Design and Analysis of a Linear Feedback Shift Register with Reduced Leakage Power

M. Janaki Rani
Research scholar, Sathyabama University,
Chennai, India

S. Malarkkan
Principal, ManakulaVinayagar Institute of
Technology, Puducherry,

ABSTRACT

As the CMOS technology is scaling down, leakage power has become one of the most critical design concerns for the chip designer. This paper proposes a low leakage linear feedback shift register that can be used in a crypto-processor. In this work, three bit, four bit and five bit linear feedback shift registers are implemented in 90nm and 65nm technology .This paper also proposes two leakage reduction techniques such as reverse body bias and transistor stack, which are applied to the above circuits. The leakage power of the circuits is analyzed with and without the application of reduction techniques. The results show that for all the circuits the combined effect of (RBB + Stack) leakage reduction method gives the least leakage power of 23.16nW, 47.53nWand 72.18nW for 3-bit, 4-bit and 5-bit linear feedback shift register respectively at 90nm technology. In 65nm technology the combined leakage reduction method gives the least leakage power of 33.86nW, 64.73nWand 95.14nW respectively. The circuits have been simulated with HSPICE using MOSFET models of level 54 with a supply voltage of 1 volt.

Keywords

Leakage power, linear feedback shift register, reverse body bias and transistor stack.

1. INTRODUCTION

The rapid growth in semiconductor device industry has led to the development of high performance portable systems with enhanced reliability. In such portable applications, it is extremely important to minimize current consumption due to the limited availability of battery power [1]. Therefore power dissipation becomes an important design issue in VLSI circuits. A significant portion of the total power consumption in high performance digital circuits is due to leakage currents. Leakage power makes up to 50% of the total power consumption in today's high performance microprocessors [2]. Therefore leakage power reduction becomes the key to a low power design. The leakage or static power dissipation is the power dissipated by the circuit when it is in standby mode and is given by

$$P_{leak} = I_{leak} * V_{dd} \qquad (1)$$

Where I_{leak} is the leakage current which flows in a transistor when it is in OFF state and V_{dd} is the supply voltage. The leakage current consists of various components, such as sub-threshold leakage, gate leakage, reverse-biased junction leakage, gate-induced drain leakage [4]. Among these, sub-threshold leakage and gate-leakage are dominant. The sub-threshold leakage current of a MOS device can be modeled as follows [3]:

$$I_{sub} = I_0 \exp[(V_{gs} - V_t)/(nV_T)][1 - exp(-V_{ds}/V_T)] \quad (2)$$

$$\text{And } I_0 = \mu_{eff} C_{ox} (W/L) V_T^2 \qquad (3)$$

Where $\mu_{eff}$is the electron/hole mobility, C_{ox} is the gate capacitance per unit area, W and L are width and length of the channel respectively, V_t is the threshold voltage, n is the sub-threshold swing co-efficient, V_T is the thermal voltage, V_{gs} is the transistor gate to source voltage and $V_{ds}$is the drain to source voltage.

2. LINEAR FEEDBACK SHIFT REGISTERS

A Linear feedback shift register (LFSR) is similar to a shift register with a feed back. The outputs of some of the flip flops in the shift register are feedback as input to a XOR gate and the output of XOR gate is the input to the first flip flop in the shift register. The initial value stored in the shift register is called the seed value and it can never be all zeros. Depending on the outputs feedback to the XOR gate a LFSR generates a random sequence of bits. Because of this property LFSRs are used in communication and error correction circuits for generating pseudo-noise and pseudo-random number sequences and they are also used in data encryption and data compression circuits in cryptography [5,6,7,8]. Fig.1 shows the block diagram of a LFSR with a characteristic polynomial f(x) = $1+x+x^3$. The output bit positions in LFSR which are feedback to the XOR gate are called taps and in this LFSR the taps are at position 1 (Q0) position 3 (Q2). The rightmost bit Q2 is called the output bit.bit positions that affect the next state are called taps. In this diagram the taps are 1, 3. The rightmost bit of the LFSR is called the output bit. The taps are exclusively ORed sequentially with the output bit and then feedback into the leftmost bit and during each clock pulse LFSR produce a sequence of bits called as output stream. In this way a LFSR can generate 2^n-1 different output sequences and it is called as maximum length LFSR. The characteristic polynomial of a LFSR is defined by the taps in the LFSR. For example in Fig.1a taps are at positions 1 & 3 and hence the characteristic polynomial is $1+x+x^3$ and the '1' in the polynomial correspond to the input to the first D flip-flop. Fig. 2 and Fig. 3 show the diagram of LFSR with polynomials $1+x+x^4$and $1+x^2+x^5$ respectively. Table I shows the output sequence generated by a 3-bit LFSR with the seed value [1 1 1].

Table 1. Output sequence of LFSR

Clock Pulse	Output of LFSR		
	Q0	Q1	Q2
1	1	1	1(Seed value)
2	0	1	1
3	1	0	1
4	0	1	0
5	0	0	1
6	1	0	0
7	1	1	0
8	1	1	1(Starts repeat)

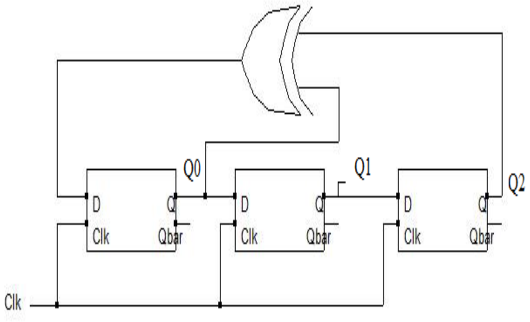


Fig 1: Three bit LFSR ($1+x+x^3$)

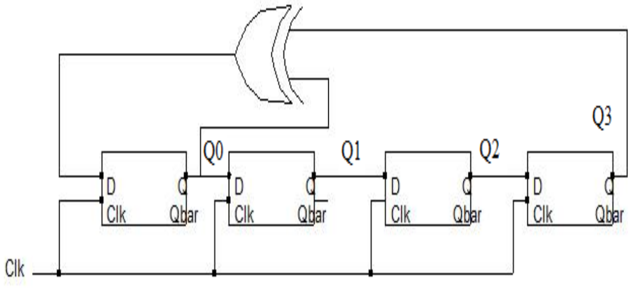


Fig 2: Four bit LFSR ($1+x+x^4$)

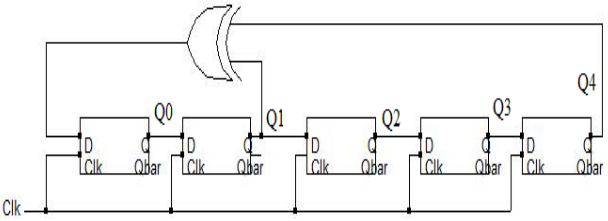


Fig 3: Five bit LFSR ($1+x^2+x^5$)

3. PROPOSED DESIGN OF LFSR AND REDUCTION METHODS

The hardware implementation of LFSRs requires D flip-flops and XOR gates. Fig. 4 and Fig. 5 show the circuit of low power D flip-flop designed using pass transistors and an XOR gate respectively. The D flip-flop combines a pair of master and slave D latch. The circuit uses pass transistors (PT) and inverters for the master-slave latches [9] as shown in Fig. 4. The two chained inverters are in memory state when the PMOS loop transistor is on, that is when Clk = 0.Other two chain inverters on the right hand side acts in the opposite way. The flip-flop changes its state during the falling edge of the clock. The CMOS implementation of a 3-bit LFSR is shown in Fig. 6.

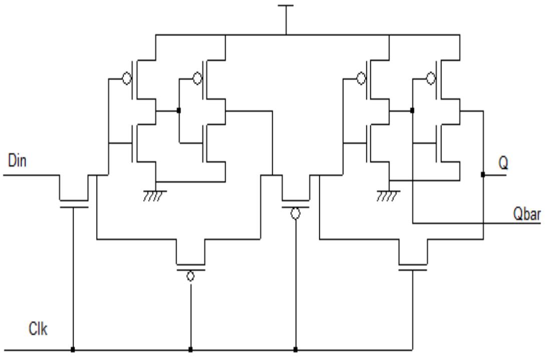


Fig 4: D flip-flop

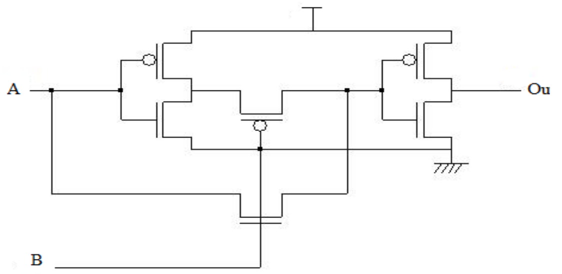


Fig 5: CMOS XOR gate

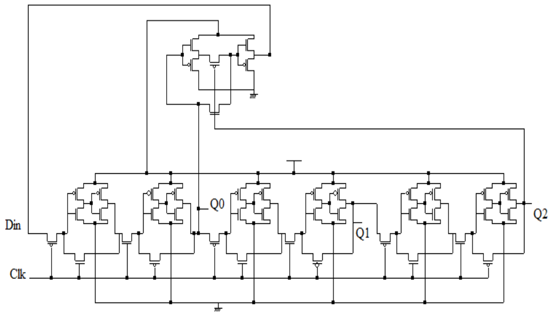


Fig 6: CMOS three bit LFSR (1+x+x^3)

The leakage power in this LFSR can be reduced using techniques like MTCMOS power gating, transistor stack, body bias etc. In this work transistor stack and reverse body bias methods are proposed for leakage reduction.

3.1 Transistor stack method

The leakage current flowing through a stack of series connected transistors reduces when more than one transistor of the stack is turned OFF. This effect is known as the “Stacking Effect” [10]. When two or more transistors that are switched OFF are stacked on top of each other then they dissipate less leakage power than a single transistor that is turned OFF as shown in Fig. 7a and 7b. This is because each transistor in the stack induces a slight reverse bias between the gate and source of the transistor right below it, and this increases the threshold voltage of the bottom transistor making it more resistant to leakage. Therefore in Figure 7a transistor T2 leaks less current than transistor T1 and T3 leaks less than T2. Hence the total leakage current through the transistors T1, T2 and T3 is decreased as it flows from V_{dd} to ground. So I_{leak1} is less than I_{leak2} [11]. If natural stacking of transistors does not exist in a circuit, then to utilize the stacking effect a single transistor of width W is replaced by two transistors each of width W/2 [12] as shown in Fig. 7c.

The leakage reduction achievable in a two-stack comprising of devices with widths W_u and W_l compared to a single device of width w is given by following equation [13].

$$X=\frac{I_{device}}{I_{stack}}=\frac{w}{W_u^{\alpha}W_l^{1-\alpha}}10\frac{\lambda_d V_{dd}}{s}(1-\alpha) \qquad (4)$$

$$\text{Where} \quad \alpha=\frac{\lambda d}{1+2\lambda d} \qquad (5)$$

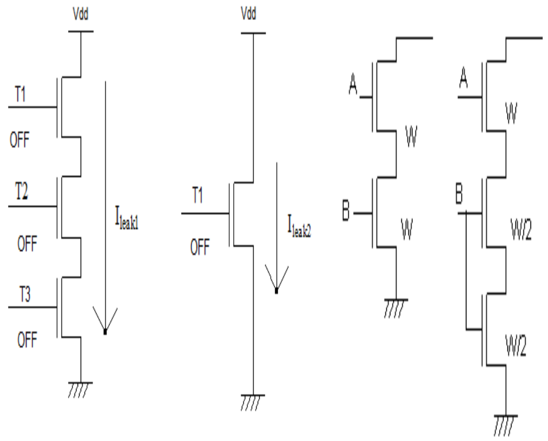
λ_d is the drain-induced barrier lowering (DIBL) factor and s is the sub-threshold swing co-efficient. When $W_u = W_l = W/2$ then the leakage reduction factor or stack effect factor X is rewritten as

$$X=\frac{w}{\frac{w}{2}^{\alpha}\frac{w}{2}^{(1-\alpha)}}10\frac{\lambda_d V_{dd}}{s}(1-\alpha) \qquad (6)$$

$$X=2\times 10^{\frac{\lambda_d V_{dd}}{s}}\left(\frac{1+\lambda_d}{1+2\lambda_d}\right) \qquad (7)$$

$$X=2\times 10^{u} \qquad (8)$$

Where u is the universal two-stack exponent which depends only on the DIBL factor λ_d, sub-threshold swing factor s and supply voltage V_{dd}. For example, in the 90nm process technology, consider an NMOS transistor of width W =100 nm and W/2 = 50nm, DIBL factor λ_d = 0.08, V_{dd}=1V and sub-threshold swing factor s= 90mV/decade. Then α = 0.07 and as per equation 7, the stack effect factor X is calculated to be 13.52.This gives I_{stack} = 0.074 I_{device}, and thus the leakage current through a stack of two off devices is less than that through a single off device.



(a) (b) (c)

Fig 7: Transistor stack effect

3.2 Reverse body bias method

Reverse body biasing (RBB) can be used to dynamically raise the threshold voltage during standby mode, thereby reducing the leakage power [14]. By applying reverse bias to the body of the devices, the threshold voltages can be adjusted because of the body effect. For example, biasing an NMOS device body with a voltage lower than Ground, or biasing a PMOS device body with a voltage higher than V_{CC} will increase the threshold voltage. The effect of body bias voltage on leakage power for a NMOS transistor is shown in Fig. 8 [15].

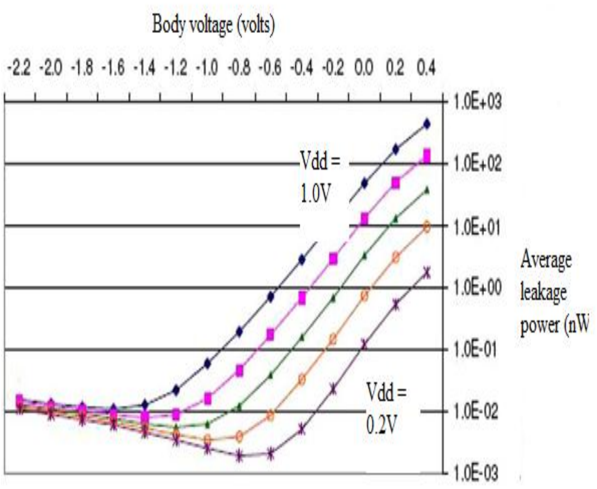


Fig 8: Effect of body bias voltage on leakage power [15]

The threshold voltage V_t is related to the reverse bias voltage between the source and body V_{sb} by the following equation

$$V_t = V_{t0} + \gamma\{(\sqrt{2\phi_f + |V_{sb}|}) - (\sqrt{2\phi_f})\} \qquad (9)$$

Where V_{t0} is the zero bias V_t for V_{sb} = 0 volt and it is mostly a function of the manufacturing process. The parameter ϕ_f is Fermi potential and γ is body effect co-efficient and it expresses the impact of changes in $V_{sb.}$ For typical body effect co-efficient values in modern technologies, a 100mV change in the body bias will result in approximately 20mV change in V_t. For example, if 500 mV reverse body biasing is applied to a circuit during the standby mode, then the V_t will change by approximately 100mV, which results in approximately a 10x reduction in leakage currents.

4. SIMULATION RESULTS

In this paper, three bit (1+x+x^3), four bit (1+x+x^4) and five bit (1+x^2+x^5) LFSRs are implemented in 90nm and 65nm technology. Low leakage DFF using pass transistors and low power XOR gate are used for the design. Then the proposed leakage reduction techniques RBB and transistor stack are applied separately to all the above circuits and then a combination of RBB and stack is also applied. The leakage power dissipation of the above circuits is compared with and without the power reduction techniques. The net lists of the circuits are extracted and simulated with BSIM4 models of MOSFET [17]. The simulations are done in HSPICE with a supply voltage of 1 volt, at a temperature of 27° C with a load capacitance of 50fF. The simulation results of LFSRs in 90nm and 65nm process technologies are shown in Table II and Table III. The leakage power decreases with both the methods. Fig. 9 and Fig. 10 show the % leakage power reduction in LFSRs in 90nm and 65nm respectively.

Table 2.Leakage power of LFSRs (90nm)

S.No	Reduction Technique	P_{leak} of LFSR (n W)		
		1+x+x^3	1+x+x^4	1+x^2+x^5
1	Base Case	32.45	68.93	97.31
2	RBB	27.11	59.62	85.30
3	Stack	25.84	52.47	78.46
4	RBB + Stack	23.16	47.53	72.18

Table 3.Leakage power of LFSRs (65nm)

S.No	Reduction Technique	P_{leak} of LFSR (n W)		
		1+x+x^3	1+x+x^4	1+x^2+x^5
1	Base Case	42.50	93.05	126.45
2	RBB	40.24	87.19	115.27
3	Stack	35.61	75.32	102.96
4	RBB + Stack	33.86	64.73	95.14

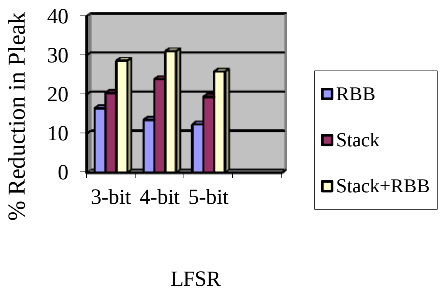


Fig 9: Leakage reduction in LFSRs at 90nm

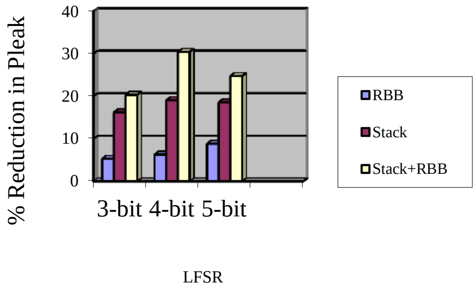


Fig 10: Leakage reduction in LFSRs at 65nm

5. CONCLUSION

In this paper CMOS implementation of LFSRs using pass transistors and XOR gate are presented. In this work the analysis of leakage power of LFSRs are carried out in 90 nm and 65 nm technologies using two reduction techniques RBB and transistor stack. The leakage power decreases with both the proposed methods and the reduction is more with the combined approach of RBB and stack. The reduction is high in the case of 4-bit LFSR with 31.04% and 30.43% in 90nm and 65nm respectively with RBB+stack method. With RBB technique alone, the percentage leakage reduction is more in 90nm (16.45% in 3-bit LFSR circuit) and it increases to 28.62% for the combined RBB and stack approach. Hence the proposed combined RBB+Stack approach can be used for the design of low leakage LFSR for use in cryptograph

6. REFERENCES

[1] Deepak subramanyan, B.S. and Adrian Nunez, 2007 “Analysis of Sub-threshold Leakage Reduction in CMOS Digital Circuits”, *Proceedings of the 13th NASA VLSI Symposium,* USA, June 5-6.

[2] International Technology Roadmap for Semiconductors: www.itrs.net/Links/2005ITRS/Design 2005.pdf.

[3] Borivoje Nikolic, 2008 “Design in the Power–Limited Scaling Regime”, IEEE Transactions on Electron Devices, Vol. 55, No. 1, pp.71-83.

[4] Yongpan Liu, Robert P. Dick, Li Shang and Huazhong Yang, 2007 “Accurate Temperature Dependent Integrated Circuit Leakage Power Estimation is Easy”, EDAA.

[5] Davida, G.I. and Rodrigues, 1994 “Data Compression Using Linear Feedback Shift Registers”, Proceedings of the IEEE Data Compression Conference, Los Alamitos.

[6] Moon, T. K. and Veeramachaneni. S. 1999 “Linear Feedback Shift Registers as Vector Quantisation Codebooks”, Electronics Letters, Vol. 35, No. 22, pp. 1919-1920.

[7] Jamil. T and Ahmad . A. 2002 “An Investigation into the Application of Linear Feedback Shift Registers for Steganography”, Proceedings of IEEE SOUTHEASTCON Conference, Columbia, pp. 239-244.

[8] Alspector, J., Gannett, J. W., Haber, S., Parker, M. B., and Chu, R. 1990 “Generating Multiple Analog Noise Sources from a Single Linear Feedback Shift Register with Neural Network”, Proceedings of the IEEE International symposium on Circuits and Systems, New Orleans, Vol. 2, pp.1058-1061.

[9] Janaki Rani M. and Malarkann S, 2012 “Leakage Power Reduction and Analysis of CMOS Sequential Circuits”, International Journal of VLSI Design and Communication Systems (VLSICS), Vol.3, No. 1. February 2012, pp. 13-23.

[10] M.C. Johnson, D.Somasekhar, L.Y. Chiou, and K.Roy, 2002, “Leakage Control with Efficient Use of transistor Stacks in Single threshold CMOS”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 10, No. 1, pp. 1-5.

[11] VasanthVenkatachalam and Michael Franz, 2005 “Power Reduction Techniques for Microprocessor Systems”, ACM Computing Surveys, Vol. 37, No. 3, pp. 195-237, September.

[12] Siva Narendra, Vivek De, ShekarBorkar, Dimitri A Antonisdis and Anantha P. Chandrakasan, 2004 “Full-Chip Sub-threshold Leakage Power Prediction and Reduction Techniques for Sub 0.18-µm CMOS”, IEEE Journal of Solid State Circuits, Vol.39, No.2, pp.501-510.

[13] Siva Narendra, ShekharBorkar, Vivek De, Dimitri Antoniadis, and AnanthaChandrakasan, 2001 “Scaling of Stack Effect and its Application for Leakage Reduction”, ISLPED ’01, pp. 195-200.

[14] Keshavarzi, A., Narendra, S., Borkar, S., Hawkins, C., Roy, K., De, V. 1999 “Technology Scaling Behavior of Optimum Reverse Body Bias for Standby Leakage Power Reduction in CMOS IC’s,” International Symposium on Low Power Electronics and Design, pp 252-254.

[15] HeungJun Jeon, Yong-Bin Kim and Minsu Choi, 2010 “Standby Leakage Power Reduction Technique for Nanoscale CMOS VLSI Systems”, IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 5, May,pp.1127-1133.

7. AUTHORS PROFILE

Ms. M. Janaki Rani received her B.E. degree in EIE in the year 1990 from Annamalai University, Tamil Nadu, India and M.E. degree in Electronics in the year 2002 from MIT, Anna University, and Chennai, India. She is working as an Associate Professor in ECE Dept., Dr. M.G.R. University, and Chennai. She has around 18 years of teaching experience. Currently she is doing her research in the area of low power VLSI Design in Sathyabama University, Chennai. Her research interests include Low power VLSI design, VLSI signal processing, advanced digital system design and embedded system design. She has published many papers in national and international conferences & journals.

Dr.S.Malarkkan, Principal in ManakulaVinayagar Institute of technology, Puducherry obtained his B.E. Degree from Thiagarajar College of Engineering, Madurai in the year 1988 and M.E. Degree in Optical Communication and Ph.D in Wireless & Mobile Communication from College of Engineering, Anna University, Chennai. He has over 22 years of experience in teaching and his area of interest includes analog and digital communication, mobile communication and wireless networks. He is a life member of ISTE, CSI and a fellow of IETE. He was serving as a member in IETE Executive Committee, Chennai zone from 2006 to 2008.