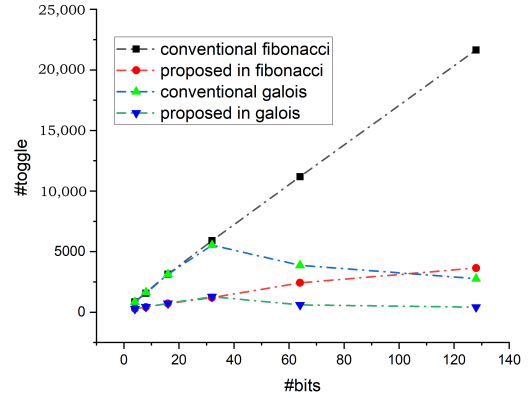

Figure 14. Toggle reduction for 400 output patterns.

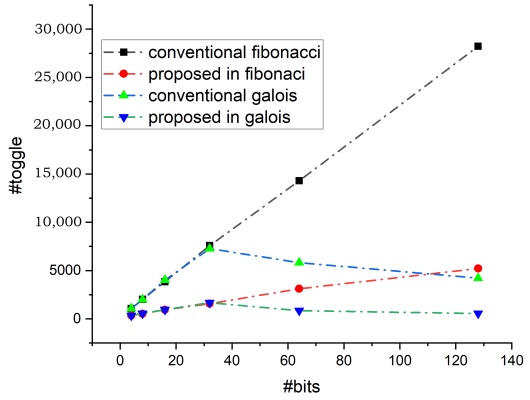

Figure 15. Toggle reduction for 500 output patterns.

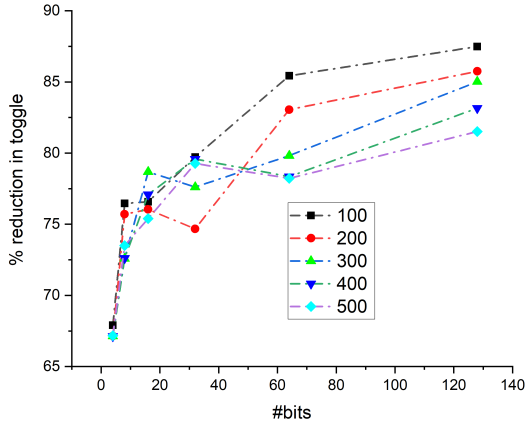

Figure 16. Percentage reduction of toggle rate in Fibonacci configuration.

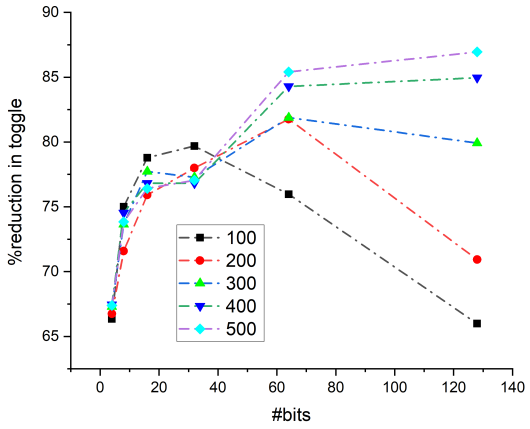

Figure 17. Percentage reduction of toggle rate in Galois configuration.

The proposed design is implemented in the Artix-7 FPGA board. Table 5 shows the implementation results across different bits of the proposed design for 10 ns clock. The total on-chip power dissipation shows only a variation from 0.133W to 0.21W when the polynomial degree changes from 4 to 128, which is approximately 57.89% only. The flip-flop count increases from 14 to 388, and the LUT usage rises from 37 to 728 from 4 to 128 bits. Despite this, the power overhead is limited to just 57.89%, indicating that the increase in resource usage has minimal impact on overall power consumption. The results are compared against a baseline conventional architecture (given in Table 6) that does not incorporate any low-power techniques, as in the proposed design.

Table 5. Performance metrics of proposed design on FPGA.

Poly	Clk	Total	WNS	Utilization			Total	Dyn.	Stat.	Jn.
deg.	(ns)	Del.	(ns)	FF	LUT	IO	pow. (W)	pow. (W)	pow. (W)	tmp. (°C)
4	10	3.079	6.902	14	37	17	0.133	0.003	0.131	25.2
8	10	4.582	5.156	26	60	20	0.135	0.005	0.131	25.3
16	10	5.483	4.449	50	126	53	0.141	0.010	0.131	25.3
32	10	5.658	4.117	98	266	101	0.151	0.020	0.131	25.3
64	10	5.624	4.193	195	471	197	0.172	0.042	0.131	25.3
128	10	6.711	3.104	388	728	389	0.21	0.079	0.131	25.5

Poly deg.: represents the degree of polynomial; Total Del.: represents the total delay; Total pow. (W): represents the total power dissipation in watt; Dyn. pow. (W): represents the dynamic power dissipation in watt; Stat. pow. (W): represents the static power dissipation in watts; Jn. tmp. (°C): represents the juntion temperature in celsius.

Table 6. Performance metrics of conventional circuit on FPGA.

Poly	Clk	Total	WNS	Utilization			Total	Dyn.	Stat.	Jn.
deg.	(ns)	Del.	(ns)	FF	LUT	IO	pow. (W)	pow. (W)	pow. (W)	tmp. (°C)
4	10	1.818	8.15	8	11	17	0.132	0.001	0.131	25.2
8	10	2.032	7.939	16	14	20	0.133	0.002	0.131	25.3
16	10	2.829	7.145	32	27	53	0.141	0.010	0.131	25.3
32	10	3.787	6.275	64	49	101	0.138	0.008	0.131	25.3
64	10	5.599	4.228	64	94	197	0.146	0.0015	0.131	25.3
128	10	8.522	1.736	256	183	389	0.16	0.029	0.131	25.5

Poly deg.: represents the degree of polynomial; Total Del.: represents the total delay; Total pow. (W): represents the total power dissipation in watt; Dyn. pow. (W): represents the dynamic power dissipation in watt; Stat. pow. (W): represents the static power dissipation in watts; Jn. tmp. (°C): represents the juntion temperature in celsius.

Table 7 provides a detailed comparison between the proposed and conventional LFSR-based pattern generators across various bit-widths. The proposed architecture demonstrates a consistent enhancement in throughput, particularly at higher bit-widths, achieving 19.1 bits/cycle at 128 bits compared to 15 bits/cycle in the conventional counterpart. While there is a moderate increase in power-delay product (PDP), this trade-off is offset by the improved data delivery rate and operating frequency. The area-delay product (ADP) is

higher for the proposed design due to additional control logic required for transition minimization. Nonetheless, the design exhibits favorable scalability and energy efficiency, indicating its suitability for low-power BIST applications where high-speed test pattern delivery is critical.

Table 7. Comparison of performance metrics.

Poly	Conventional LFSR				Proposed Circuit			
deg.	Fmax (MHz)	TP (Gbps)	PDP	ADP	Fmax (MHz)	TP (Gbps)	PDP	ADP
4	550.1	2.2	0.2	20	324.8	1.3	0.4	113.9
8	492.6	3.9	0.3	28.4	218.2	1.7	0.6	274.9
16	353.5	5.7	0.4	76.4	224.8	3.6	0.6	560.6
32	264.1	8.5	0.5	185.6	176.7	5.7	0.8	1505
64	178.6	11.4	0.8	526.3	177.8	11.4	0.8	2648.9
128	117.3	15	1.4	1559.5	149	19.1	1.4	4885.6

Poly deg.: represents the degree of polynomial

As the bit-width increases (particularly at 64 and 128 bits), the proposed design achieves competitive or in some cases superior maximum operating frequency compared to the conventional structure, demonstrating improved scalability, as illustrated in Figure 18. Moreover, the proposed approach consistently delivers higher throughput across all configurations, highlighting its efficiency in pattern generation, as shown in Figure 19. For instance, at 128 bits, the proposed design achieves a throughput of 19.1 compared to 15 in the conventional case, ensuring better data availability per clock cycle—an important factor for high-speed test applications. The Power Delay Product (PDP), which reflects energy efficiency (with lower values being preferable), is presented in Figure 20. Although the proposed design exhibits a slightly higher PDP across all bit-widths—primarily due to the additional logic for transition control—the increase remains modest (e.g., 0.6 vs. 0.5) and is justified by the significant improvements in throughput and scalability.

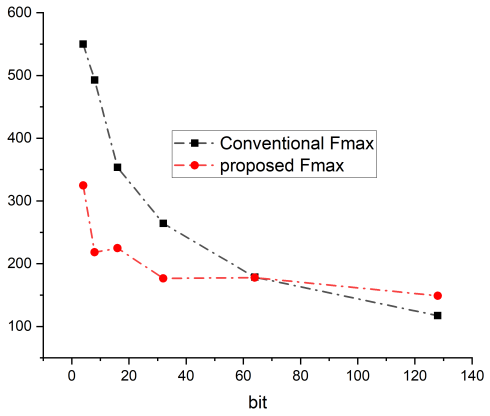

Figure 18. Maximum operating frequency comparison.

Additional randomness tests, such as those from the National Institute of Standards and Technology (NIST) [41], are conducted to evaluate randomization criteria, as shown in Table 8. Statistical benchmark tests are run on 128 bit-length with 8000 sequences created by the RP-PRPG and compared to a conventional LFSR with the same configuration. Table 7 shows that if a pseudorandom bit sequence's p-value surpasses the threshold in all tests, it is considered random. It covers the following tests: a random excursion test, frequency (monobit) test, approximate entropy test, non-overlapping template matching test, frequency test within a block, runs test, test for the longest run of several runs in a block, binary matrix rank test, overlapping template matching test, Maurer's "Universal Statistical"

test, linear complexity test, serial test, cumulative sums (Cusum) test, and random excursion variant test.

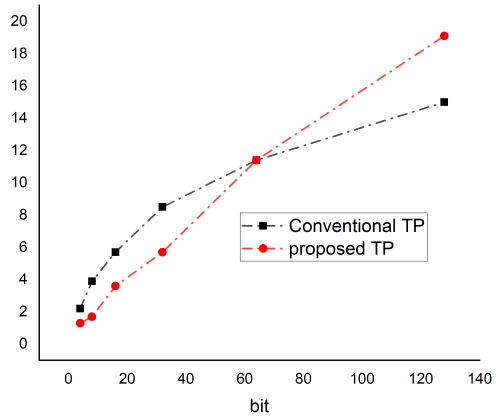

Figure 19. Throughput comparison.

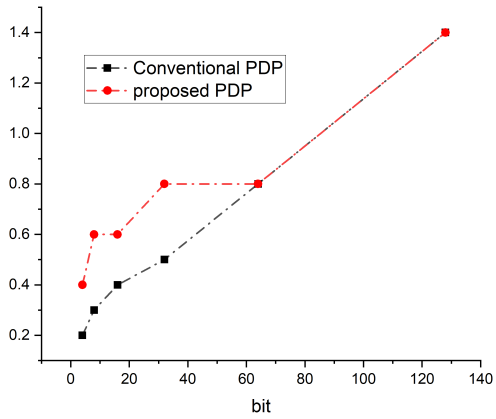

Figure 20. Power delay product comparison.

Table 8. NIST statistical tests comparison for conventional LFSR and RP-PRPG.

NIST Test	Conventional LFSR (*p*-Value)	RP-PRPG (*p*-Value)
Frequency (Monobit) Test	32.03%	10.94%
Frequency Test within a Block	81.25%	0
Runs Test	13.28%	1.56%
Test for the Longest Run of Ones in a Block	0	0
Binary Matrix Rank Test	99.22%	0
Non-overlapping Template Matching Test	75.78%	83.59%
Overlapping Template Matching Test	91.4%	100%
Maurer's "Universal Statistical" Test	0	100%
Linear Complexity Test	0.78%	97.66%
Serial Test	0	0
Approximate Entropy Test	0	0
Cumulative Sums (Cusum) Test	23.44%	10.94%
Random Excursions Test	-	-
Random Excursions Variant Test	-	-

The gathered sequences with a size of 1,024,000 bits passed these tests. To summarize, the proposed RP-PRPG has generally better statistical features compared to conventional LFSR. The overlapping template-matching test, Maurer's "Universal Statistical" test, and linear complexity test were successful and in other cases the *p*-values were higher than those observed for conventional LFSR. The overlapping template-matching test focuses on

the number of occurrences of pre-specified target strings. Maurer's "Universal Statistical" test aims to determine the number of bits between matching patterns (a measure related to the length of a compressed sequence). The test determines whether or not the sequence can be greatly compressed without losing information. A highly compressible sequence is deemed non-random. The linear complexity test focuses on the length of a linear feedback shift register (LFSR). The goal of this test is to see if the sequence is complicated enough to be deemed random. Random sequences have longer LFSRs. An LFSR that is too short indicates non-randomness. Pattern generators built for use in cryptographic applications may need to meet more stringent requirements than for different applications. In particular, their outputs must be unpredictable in the absence of knowledge regarding their inputs.

5. Comparison Investigation

Numerous researchers have explored low-power test pattern generation techniques, including gated clock techniques, adaptive power management, weighted random pattern generators, using control logic to decide the process of pattern generation based on power constraints, and the use of multiple polynomial, hybrid test patterns, pattern compression techniques, and low-transition methods. Our work focuses on reducing the power by managing the toggle count by adapting a structure similar to bipartite LFSR combined with a zero-forcing circuit. The proposed circuit is compared with those presented in other similar works [11,31,36,42] in which the authors attempted to reduce the power while maintaining the pseudorandomness. While these designs were selected for comparison based on our understanding, the findings apply to a broad range of low-power pattern generation approaches, not just those mentioned above.

Govindaraj et al. [11] explore the possibilities of reducing the power consumption in TPG which is designed using LFSR where a converter from binary to excess-4 as well as a binary ripple counter is used. Combinational circuits from ISCAS'85 and sequential circuits from ISCAS'89 were used to apply the patterns from the TPG and it was found by the authors that the switching activity between the successive patterns was minimal due to the high correlation between them, contributing to the overall minimization of power dissipation. The authors also explored the possibilities of performance by comparing the test lengths of the circuits. Paper [31] also explores the possibilities of increasing the correlation between successive patterns by reducing the switching activity and thus the power reduction. A programmable low-power LFSR has been realized which allows the user to select the seed value and can be parameterized for *n-bit* and various polynomials. Using 100 test patterns, the design was simulated for 4-, 8-, 16-, 32-, and 64-bit LFSRs with various polynomials. To compare the decrease in the transition count, this was carried out in addition to comparable simulations for standard LFSRs. Compared to traditional LFSRs, this method successfully decreased the quantity of output vector transitions by about 70%. A weighted TPG is proposed in [36], targeting the architecture of scan-based BIST. Weighted patterns are generated in order to enable/disable scan chains with a reduced area as well as power consumption. Maximum length of the weighted patterns are generated by making use of separate weights for a specific chain, which helps in achieving low power and reduced hardware overhead. Fewer transitions are used by these weighted patterns and the authors have experimented with 32-bit TPG. A low power pattern generator by leveraging linear feedback shift register (LFSR) using bit swapping is proposed in [42]. The circuit works by reducing number of transitions and a comparison with conventional LFSR shows that a reduction of 27.48% in dynamic power dissipation is achieved by the circuit. Table 9 summarizes the circuit configurability, maximum possible cycle length, switching activity, dynamic power, and hardware complexity. The configurability, maximum cycle duration, and concept of power reduction by managing switching activity are all considered to be

common parameters across all references. Additionally, all values are presented exactly as reported in the references, without any modifications from our side.

Table 9. Summary of prior works and proposed work.

Related Work	Configurability	Cycle Length	Switching Activity	Dyn. Pow.	Hardware Utilization
[11]	No	$2^m - 1$	49 toggles (32 test patterns)	0.54 mW for 4-bit	High
[30]	No	$2^m - 1$	70% reduction	Not discussed	Not discussed
[35]	No	$2^m - 1$	23.5% reduction	73 W for 16-bit	Low
[40]	No	$2^m - 1$	Reduced	10,224.310 nW	Not discussed
[42]	No	$2^m - 1$	Reduced	4.42 W	Not discussed
Prop.	Yes	$2^m - 1$	89 toggles (100 test vectors)	0.003 W	Moderate

Dyn. pow.: represents the dynamic power dissipation.

Several low-transition test pattern generators have been proposed to address the power challenges associated with Built-In Self-Test (BIST). One widely cited method is Dual-Speed LFSR (DS-LFSR), which uses two LFSRs operating at different clock speeds to reduce switching activity by controlling the correlation between consecutive patterns [43]. The Low-Transition Dual LFSR architecture improves on this by introducing AND/OR gates between dual LFSRs to suppress transitions at output lines. Similarly, the 2HS-PG (Half-Start–Half-Stop Pattern Generator) applies a novel toggling control mechanism to reduce transitions between adjacent test vectors [44]. The Low-Transition Generalized LFSR (LT-GLFSR) incorporates bipartite and bit-insertion strategies to achieve both average and peak power reduction during testing [45]. Moreover, test compression architectures using LFSR reseeding and optimized encoding have also been proposed to minimize the power usage while maintaining effective fault coverage. While these techniques reduce transitions effectively, they often involve additional control logic or complex encoding strategies. In contrast, our proposed method offers a simpler architecture with minimal overhead while still achieving significant power reduction, making it an attractive option for low-power BIST applications.

Recent efforts in low-power and secure pattern generation include a Model Predictive Control Pseudorandom Pattern Generator for Low-Power BIST [46], which anticipates scan outputs to reduce switching activity and power consumption, while maintaining fault coverage. Implemented on FPGA, it outperforms traditional PRPGs in terms of power and area. On the security front, the SQTRNG design [47] uses spintronic devices and quaternary logic to generate high-quality true random numbers with improved throughput and efficiency, making it suitable for cryptographic applications. These studies reflect growing trends toward energy-efficient and secure pattern generation architectures.

6. Conclusions and Future Work

The proposed low-power RP-PRPG was successfully designed, verified, and investigated using Xilinx Vivado, with a design that is parameterizable for N bits, several circuit structures, user-specified seeds, as well as polynomials. To evaluate and analyze the reduction in the transition count, the design was simulated and compared the design for 4, 8, 16, 32, 64, and 128 bits, as well as conventional LFSR configurations across a set of output sequences. By integrating two-stage LFSRs and a zero forcing circuit, the proposed methodology increases the correlation between consecutive patterns, resulting in fewer output transitions compared to traditional LFSR structures. The toggle count of RP-PRPG is compared to that of the typical LFSR and it is observed that the number of transitions dropped by more than 70%, which in turn led to a considerable decrease in power. The design has the ability to modify the configuration to Fibonacci or Galois and the circuit can generate a distinct set of patterns based on the same seed and polynomial. In future, the de-

sign can be used in concurrence with ATPG vector test compression to produce reseeding cubes after reviewing the characteristics of pattern generation for further pattern count reduction, thus further reducing the test power, test cost, and test time in the case of BIST applications. Also, the proposed design can be utilized to construct an efficient hardware architecture for implementing crypto processors using multi-LFSR structures leveraging parallel processing techniques while considering a balance between area and delay.

Author Contributions: Conceptualization, R.B. and G.R.S.; methodology, G.R.S.; software, U.H.R.; validation, G.R.S. and R.B.; formal analysis, U.H.R.; investigation, G.R.S.; resources, G.R.S.; data curation, G.R.S.; writing—original draft preparation, U.H.R.; writing—review and editing, G.R.S.; supervision, R.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Touba, N.A.; Mccluskey, E.J. Transformed Pseudo-Random Patterns for BIST. In Proceedings of the 13th IEEE VLSI Test Symposium, Princeton, NJ, USA, 30 April–3 May 1995; pp. 410–416.
2. Ying, J.C.; Tseng, W.D.; Tsai, W.J. Asymmetry dual-LFSR reseeding for low power BIST. *Integr. VLSI J.* **2017**, *60*, 272–276. [CrossRef]
3. Abraitis, V.; Tamoševičius, Ž. LSFR and BIST based Delay Test for ASIC and FPGA. *Elektron. Elektrotechnika* **2008**, *87*, 45–48.
4. Yu, C.; Reddy, S.M.; Pomeranz, I. Weighted pseudo-random BIST for N-detection of single stuck-at faults. In Proceedings of the Asian Test Symposium, Kenting, Taiwan, 15–17 November 2004; pp. 178–183. [CrossRef]
5. Pomeranz, I.; Parvathala, P.K.; Patil, S. Estimating the fault coverage of functional test sequences without fault simulation. In Proceedings of the 16th IEEE Asian Test Symposium, Beijing, China, 8–11 October 2007. [CrossRef]
6. Basturkmen, N.Z.; Reddy, S.M.; Pomeranz, I. A low power pseudo-random BIST technique. In Proceedings of the 8th IEEE International On-Line Testing Workshop, IOLTW, Isle of Bendor, France, 8–10 July 2002; pp. 140–144. [CrossRef]
7. Abdelhaleem, S.H.; Abd-El-Hafiz, S.K.; Radwan, A.G. Analysis and Guidelines for Different Designs of Pseudo Random Number Generators. *IEEE Access* **2024**, *12*, 115697–115715. [CrossRef]
8. Pomeranz, I. Storage and Counter Based Logic Built-In Self-Test. *IEEE Access* **2023**, *11*, 139335–139344. [CrossRef]
9. Agrawal, V.D.; Kime, C.R.; Saluja, K.K. A Tutorial on Built-ln Self-Test Part 1: Principles. *IEEE Des. Test Comput.* **1993**, *10*, 73–82. [CrossRef]
10. Agrawal, V.D.; Kime, C.R.; Saluja, K.K. Tutorial on built-in self-test. Part 2. Applications. *IEEE Des. Test Comput.* **1993**, *10*, 69–77. [CrossRef]
11. Govindaraj, V.; Dhanasekar, S.; Martinsagayam, K.; Pandey, D.; Pandey, B.K.; Nassa, V.K. Low-power test pattern generator using modified LFSR. *Aerosp. Syst.* **2023**, *7*, 67–74. [CrossRef]
12. Gergely, A.M.; Crainicu, B. A succinct survey on (Pseudo)-Random Number Generators from a Cryptographic Perspective. In Proceedings of the 5th International Symposium on Digital Forensic and Security, ISDFS, Tirgu Mures, Romania, 26–28 April 2017; pp. 1–6. [CrossRef]
13. Jin, Y. Design-for-Security vs. Design-for-Testability: A Case Study on DFT Chain in Cryptographic Circuits. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI, Tampa, FL, USA, 9–11 July 2014; pp. 19–24. [CrossRef]
14. Ramasamy, J.; Samiappan, D. A Modified PRBS: Vertical Stacked LFSR Primitive Polynomial for Secure Data Communication. *Procedia Comput. Sci.* **2022**, *215*, 947–954. [CrossRef]
15. Hwang, S.Y.; Park, G.Y.; Kim, D.H.; Jhan, K.S. Efficient implementation of a pseudorandom sequence generator for high-speed data communications. *ETRI J.* **2010**, *32*, 222–229. [CrossRef]
16. N.; i S.; Krishnaswamy, S.; Zolfaghari, B.; Mitra, P. Key-Dependent Feedback Configuration Matrix of Primitive σ-LFSR and Resistance to Some Known Plaintext Attacks. *IEEE Access* **2022**, *10*, 44840–44854. [CrossRef]
17. Ahmed, N.; Tehranipour, M.H.; Nourani, M. Low Power Pattern Generation for BIST Architecture. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Vancouver, BC, Canada, 23–26 May 2004. [CrossRef]

18. Kim, Y.; Yang, M.-H.; Lee, Y.; Kang, S. A New Low Power Test Pattern Generator using a Transition Monitoring Window based on BIST Architecture. In Proceedings of the Asian Test Symposium, Calcutta, India, 18–21 December 2005. [CrossRef]
19. Lee, J.; Touba, N.A. Low Power Test Data Compression Based on LFSR Reseeding. In Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD 2004), San Jose, CA, USA, 11–13 October 2004. [CrossRef]
20. Wen, X. VLSI Testing and Test power. In Proceedings of the International Green Computing Conference and Workshops, IGCC, Orlando, FL, USA, 25–28 July 2011. [CrossRef]
21. Girard, P. Survey of Low-Power Testing of VLSI Circuits. *IEEE Des. Test Comput.* **2002**, *19*, 82–92. [CrossRef]
22. Tehranipoor, M.; Nourani, M.; Ahmed, N. Low Transition LFSR for BIST-Based Applications. In Proceedings of the 14th Asian Test Symposium (ATS'05), Calcutta, India, 18–21 December 2005. [CrossRef]
23. Girard, P. Low power testing of VLSI circuits: Problems and solutions. In Proceedings of the Proceedings—International Symposium on Quality Electronic Design, ISQED, San Jose, CA, USA, 20–22 March 2000; pp. 173–179. [CrossRef]
24. Bosio, A.; Girard, P.; Virazel, A. Test of low power circuits: Issues and industrial practices. In Proceedings of the 2016 IEEE International Conference on Electronics, Circuits and Systems, ICECS, Monte Carlo, Monaco, 11–14 December 2016; pp. 524–527. [CrossRef]
25. Filipek, M.; Mrugalski, G.; Mukherjee, N.; Nadeau-Dostie, B.; Rajski, J.; Solecki, J.; Tyszer, J. Low-Power Programmable PRPG with Test Compression Capabilities. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2015**, *23*, 1063–1076. [CrossRef]
26. Aloisi, W.; Mita, R. Gated-Clock Design of Linear-Feedback Shift Registers. *IEEE Trans. Circuits Syst. II Express Briefs* **2008**, *55*, 546–550. [CrossRef]
27. Giustolisi, G.; Mita, R.; Palumbo, G.; Scotti, G. A Novel Clock Gating Approach for the Design of Low-Power Linear Feedback Shift Registers. *IEEE Access* **2022**, *10*, 99702–99708. [CrossRef]
28. Shaer, L.; Sakakini, T.; Kanj, R.; Chehab, A.; Kayssi, A. (2016, June 20). A low power reconfigurable LFSR. In Proceedings of the 18th Mediterranean Electrotechnical Conference: Intelligent and Efficient Technologies and Services for the Citizen, MELECON, Limassol, Cyprus, 18–20 April 2016. [CrossRef]
29. Xiang, D.; Wen, X.; Wang, L.T. Low-Power Scan-Based Built-In Self-Test Based on Weighted Pseudorandom Test Pattern Generation and Reseeding. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2017**, *25*, 942–953. [CrossRef]
30. Maragathaeswari, B.; Remadevi, G.; Bakthavatchalu, R. Design of a Programmable Low Power Linear Feedback Shift Register for BIST Applications. In Proceedings of the 6th IEEE International Test Conference India, ITC India, Anaheim, CA, USA, 23–30 September 2022; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2022. [CrossRef]
31. Dilip, P.S.; Somanathan, G.R.; Bhakthavatchalu, R. Gray code for test pattern generation. *AIP Conf. Proc.* **2020**, *2222*, 020008. [CrossRef]
32. Narasimha, P.; Krishna, M.V.; Somanathan, G.R.; Bhakthavatchalu, R. Design and analysis of gray code generator as test pattern generator. In Proceedings of the 6th International Conference on Communication and Electronics Systems, ICCES, Coimbatore, India, 8–10 July 2021; pp. 83–88. [CrossRef]
33. Ahmadunnisa, S.; Mathe, S.E. Multi-LFSR Architectures for BRLWE-Based Post Quantum Cryptography. *IEEE Access* **2024**, *12*, 96258–96272. [CrossRef]
34. Abdel-Hafeez, S. Programmable Feedback Shift Register. *Circuits Syst. Signal Process.* **2023**, *42*, 4784–4808. [CrossRef]
35. Vishnupriya, S.; Senthilpari, C.; Yusoff, Z. A Low-Power and Area-Efficient Design of a Weighted Pseudorandom Test-Pattern Generator for a Test-Per-Scan Built-in Self-Test Architecture. *IEEE Access* **2021**, *9*, 29366–29379. [CrossRef]
36. Charles E. Stroud, In *A Designer's Guide to Built-In Self-Test*; Kluwer Academic Publishers: Dordrecht, The Netherlands, 2007; Volume 136.
37. Wang, L.-T.; Wu, C.-W. *VLSI Test Principles and Architectures*; Morgan Kaufmann Publishers: San Fransisco, CA, USA, 2006.
38. Paar, C.; Pelzl, J. *Understanding Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010. [CrossRef]
39. Rueppel, R.A. *Analysis and Design of Stream Ciphers*; Springer: Berlin/Heidelberg, Germany, 1986; pp. 31–53
40. Hussain, S.; Priya, P.; Prof, A. Test Pattern Generator (TPG) for Low Power Logic Built In Self Test (BIST). *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.* **2013**, *2*, 2278–8875.
41. Bassham, L.; Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Leigh, S.; Levenson, M.; Vangel, M.; Heckert, N.; Banks, D. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; Special Publication (NIST SP); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
42. Singh, B.; Arun Khosla, S.B. Power Optimization of Linear Feedback Shift Register (LFSR) for Low Power BIST. In Proceedings of the IEEE International Advance Computing Conference (IACC 2009), Patiala, India, 6–7 March 2009.
43. Wang, S.; Gupta, S.K. DS-LFSR: A BIST TPG for low switching activity. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2002**, *21*, 842–851. [CrossRef]

44. Pandey, S.K.; Paramasivam, C. Design of Low Switching Pattern Generator for BIST Architecture. In *Micro-Electronics and Telecommunication Engineering*; Sharma, D.K., Peng, S.L., Sharma, R., Zaitsev, D.A., Eds.; ICMETE 2021. Lecture Notes in Networks and Systems; Springer: Singapore, 2022; Volume 373. [CrossRef]
45. Sakthivel, P.; Nirmal Kumar, A. Low Transition-Generalized Linear Feedback Shift Register Based Test Pattern Generator Architecture for Built-in-Self-Test. *J. Comput. Sci.* **2012**, *8*, 815–821.
46. Nilima, S.; Warade, T.R. Design of Model Predictive Control Pseudorandom Pattern Generator for Low Power BIST. *J. Eng. Sci. Technol.* **2022**, *17*, 207–224.
47. Amirany, A.; Mohebbi, L. SQTRNG: Spintronic Quaternary True Random Number Generator. *SPIN* **2022**, *15*, 207–224. [CrossRef]