RESEARCH PAPER

Low Power Parallel Architectures for LFSR Using State- Space Transformations

Umashankar Singh[1], Laxmi Kumre[2]
[1,2]Maulana Azad National Institute of Technology, Bhopal (M.P.)

***Corresponding Author**
Email: umashankar.singh25@gmail.com

Received: 1st february, 2026; **Revised:** 5th February, 2026; **Accepted:** 10th February, 2026; **Available Online:** 09th June, 2026

ABSTRACT

Linear feedback shift registers (LFSRs) employ parallel designs for Bose Chaudhuri Hocquenghem (BCH) encoders and cyclic redundancy checks (CRCs). The multi-bit serial and parallel LFSR design is presented in this study. Linear feedback shift registers with effective designs eliminate hold time violations and minimize the feedback loop. Our efficiency metric, the area-time product (A.T.), is defined as (C.P) (XOR + 1.5 D. E.), where 1.5 is the expected ratio of an XOR gate to a delay element in terms of the number of NAND gates. That's because an XOR gate requires four 2-input NAND gates, and a delay element requires six 2-input NAND gates. The better the implementation, the lower the A.T. value. The time product for normalized values in the bottom area indicates the preferred implementations. The building of 32-D flip-flops is necessary for a typical 32-bit LFSR. To achieve 32-bit LFSR capabilities with reduced size, power consumption, and clock route count, 4-bit flip-flops may be used. The Xilinx Vivado Tool examined the setup and hold violations for the 4-bit LFSR. Three timing violations with a slack of
0.269 ns are present for a 4-bit LFSR. Consequently, the experimental data shows that the total on-chip power is growing linearly. For CRC-32, 30% power and 6% gate count savings are achieved.

Index Terms—BCH encoders, linear feed-back shift register, state-space transform matrix, parallel architecture, CRC, low power, generator polynomial.

How to cite this article: Singh U, Kumre L. Low power parallel architectures for LFSR using state-space transformations. Int J Drug Deliv Technol. 2026;16(75s): 1759-1769. DOI: 10.25258/ijddt.16.75s.187

Source of support: Nil.

Conflict of interest: Nil

.

INTRODUCTION

Data transmission is done using a Bose Chaudhuri hocquenghem encoder and cyclic redundancy check. The work may be extended to measure the significance of the test patterns generated by the Test Pattern Generator. The feedback loop complexity of a parallel CRC transformation matrix and state-space transform is decreased by parallel designs for linear feedback shift registers (LFSRs). This concept achieves a considerable reduction in power consumption without raising CPD as compared to earlier designs [1]. Further research on the efficient parallel design of LFSR is required. Future research was done in a matrix using the state-space transformation approach. The Xilinx Vivado Tool was used to analyse the setup and hold violations for the 4-bit LFSR. For CRC-32, 30% power and 6% gate count savings are achieved. The superior implementations are shown by the time product for normalized values in the lower area. 32 D flip-flops are needed to design a typical 32-bitsLFSR. Reduced size, power, and clock route count are achieved 4-bits flip-flops to accomplish 32-bit LFSR capability [2],[3]. The same kind of transformations are thoroughly searched for in order to find the transformation that results in the fewest total gate counts [4]. In [5], triangular transformation matrices are used. In a different area of research, the LFSR function is understood as recursive filtering, and recursive filters are processed in parallel [6]. These parallel LFSRs are simpler to construct when the format of the recursive filter changes [7]. In comparison to the state-space transformation, it has more gates. The unfolding approach may also be used to derive parallel LFSRs from serial LFSRs. While their area is bigger. The viable clock frequency can be raised by modifying the divisor polynomial[10] or by including alternative look-ahead pipelining in the crucial loop [8]. We achieve our design by examining several transformations of state-space. My approach begins with the inverse transformation matrix and looks for a matrix that lowers the gate count of the pre-processing matrix multiplication [9]. As opposed to looking for a transformation matrix of a specific format that would reduce the total gate count. The recommended matrix [13],[14],[15] results in fewer nonzero entries in the feedback matrix. For systems employing substructure sharing, a reduced critical path delay (CPD) computation approach is also offered to better assess the logic complexity [16],[17]. The recommended design is based on how many logic gates are in use in the system using the unfolding technique. Although their size is larger, alternative look-ahead pipelining applied to the important loop [18] or divisor polynomial modification [19], can enhance the viable clock frequency. In those that rely on Pre-processing, feedback matrix multiplications and state space transform was require to one clock cycle.

I. PARALLEL LFSR ARCHITECTURES

The arrangement of the serial LFSR represented in figure 1 and given to the generator polynomial $g(x) = x^{n-k} + g_{n-k-1} x^{n-k-1} + \cdots + g_1 x + g_0$. To the division of $u(x)\ x^{n-k}$ by g (x) will

be performed by 4 bits LFSR. When the input with the greatest number of taps (u (x)) was added to [20],[21]. The only element that matters for CRC and BCH encoding is the remainder r(x) [22],[23],[24]. The most significant coefficient is entered initially between the coefficients of u(x), and r(x) is found in the registers after the final coefficient of u(x) to be submitted. The data flow through the register is managed by the clock signal. Each flip-flop's data is moved to the next flip-flop in the register when the clock signal is high. The data inhe first flip-flop moves to the second flip-flop, the data in the second flip-flop moves to the third flip-flop and so on, making the data to "shift" through the register.

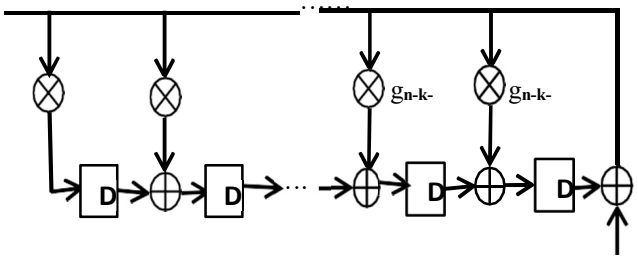
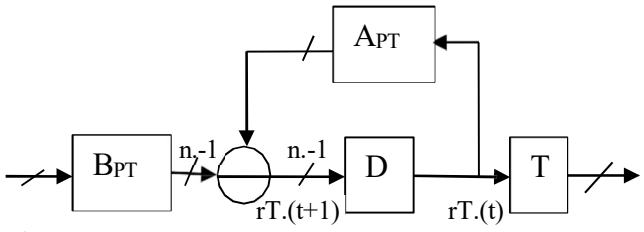


Figure 1: Architecture of serial LFSR. u(x)

It was suggested in [25], to change BpT and ApT, which are often known as the feedback and pre-processing matrices, to solve this issue. The values are as follows: up(t) = [u(t)... u(t+p-2), u(t+p-1)] and Bp = [Ap−1b…. Ab, b]. A p-parallel LFSR that modified p bits every clock cycle can be made using figure 2 displays a block schematic for building such a converted p-parallel LFSR. T has dimensions of (n − k) × (n − k), and as T increases, so does the complexity of the three matrix multiplications. From [26],[27] it turns out that the transformation also lowers the total gate count. In [3], a thorough search was conducted to identify the b1 that results in the least gate count. CMOS procedure A 1-XOR-gate that is exceptionally short [28]. becomes superfluous when 5 or 6 XOR gates fit inside a 1 ns delay an LFSR sequence can have a maximum the state vector as r(t) = T x rT (t) where, T is non-singular and is referred to as the transformation matrix. where,

$A_{PT} = T^{-1} \times A^{P} \times T$ $B_{PT} = T^{-1} \times B_P$



greatest number of bit patterns are produced by an LFSR and its maximal length is equal to 2^n-1 clock cycle.

$$g_0 \quad \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$$

$$A = \begin{matrix} g_{n-k-1} \\ g_{n-k-2} \\ \vdots \\ g_1 \\ g_0 \end{matrix} \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & 0 \end{bmatrix}$$

COMPARISONS OF PARALLEL LFSRS

An almost complete collection of patterns and 2^n-1 clock cycle states may be achieved by an LFSR with suitable design. In this architecture, more intricate logic involving data inputs and register feedbacks generates the register inputs. To reduce the length of the data channel, a pipelining stage of width p is added. Therefore, in comparison to our approach, it requires p more delay elements (DEs). To the normalized area-time product (ATP), computed as (1.5 DE + XOR) CPD [1], is used to assess the efficiency of designs with various CPDs. In [7]'s architectural design, in a clock cycle, nearly all logic gates are active.

TABLE I COMPARISON OF PARALLEL LFSRS

Z	DESIGN	XOR	DE	CPD	ATP
CRC-12	[3]	113	35	5	827
	[7]	109	36	5	815
	[1]	103	24	4	695
	Proposed	101	22	4	536
CRC-16	[3]	187	48	5	1295
	[7]	113	50	5	940
	[1]	94	32	5	710
	Proposed	92	30	5	685
SDLC	[3]	207	48	5	1395
	[7]	139	50	5	1070
	[1]	97	32	3	435
	Proposed	95	31	3	425
CRC-16 Reverse	[3]	219	46	5	1440
	[7]	126	50	5	1005
	[1]	82	32	4	520
	Proposed	80	30	4	500
SDLC Reverse	[3]	217	48	5	1445
	[7]	127	50	5	1010
	[1]	90	32	4	552
	Proposed	85	31	4	526
CRC-32	[3]	968	96	5	5560
	[7]	794	96	5	4690
	[1]	675	64	5	3855
	Proposed	625	56	5	3545

n.-1

P n.-1

Figure 2: Architecture of parallel LFSR.

While the search is running, then remaining columns or rows are obtained via shifting modulo reduction. Rather, the objective is to reduce the weight of each row in BPT. When using SS [1], a matrix multiplication can be finished with fewer XOR gates, indicating that shared intermediate results for multiple outputs are calculated just once. Cycle 't' by r.(t) = [r.n−k−1(t), r.n−k−2(t) r.0(t)]. Let u.(t) be the input of clock cycle 't'. Then r. (t + 1) = A × r.(t) + b × u.(t) where, 'A' is companion matrix. The results of our comparison for the starting XOR gate count found. The suggested approach is contrasted with earlier ones and the outcome for various generating polynomials. The LFSR feedback function is usually represented by a characteristic polynomial. The

The number of XOR gates required to finish an operation may be calculated for an implementation by counting all of the 1s in the rows of the coupling matrices, deducting 1 from each row subtotal, and then computing the overall number of XOR gates. The input size is equal to the generator polynomial degree, r = n, in order to do an exhaustive search and reduce the hardware complexity of parallel retimed CRC computation systems. For n-bits CRC system's state space matrix was created in order to simplify the feedback loop. The suggested approach is contrasted with earlier ones and the outcome for various generating polynomials. where the number of delay elements is represented by DE. The findings show that my parallel architectures can produce hardware designs with the same CPD and the smallest XOR gates. To improve the data's interpretive qualities, the relative area time product values are listed using the suggested technique of normalization, in the rightmost column indicated by parenthesis. Throughout the experiment, we find that one object draws our attention. Our design can always obtain the best AT for various generator polynomials.

ute count. The setup and hold violations for the 4-bit LFSR investigated using the xilinx vivado tool. Timing violations: for a 4-bit LFSR, there are three with a slack of 0.230 ns. We calculated the static and dynamic power of 4bits, 8bits, 12bits, 16bits and 32bits LFSR using vivado tool. The transformation matrix is built using a parallel LFSR. As an efficiency metric, we define the area-time product (A.T.) as (C.P) (XOR + 1.5 D.E.), where 1.5 is the expected quantity of NAND gates that separate an XOR gate from a delay element. This is based on the notion that a delay element needs 6 2-input NAND gates, and an XOR gate needs 4 2-input NAND gates. For an LFSR generator with 32 bits of length and 16 steps at a time, implementation is preferable when the area time product of the price be less. We calculated the static and dynamic power of 4bits, 8bits, 12bits, 16bits and 32bits LFSR using vivado tool.

TABLE III
COMPARISON OF SERIAL LFSR

No. of Bits	Junction Temperature (ºC)	Effective thermal resistance (ºC/W)	Static power (w)	Dynamic power (w)	Total power (w)
4	33.6	2.5	0.091	1.444	1.535
5	33.6	2.5	0.091	1.761	1.852
8	33.6	2.5	0.091	2.712	2.803
12	33.6	2.5	0.091	3.906	3.997
16	33.6	2.5	0.091	5.267	5.358
32	33.6	2.5	0.091	10.545	10.636

TABLE II GENERATOR POLYNOMIALS

CODE	POLYNOMIALS
CRC-12	$x^{12}+x^{11}+x^3+x^2+x+1$
CRC-16	$x^{16}+x^{15}+x^2+1$
SDLC	$x^{16}+x^{12}+x^5+1$
CRC-16 Reverse	$x^{16}+x^{14}+x+1$
SDLC Reverse	$x^{16}+x^{11}+x^4+1$
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+$ x^4+x^2+x+1

Each generator polynomial's degree is taken into the parallelism level p. One acceptable matrix to show the efficiency of the area-time product (ATP) is given below.

ATP = (1.5 DE + XOR) CPD

Generator polynomials of CRC-16 reverse, this study [1] uses a greater total number of XOR gates than the findings in [7], but the CPD essentially stays the same. The overall no. of XOR gates use in CRC-32 is less in this study [1] than in the findings in [7], but the CPD essentially stays the same.

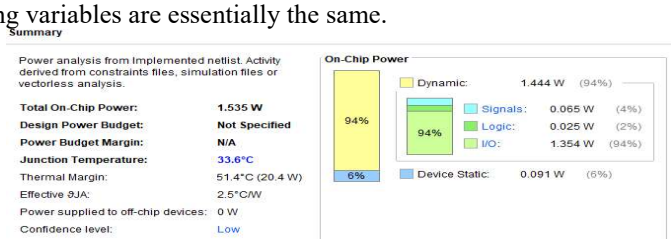
III. EXPERIMENTAL ANALYSIS

According to experimental data, the suggested architecture outperforms the recent architecture by as much as 55%. For an LFSR generator with 32 bits of length and 16 steps at a time, implementation is preferable when the area time product of the price be less. Schematic circuit diagram of 4 bits parallel LFSR as shown in figure 3, and RTL analysis shown in figure 4. The implementation is better when the A.T. value is lower. An ordinary 32-bit LFSR requires the construction of 32 D flip-flops. By using 4-bit flip-flops, 32-bit LFSR capabilities may be accomplished with less area, power consumption, and clock

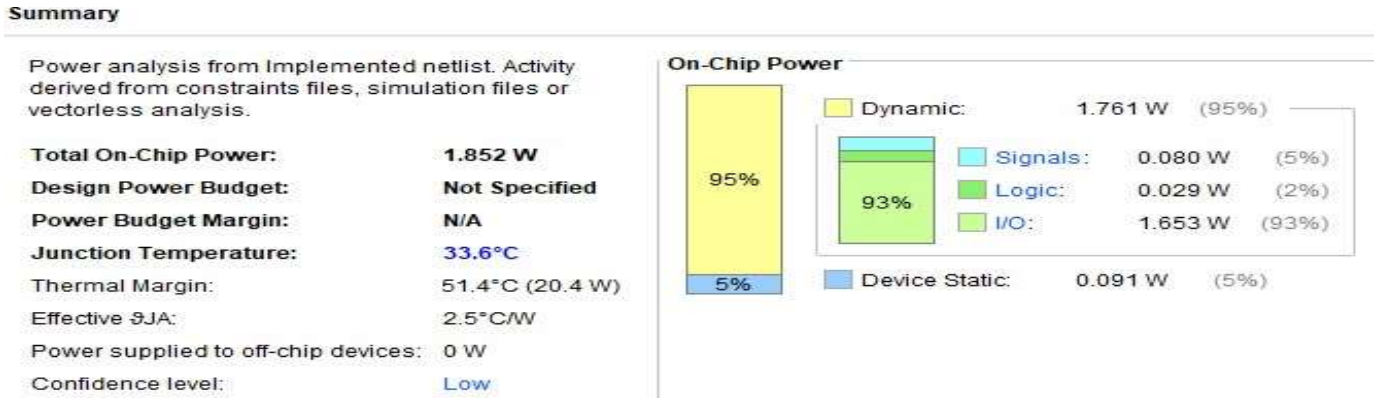
BLE IV
COMPARISON OF PARALLEL LFSR

No. of Bits	Junction Temperature (ºC)	Effective thermal resistance (ºC/W)	Static power (w)	Dynamic power (w)	Total power (w)
4	33.6	2.5	0.091	3.902	3.993
5	33.6	2.5	0.091	3.812	3.903
8	33.6	2.5	0.091	7.111	7.202
12	33.6	2.5	0.091	12.133	12.224
16	33.6	2.5	0.091	12.620	12.711
32	33.6	2.5	0.091	28.165	28.256

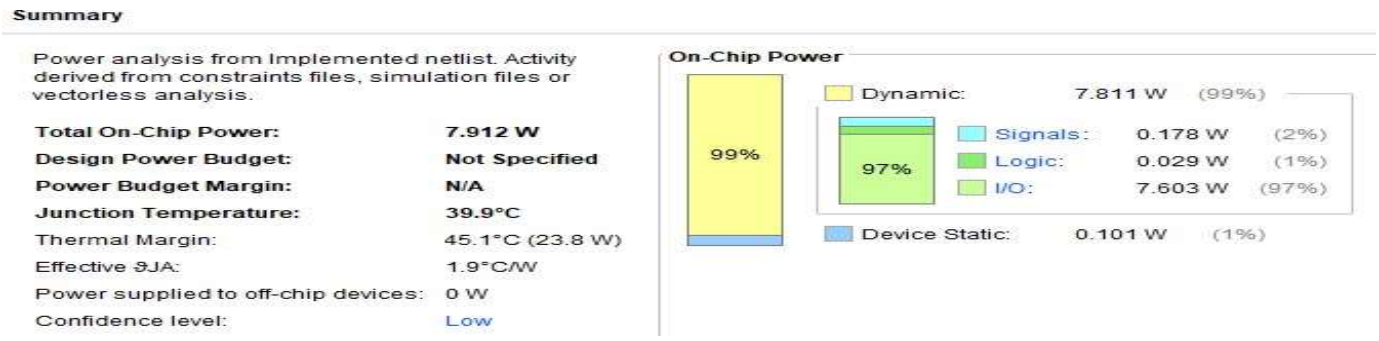
. Thus, based on the findings from the experiment, the overall within-chip power appears to be growing sequentially with a variance of 3.99W. The variations are attributed to the worst hold and negative slack. Parallel designs for linear feedback shift registers reducing the feedback loop complexity of a parallel CRC transformation matrix and state-space transform. Comparing this design to previous designs, a significant reduced the power consumption is achieved without increasing in CPD. The input size is equal to the generator polynomial degree, r = n, in order to do an exhaustive search and reduce the hardware complexity of parallel retimed CRC computation systems. The remaining variables are essentially the same.



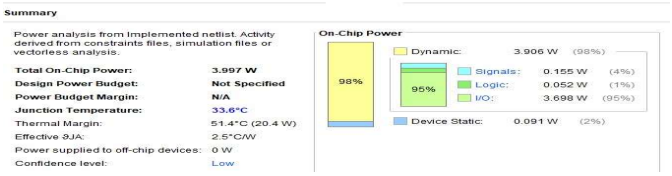
(a)



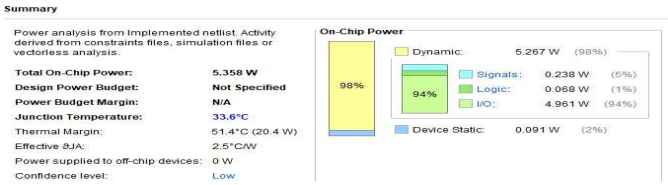
(b)



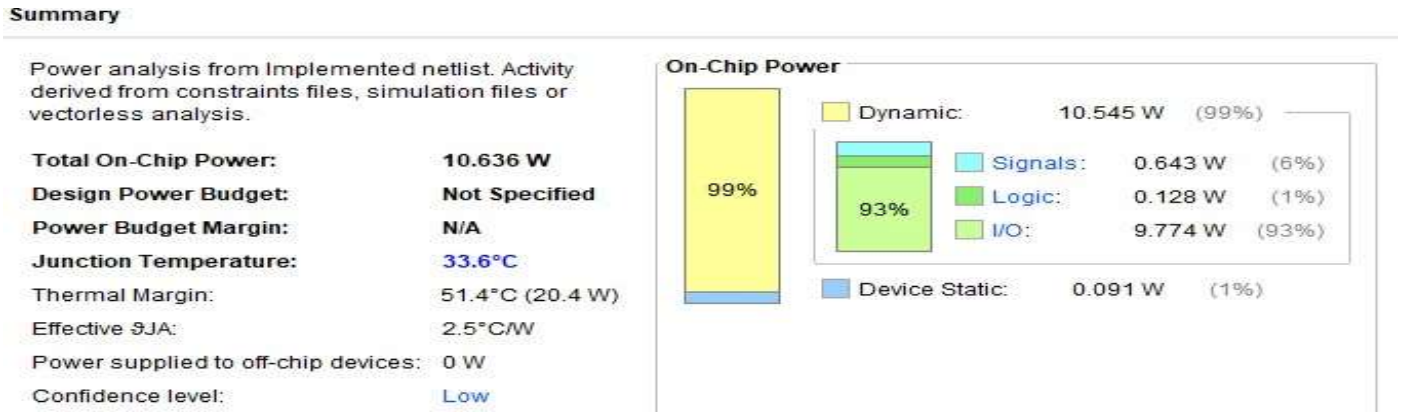
(c)



(d)

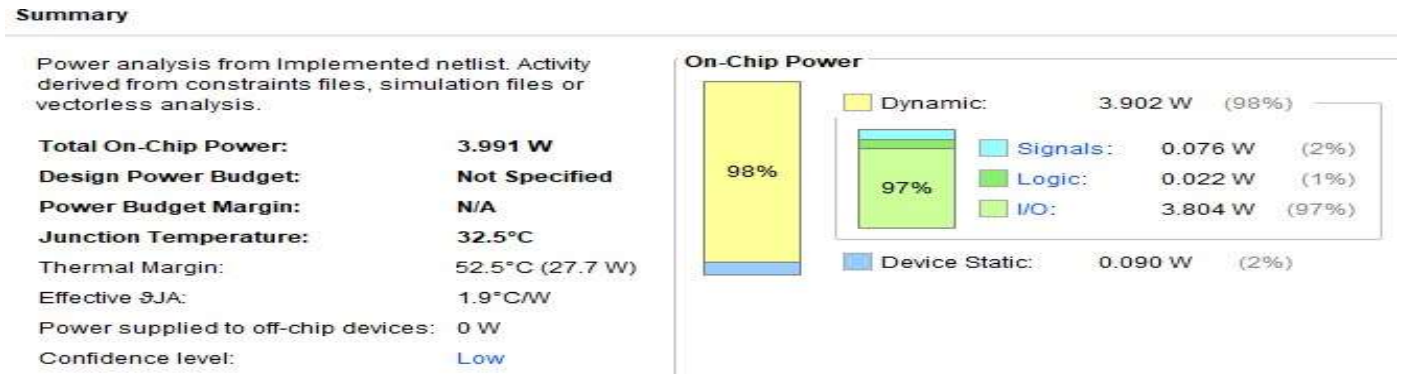


(e)



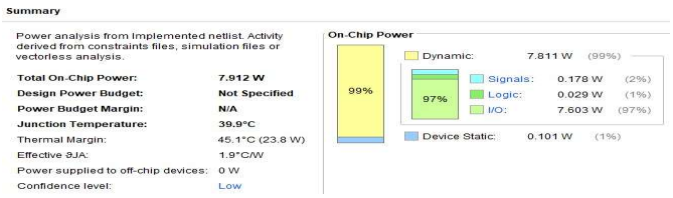
(f)

Figure 3: Power analysis of serial LFSR: (a) 4 bits (b) 5 bits (c) 8 bits (d) 12 bits (e) 16 bits (f) 32 bits.

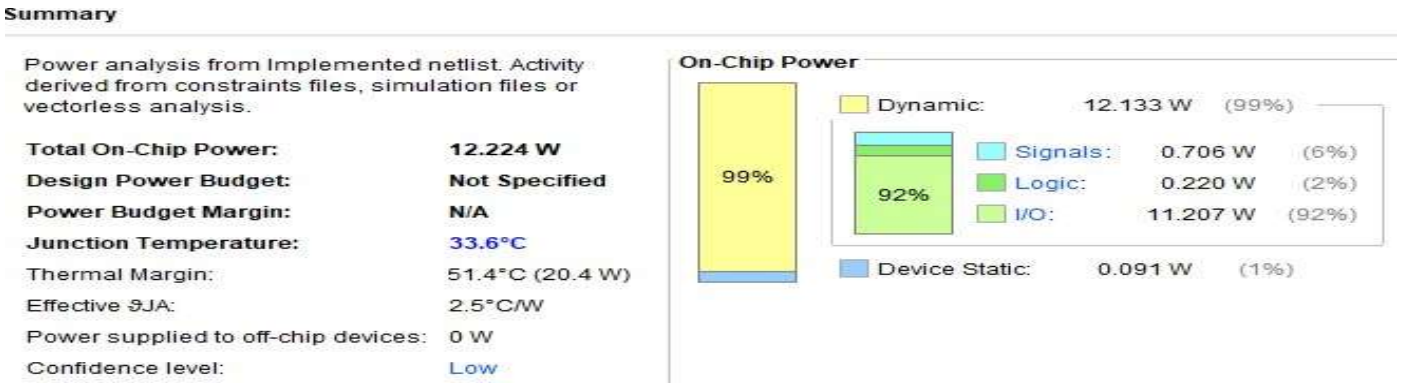


(a)

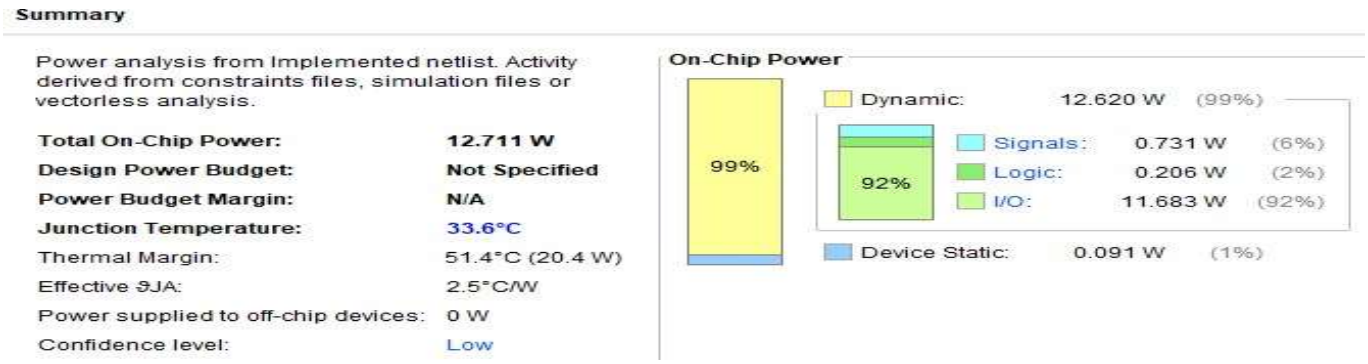
(b)



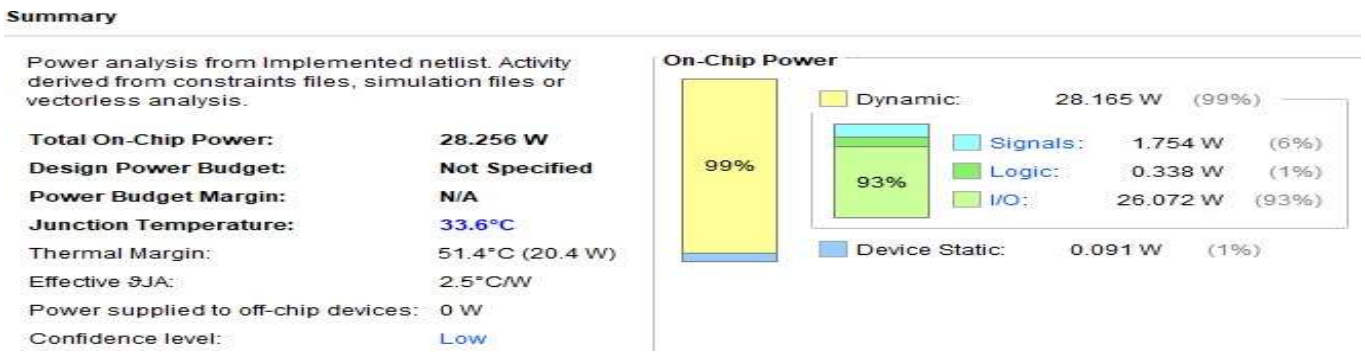
(c)



(d)



(e)



(f)

Figure 4: Power analysis of parallel LFSR: (a) 4 bits (b) 5 bits (c) 8 bits (d) 12 bits (e) 16 bits (f) 32 bits

IV. CONCLUSION

This paper presents the design of a multi-bit parallel and serial LFSR. Thus, based on the findings from the experiment, the overall within-chip power appears to be growing sequentially with a variance of 3.99W. The variations are attributed to the worst hold and negative slack. Parallel designs for linear feedback shift registers reducing the feedback loop complexity of a parallel CRC transformation matrix and state-space transform. Comparing this design to previous designs, a significant reduced the power consumption is achieved without increasing in CPD. The remaining variables are essentially the same. For n-bits CRC system's state space matrix was created in order to simplify the feedback loop. For CRC-32, 30% power and 6% gate count savings are achieved. Reduced size, power, and clock route count are achieved 4-bits flip-flops to accomplish 32-bit LFSR capability. With the help of the Xilinx Vivado Tool, violations for the 4-bits LFSR were examined.

REFERENCES

[1] H. Choi, G. Kim, H. -Y. Song and H. Noh, "Chaotic Nature of Integer Sequences From Primitive Linear Feedback Shift Registers," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 72, no. 9, pp. 1268-1272, Sept. 2025, doi: 10.1109/TCSII.2025.3585913.

[2] X. Zhang and Y. J. Tang, "Low-Complexity Parallel Cyclic Redundancy Check," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401679.

[3] G. Giustolisi, R. Mita, G. Palumbo and G. Scotti, "A Novel Clock Gating Approach for the Design of Low-Power Linear Feedback Shift Registers," in IEEE Access, vol. 10, pp. 99702-99708, 2022, doi: 10.1109/ACCESS.2022.3207151.

[4] P. -H. Tseng, M. -H. Lee, Y. -H. Lin, H. -L. Lung, K. -C. Wang and C.
-Y. Lu, "ReRAM-Based Pseudo-True Random Number Generator With High Throughput and Unpredictability Characteristics," in IEEE Transactions on Electron Devices, vol. 68, no. 4, pp. 1593-1597, April 2021, doi: 10.1109/TED.2021.3057028.

[5] S. Li, B. Weng, L. Chen, Y. Gao, L. Ying and J. Ren, "Test Performance Analysis of Rapid Single Flux Quantum Circuits With Auxiliary Circuits," in IEEE Transactions on Applied Superconductivity, vol. 34, no. 4, pp. 1-5, June 2024, Art no. 1300905, doi: 10.1109/TASC.2024.3370391.

[6] H. -B. Yu and Q. -X. Zheng, "Predicting Truncated Galois Linear Feedback Shift Registers," in IEEE Transactions on Information Theory, vol. 70, no. 12, pp. 9179-9194, Dec. 2024, doi: 10.1109/TIT.2024.3442870.

[7] I. Pomeranz, "Extra Clocking of LFSR Seeds for Improved Path Delay Fault Coverage," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 544-552, Feb. 2020, doi: 10.1109/TVLSI.2019.2947340.

[8] I. Pomeranz, "Padding of LFSR Seeds for Reduced Input Test Data Volume," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 5, pp. 1004-1008, May 2021, doi: 10.1109/TCAD.2020.3011665.

[9] M. Li and D. Lin, "The Adjacency Graphs of FSRs With Affine Characteristic Functions," in IEEE Transactions on Information Theory, vol. 68, no. 1, pp. 649-658, Jan. 2022, doi: 10.1109/TIT.2021.3120841.

[10] Y. Li and T. Cui, "Linear Forgery Attacks on the Authenticated Encryption Cipher ACORN-Like," in Chinese Journal of Electronics, vol. 34, no. 1, pp. 257-265, January 2025, doi: 10.23919/cje.2023.00.016.

[11] Y. Wu, "High-Speed LFSR Decoder Architectures for BCH and GII Codes," in IEEE Journal on Selected Areas in Information Theory, vol. 4, pp. 331-350, 2023, doi: 10.1109/JSAIT.2023.3304235.C. Cheng and K. K. Parhi, "High speed VLSI architecture for general linear feedback shift register (LFSR) structures," *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2009, pp. 713-717, doi: 10.1109/ACSSC.2009.5469943.

[12] J. Rajski, M. Trawka, J. Tyszer and B. Włodarczak, "A Nonlinear Stream Cipher for Encryption of Test Patterns in Streaming Scan Networks," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 535-547, Feb. 2025, doi: 10.1109/TCSI.2024.3447080.

[13] X. Wen et al., "A Linear Recurrence-Based Pseudorandom Number Generator Optimized for Detector Emulators," in IEEE Transactions on Nuclear Science, vol. 70, no. 8, pp. 2139-2147, Aug. 2023, doi: 10.1109/TNS.2023.3285251.

[14] H. Bae et al., "High-Speed Counter With Novel LFSR State Extension," in IEEE Transactions on Computers, vol. 72, no. 3, pp. 893-899, 1 March
2023, doi: 10.1109/TC.2022.3187343.

[15] K. Mandal, B. Yang, G. Gong and M. Aagaard, "Analysis and Efficient Implementations of a Class of Composited de Bruijn Sequences," in IEEE Transactions on Computers, vol. 69, no. 12, pp. 1835-1848, 1 Dec.
2020, doi: 10.1109/TC.2020.2979460.

[16] M. Sasmal, T. Joseph and B. T. S., "Approximate Multiplier Design With LFSR-Based Stochastic Sequence Generators for Edge AI," in IEEE Computer Architecture Letters, vol. 23, no. 1, pp. 91-94, Jan.-June 2024, doi: 10.1109/LCA.2024.3379002.

[17] M. Li and D. Lin, "Partial Cycle Structure of FSRs and Its Applications in Searching De Bruijn Sequences," in IEEE Transactions on Information Theory, vol. 69, no. 1, pp. 598-609, Jan. 2023, doi: 10.1109/TIT.2022.3201519.

[18] F. Karimzadeh, N. Cao, B. Crafton, J. Romberg and A. Raychowdhury, "A Hardware-Friendly Approach Towards Sparse Neural Networks Based on LFSR-Generated Pseudo-Random Sequences," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 2,
pp. 751-764, Feb. 2021, doi: 10.1109/TCSI.2020.3037028.

[19] D. Kim, J. Song and D. Yoon, "On the Estimation of Synchronous Scramblers in Direct Sequence Spread Spectrum Systems," in IEEE Access, vol. 8, pp. 166450-166459, 2020, doi: 10.1109/ACCESS.2020.3023425.

[20] I. Pomeranz, "Direct Computation of LFSR-Based Stored Tests for Broadside and Skewed-Load Tests," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 12, pp. 5238-5246, Dec. 2020, doi: 10.1109/TCAD.2020.2966452.

[21] I. Pomeranz, "Storage-Based Logic Built-In Self-Test With Partitioned Deterministic Compressed Tests," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 31, no. 9, pp. 1259-1268, Sept. 2023, doi: 10.1109/TVLSI.2023.3285691.

[22] A. Ahmed, N. M. Khan, S. K. Haider, M. I. Daud, A. U. Rehman and E.
T. Eldin, "Linear Gain Controller Aided Iterative Soft Sequential Acquisition for Primitive Polynomials," in IEEE Access, vol. 11, pp. 67411-67433, 2023, doi: 10.1109/ACCESS.2023.3291685.

[23] I. Pomeranz, "Storage-Based Logic Built-in Self-Test With Multicycle Tests," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 10, pp. 3553-3557, Oct. 2022, doi: 10.1109/TCAD.2021.3128446.

[24] Y. Xiong, N. J. Pieper, B. Narasimham, D. R. Ball and B. L. Bhuva, "Efficacy of Spatial and Temporal RHBD Techniques at Advanced Bulk FinFET Technology Nodes," in IEEE Transactions on Nuclear Science, vol. 70, no. 8, pp. 1814-1820, Aug. 2023, doi: 10.1109/TNS.2023.3246067.

[25] Y. Kong, H. Liu, V. Garg and S. Yu, "A 28-nm Digital Compute-in-Memory Ising Annealer With Asynchronous Random Number Generator for Traveling Salesman Problem," in IEEE Solid-State Circuits Letters, vol. 9, pp. 1-4, 2026, doi: 10.1109/LSSC.2025.3639178.

[26] S. Ma and J. Guan, "Improved Key Recovery Attacks on Simplified Version of K2 Stream Cipher," in The Computer Journal, vol. 64, no. 8,
pp. 1253-1263, Oct. 2020, doi: 10.1093/comjnl/bxaa154.

[27] A. Kumar Panda and K. Chandra Ray, "A Coupled Variable Input LCG Method and its VLSI Architecture for Pseudorandom Bit Generation," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 4, pp. 1011-1019, April 2020, doi: 10.1109/TIM.2019.2909248.A. Mamun and R. Katti, "A new parallel architecture for low power linear feedback shift registers," *2004 IEEE International Symposium on Circuits and Systems (ISCAS)*, Vancouver, BC, Canada, 2004, pp. II-333, doi: 10.1109/ISCAS.2004.1329276.

[28] A. Salib, M. F. Flanagan and B. Cardiff, "Time-Skew Estimation for Random Sampling Sequence Time-Interleaved ADCs," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 10,
pp. 1809-1813, Oct. 2020, doi: 10.1109/TCSII.2019.2956101.

[29] Y. Wang et al., "A Lightweight Authentication Protocol Against Modeling Attacks Based on a Novel LFSR-APUF," in IEEE Internet of Things Journal, vol. 11, no. 1, pp. 283-295, 1 Jan.1, 2024, doi: 10.1109/JIOT.2023.3314058.

[30] N. Petra, D. De Caro and A. G. M. Strollo, "A Novel Architecture for Galois Fields GF(2^m) Multipliers Based on Mastrovito Scheme," in *IEEE Transactions on Computers*, vol. 56, no. 11, pp. 1470-1483, Nov. 2007, doi: 10.1109/TC.2007.70741.

[31] S. H. AbdELHaleem, S. K. Abd-El-Hafiz and A. G. Radwan, "Analysis and Guidelines for Different Designs of Pseudo Random Number Generators," in IEEE Access, vol. 12, pp. 115697-115715, 2024, doi: 10.1109/ACCESS.2024.3445277.

[32] Z. Xie, Y. J. Tang and X. Zhang, "Low-Latency Nested Decoding for Short Generalized Integrated Interleaved BCH Codes," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 10, pp. 1563-1567, Oct. 2022, doi: 10.1109/TVLSI.2022.3179944.

[33] H. Chen, "CRT-Based High-Speed Parallel Architecture for Long BCH Encoding," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 56, no. 8, pp. 684-686, Aug. 2009, doi: 10.1109/TCSII.2009.2024247.

[34] H. Yoo, J. Jung, J. Jo and I. -C. Park, "Area-Efficient Multimode Encoding Architecture for Long BCH Codes," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 12, pp. 872-876, Dec. 2013, doi: 10.1109/TCSII.2013.2281941.

[35] M. Sprachmann, "Automatic generation of parallel CRC circuits," in *IEEE Design & Test of Computers*, vol. 18, no. 3, pp. 108-114, May-June 2001, doi: 10.1109/54.922807.

[36] Xinmiao Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 957-967, Sept. 2004, doi: 10.1109/TVLSI.2004.832943.

[37] J. L. Imaña, "LFSR-Based Bit-Serial GF(2^m) G F (2^ m) Multipliers Using Irreducible Trinomials," in *IEEE Transactions on Computers*, vol. 70, no. 1, pp. 156-162, 1 Jan. 2021, doi: 10.1109/TC.2020.2980259.

[38] J. Jung, H. Yoo, Y. Lee and I. -C. Park, "Efficient Parallel Architecture for Linear Feedback Shift Registers," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 11, pp. 1068-1072, Nov. 2015, doi: 10.1109/TCSII.2015.2456294.D. Xiang, X. Wen and L. -T. Wang, "Low-Power Scan-Based Built-In Self-Test Based on Weighted Pseudorandom Test Pattern Generation and Reseeding," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 942-953, March 2017, doi: 10.1109/TVLSI.2016.2606248.

[39] N. Petra, D. De Caro and A. G. M. Strollo, "A Novel Architecture for Galois Fields GF(2^m) Multipliers Based on Mastrovito Scheme," in *IEEE Transactions on Computers*, vol. 56, no. 11, pp. 1470-1483, Nov. 2007, doi: 10.1109/TC.2007.70741.

[40] H. Chen, "CRT-Based High-Speed Parallel

Architecture for Long BCH Encoding," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 56, no. 8, pp. 684-686, Aug. 2009, doi: 10.1109/TCSII.2009.2024247.

[41] H. Yoo, J. Jung, J. Jo and I. -C. Park, "Area-Efficient Multimode Encoding Architecture for Long BCH Codes," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 12, pp. 872-876, Dec. 2013, doi: 10.1109/TCSII.2013.2281941.

[42] M. Sprachmann, "Automatic generation of parallel CRC circuits," in *IEEE Design & Test of Computers*, vol. 18, no. 3, pp. 108-114, May-June 2001, doi: 10.1109/54.922807.

[43] Xinmiao Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 957-967, Sept. 2004, doi: 10.1109/TVLSI.2004.832943.

[44] J. L. Imaña, "LFSR-Based Bit-Serial GF(2^m) G F (2^ m) Multipliers Using Irreducible Trinomials," in *IEEE Transactions on Computers*, vol. 70, no. 1, pp. 156-162, 1 Jan. 2021, doi: 10.1109/TC.2020.2980259.

[45] J. Jung, H. Yoo, Y. Lee and I. -C. Park, "Efficient Parallel Architecture for Linear Feedback Shift Registers," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 11, pp. 1068-1072, Nov. 2015, doi: 10.1109/TCSII.2015.2456294.

[46] D. Xiang, X. Wen and L. -T. Wang, "Low-Power Scan-Based Built-In Self-Test Based on Weighted Pseudorandom Test Pattern Generation and Reseeding," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 942-953, March 2017, doi: 10.1109/TVLSI.2016.2606248.

[47] Jing-Shiun Lin, Chung-Kung Lee, Ming-Der Shieh and Jun-Hong Chen, "High-speed CRC design for 10 Gbps applications," *2006 IEEE International Symposium on Circuits and Systems (ISCAS)*, Kos, Greece, 2006, pp. 4 pp.-, doi: 10.1109/ISCAS.2006.1693300.

[48] C. Kennedy and A. Reyhani-Masoleh, "High-speed parallel CRC circuits," *2008 42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2008, pp. 1823-1829, doi: 10.1109/ACSSC.2008.5074742.