ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Volume 10 Issue 5 May 2024

Secure 16-bit Low Power Linear Feedback Shift Register for Advance Communication System at 90nm Technology

[1] Ahmad Raza, [2] Dr. Mahesh Kumar Singh, [3] Abhishek Upadhyay

[1][2][3] Dept. of Electronics and Comm. Engineering, National Institute of Technology Delhi, India
Email: [1] 222220011@nitdelhi.ac.in, [2] ksmahesh@nitdelhi.ac.in, [3] abhishekupadhyay@gmail.com

Abstract*— To move a data word's bit position to the left or right, utilize a shift register. The brief proposes XOR gate, NOT gate as feedback latch based linear shift register. This paper presents a high secure linear feedback shift register, which can perform both serial and parallel operations. They reduce the power consumption and delay by replacing gate as feedback with the proposes based latch. The proposes 16-bit linear feedback shift register were simulated using 90nm CMOS process. A linear feedback shift register (LFSR) has been studied in this paper XOR gate and NOT gate use as feedback for enhancement of security purpose. They consume power 94.59% and 95.16% and reduce delay 86.72% and 27.40% with Vdd= 1.8V and a clock frequency of 100MHz.

***Index Terms*— Low Area, Low Power, Shift Register, Short Delay, Power Delay Product (PDP), XOR Feedback**

I. INTRODUCTION

Linear Feedback Shift Registers (LFSR) are crucial components in many applications, particularly in the field of digital signal processing, cryptography [1], error detection and correction, and more. Here are some of the key advantages of using a Linear Feedback Shift Register:

Efficient Pseudo random Sequence Generation: LFSR are adept at generating pseudo random sequences with relatively simple hardware [2]. These sequences have statistical properties that resemble truly random sequences, making them useful in encryption algorithms and simulations [3].

Fast Operation: They can perform their operations (shift and feedback) very quickly, which is advantageous in applications where high-speed processing [4-6] is necessary, such as in communication systems.

Error Detection and Correction: LFSRs are employed in various error detection and correction techniques [7-9], such as Cyclic Redundancy Checks (CRCs). They can efficiently identify errors in data transmission and provide a means to correct them.

Shift Register Counters: LFSRs can be configured to operate as counters. This is useful in applications requiring counting or sequencing operations.

Fig. 1 shows schematic unidirectional pulse-latch circuit 1-bit binary-code shift-register consisting of D latch [10-12]. The unidirectional contain one latch including reset signal and one pass transistor. They have consisted of 10 transistors.

Fig. 2 demonstrates the unidirectional pulse latch's operation waveform. The unidirectional pulse-latch (Q and Qb) takes different data input (D and Db) when the clock signal (CL-pulse) is high.

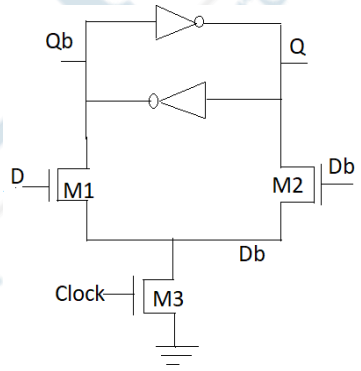

Fig. 1. Conventional Unidirectional Pulse-latch Circuit [18]

The unidirectional N-bit pulse-latch based shift register can be executed by applying the linear feedback adding with XOR gate and NOT gate in unidirectional N-pulse-latch shift register respectively [13-14]. Therefore, the pulse-latch based linear feedback shift register can lessen the delay and increase data security by exchanging XOR and NOT gate as feedback in the N-bit shift register with pulse-latch and pulse clock signals [15-18].

In short unidirectional latch based linear feedback shift reg- ister is suggested. They reduce delay and increase data security by replacing shift register with proposed unidirectional binary code-latches. This paper's remaining section is explained as follows. Describe the proposed linear feedback shift register architecture in section II. Section III is detail study comparison and various analysis and finally, in section IV, Conclusions are presented.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Volume 10 Issue 5 May 2024

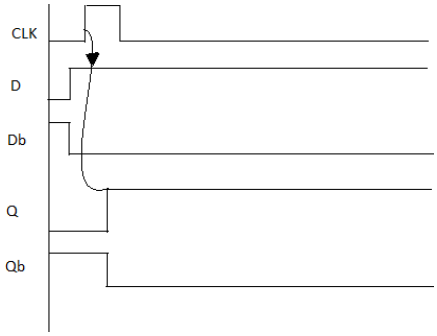

Fig. 2. Conventional Unidirectional Pulse-latch waveform [18]

II. ARCHITECTURE

A. Proposed Latch-Based Binary-Code Shift- Register

The Traditional 4-bit D latch-based binary-code shift-register is depicted in Fig.3. Initially, all data was reset by the binary-code shift-register using the reset signal. Every clock cycle, it shifts the data '1' right by one bit. The pattern of the shifting of the data recognized by the other user, very easily. In this reason the security of data will lose of latch-based shift-register.

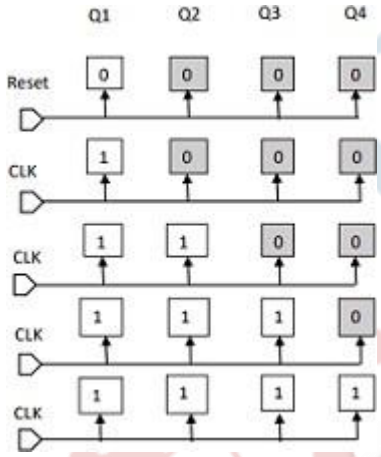

Fig. 3. Conventional unidirectional 4-bit Normal feedback-based binary-code shift-register [18]

However, the latch and two signals (CLK-odd and CLK-even) are used in the proposed linear feedback binary-code shift-register dissipated in the Fig. 4. We apply the XOR gate as feedback for improving the security purpose as per requirement. Here we adjust of the XOR gate after 4-bit latch-based shift register and all output of XOR gate attached to the first latch-based shift registers feedback as input.

Fig. 5 shows again the proposed linear feedback binary-code shift-register. Here we applying NOT gate after 4-bit latch-based shift register and combine output of NOT gate forwarding to the first latch-based shift registers feedback as input. By activating the odd and even latches, it can shift the

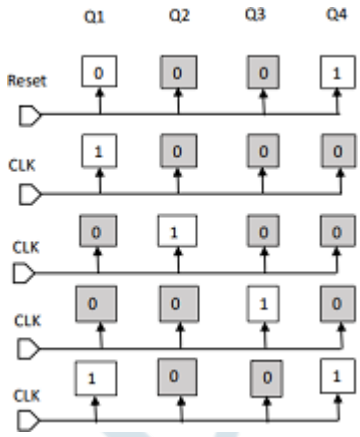

Fig. 4. Proposed unidirectional 4-bit XOR feedback-based binary-code shift- register

data to '1'. Because of generating random data as well as XOR gate, the data shifting pattern will separate then previous pattern of conventional latch-based circuit. Hence the security of the data will increase and secure from hackers.

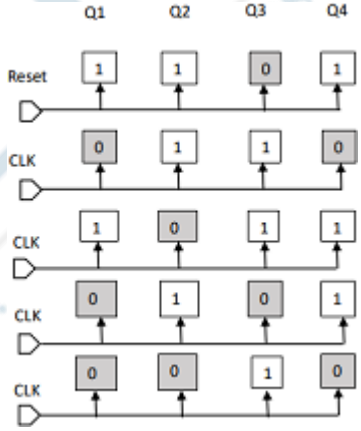

Fig. 5. Proposed unidirectional 4-bit NOT feedback based binary-code shift- register

Fig. 6 shows the conventional 16-bit binary-code shift-register that is unidirectional. It used to reset for initialize of data and CLK-signal for synchronized the data. It shifts the data '1' to right when the clock signal is CLK-odd or CLK-even and so on data will be shifted respectively.

Fig. 7 shows the proposed unidirectional 16-bit binary-code shift-register. The alignment of this 16-bit shift register is that the output of the first unidirectional latch is connected to the input of the second unidirectional latch and so on. For the reset system a pin RESET connected to every unidirectional latch. The unidirectional latch which is present in odd position with connected to the CLK-odd and which unidirectional latch present in even position with connected to CLK-even.

For the enhance security purpose we provided feedback as XOR and NOT gate to change the data forwarding pattern

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Volume 10 Issue 5 May 2024

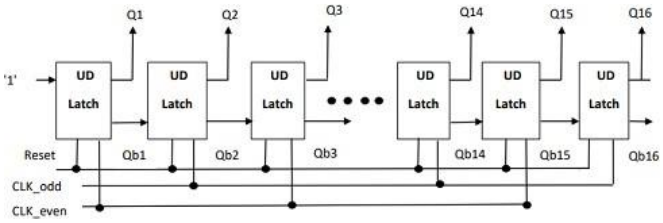

Fig. 6. Conventional unidirectional 16-bit binary-code shift-register [18]

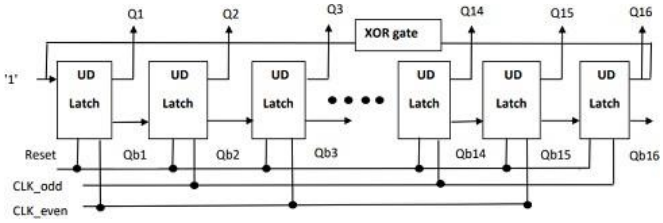

Fig. 7. Proposed unidirectional 16-bit binary-code shift-register

which is not easy to recognize by the other user and hacker. If you want more to more change the pattern of data forwarding so we have to apply more XOR and NOT after 4-bit unidi- rectional latch. At the resultant the feedback of unidirectional latch is not forwarding directly to input after one XOR gate while the data forward have to more XOR gate.

The performance of XOR gate is when the both bits are same like 0,0 or 1,1 so the resultant will be (Q= 0) and the both bit of alternate like 1,0 or 0,1 so the resultant will be (Q= 1). For this alternative feature of XOR gate the data of coming as feedback have been changed.

III. SIMULATION AND RESULTS

Fig. 8 shows the simulation waveform of proposed unidirec- tional binary-code shift-register, which were simulated with a 90nm CMOS process at a supply voltage of 1.8v and a clock frequency of 100MHz. The unidirectional linear feedback shift register shifts the data '1' right with CLK-odd and CLK-even respectively, when did not apply the linear feedback of the unidirectional latch. The pattern of data shifting shown in Fig. 8 is very simple for recognized by another user. Here its advan- tage is that the power consumption is 283.80 uW and take less delay 14.39ps but this system is not secure as per simulation waveform. Table I shows that comparison among different linear shift register when apply XOR gate as feedback, NOT gate as feedback and no feedback. Approximately 94.59% less power is consumed by a NO feedback linear shift register than a NOT gate feedback linear shift register, and 95.16%

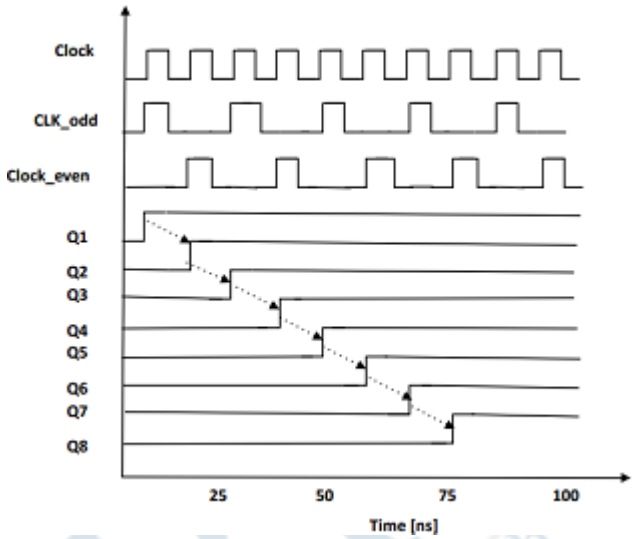

Fig. 8. Simulation waveform of Conventional binary-code shift-register [18]

less power is consumed by an XOR gate linear feedback shift register. Further delay parameter by no feedback linear shirt register is approximately 86.72% less than XOR gate linear feedback shift registers and approximately 27.40% less than NOT gate linear feedback shift register. The comparison of the security is higher when we apply XOR gate as feedback in the linear shift register.

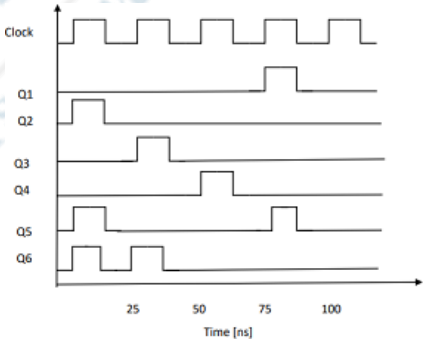

Fig. 9. Simulation waveform of proposed binary-code shift-register

Table I. Performance, Comparison, Different, Linear, Feedback

S. No.	Parameter	Normal feedback	XOR feedback	NOT feedback
01	Power [W]	283.8e-6	5.87e-3	5.25e-3
02	Delay [s]	14.39e-12	1.91e-12	380.2e-15
03	VDD (V)	1.8	1.8	1.8
04	Frequency [MHz]	100	100	100
05	Bit width of shift register	16	16	16
06	Size of Transistor [W/L]	120/90	120/90	120/90

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Volume 10 Issue 5 May 2024

IV. CONCLUSION

In this brief unidirectional linear feedback shift register is proposed. They are reducing power, delay and increase security by replacing XOR gate and NOT gate as feedback in linear shift register. Using a 90nm CMOS process, the proposed 16-bit linear feedback shift registers were simulated. They consume power 94.59% and 95.16% with Vdd = i.8V and a clock frequency of 100MHz. For security purpose is better XOR feedback linear shift register and for low power consumption is better is no feedback linear shift register and for less delay purpose is better NOT gate linear feedback shift register.

REFERENCES

[1] H. J. M. Veendrick," Short-circuit dissipation of static CMOS circuitry and its impact on the design of buffer circuits," IEEE Journal of SolidState Circuits, vol. 19, pp. 468-473, 1984.

[2] B. Wicht, T. Nirschl, and D. Schmitt-Landsiedel, "Yield and speed optimization of a latch-type voltage sense amplifier," in Proc. IEEE J. Solid-State Circuits, vol. 39, no. 7, pp. 1148–1158, Jul. 2000

[3] S. Babayan-Mashhadi and R. Lotfi, "Analysis and design of a low voltage low-power double-tail comparator," in Proc. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, 22(2), 343–352, 2014

[4] S. A. Mesgarani, M. N. Alam, F. Z. Nelson, and S. U. Ay, "Supply boosting technique for designing very low-voltage mixed-signal circuits in standard CMOS," in Proc. IEEE Int. Midwest Symp. Circuits Syst. Dig. Tech. Papers, pp. 893–896, Aug. 2010.

[5] J. Blalock, "Body-driving as a Low-Voltage Analog Design Technique for CMOS technology," in Proc. IEEE Southwest Symp. Mixed-Signal Design, pp. 113–118, Feb. 2000.

[6] D. Shinkel, E. Mensink, E. Klumperink, E. van Tuijl, and B. Nauta, "A double-tail latch-type voltage sense amplifier with 18 ps Setup+Hold time," in Proc. IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers, pp. 314–315, Feb. 2007.

[7] S. Huang, S. Diao and F. Lin," An energy-efficient high-speed CMOS hybrid comparator with reduced delay time in 40-nm CMOS process," Analog Integrated Circuits and Signal Processing, Volume 89, Issue 1, pp. 231–238, October 2016.

[8] Panigrahi, J. K., and Acharya, D. P.: Performance analysis and design of wideband CMOS voltage-controlled ring oscillator. IEEE International Conference on Industrial and Information Systems (ICIIS), pp. 234-238. (2010)

[9] Sadhu, B., Ferriss, M., Natarajan, A. S., Yaldiz, S., Plouchart, J. O., Rylyakov, A. V., and Friedman, D.: A linearized, low-phase-noise VCO based 25-GHz PLL with autonomic biasing. IEEE Journal of Solid-State Circuits, vol. 48, no.5, pp. 1138-1150. (2013)

[10] Kumar, M., Arya, S. K., and Pandey, S.: Low power digitally controlled oscillator designs with a novel 3-transistor XNOR gate. Journal of Semiconductors, vol. 33, no. 3, pp. 035001. (2012)

[11] Staszewski, R. B., and Balsara, P. T.: Phase-domain all-digital phase locked loop. IEEE Transactions on Circuits and Systems II: Express Briefs, vol.52, no. 3, pp.159-163. (2005)

[12] De Paula, L. S., Susin, A. A., and Bampi, S.: A wide band CMOS differential voltage-controlled ring oscillator. In Proceedings of the 21st ACM Annual Symposium on integrated Circuits and System Design. pp. 85-89. (2008)

[13] J.-F. Lin, M.-H. Sheu, Y.-T. Hwang, C.-S. Wong, and M.-Y. Tsai, "Low power 19-transistor true single-phase clocking flip-flop design based on logic structure reduction schemes," IEEE Trans. Very Large-Scale Integer. (VLSI) Syst., vol. 25, no. 11, pp. 3033–3044, Nov. 2017.

[14] J.-F. Lin, M.-H. Sheu, Y.-T. Hwang, C.-S. Wong, and M.-Y. Tsai, "Low power 19-transistor true single-phase clocking flip-flop design based on logic structure reduction schemes," IEEE Trans. Very Large-Scale Integer. (VLSI) Syst., vol. 25, no. 11, pp. 3033–3044, Nov. 2017.

[15] Ki-cham Woo, Hyeang-Ju Kang, Byung-Do Yang," IEEE Trans. on circuit and Syst., vol. 67, no. 10, Nov. 2020.

[16] Subha Chakraborty, Ashesh Ray Chaudhuri, Tarun Kanti Bhattacharya, "Design and analysis of MEMS cantilever based binary logic inverter", IEEE International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009, pp 184 - 188

[17] A. Hirata, H. Onodera and K. Tamaru" Estimation of Short Circuit Power Dissipation and its Influence on Propagation Delay for Static CMOS Gates", Proc. of ISCAS 96, vol. 4, pp.751 -754 1996

[18] Srinivasa R. Vemuru, and Norman Scheinberg," Short-Circuit Power Dissipation Estimation for CMOS Logic Gates," IEEE Transactions on circuits and Systems-I: Fundamental Theory and Applications, vol. 41, no. 11, p.762, November 1994.