A New Low Power and High Speed Bidirectional Shift Register Architecture

N. Sklavos, P. Kitsos, N. Zervas and O. Koufopavlou

VLSI Design Laboratory,
Electrical and Computer Engineering Department,
University of Patras, Patras, GREECE
E-mail: nsklavos@ee.upatras.gr

Abstract. In this paper a new, low power and high speed Bidirectional Shift Register (BSR) architecture is presented. It can be used for the design and the implementation of hard arithmetic operations. Reconfigurable computing, and cryptographic algorithms are two application examples where by using the new BSR their power and speed can be improved. Comparing to the conventional design, the proposed achieves 19-42 % power consumption reduction with simultaneous 25% reduction of the covered area. So the new design fits perfectly in designs with hard specifications of power dissipation and covered area (e.g. wireless). The whole design was captured by using VHDL language, and for the synthesis a 0.7 um CMOS standard cell library was used. The power measurements were taken with a custom design tool that was developed in our laboratory.

1. Introduction

New submicron CMOS technologies offer many capabilities on hardware architectures. The computer-aided techniques, which are based on these technologies, have provided the enabling methodology to design efficiently and successfully large-scale high-performance circuits for a wide spectrum of applications. These techniques have also played a major role for the reduction of design time and optimization of the circuit quality. New facilities are offered in all of stages of the creation procedure of a digital circuit: design, fabrication and packaging [1], [2]. The design cost has been minimized due to the large range of the available commercial CAD tools and the supported cell libraries. The system on chip design has only compounded the problem of power dissipation.

Power consumption is a parameter that has become very important in VLSI design the last years. The rapidly growth of the portable devices such as mobile phones and portable computers forced the digital systems' designers and researchers to design new flexible architectures and systems with low power consumption. On the other hand, the growth rate of the battery technologies is enough less than the today's demands of power consumption. For example a multimedia mobile terminal of the future, which would support services such as video conference, pen based input, data operations and voice recognition would demand average power consumption at about

40 W. With today's battery technologies such a hand-held terminal would demand at about 10 kgrs of battery for ten hours operation.

Of course the portability of the systems is not the only reason for the low power demand in the VLSI designs. In many systems that tradionally was considered that there is no problem with the power consumption, like personal computers, the issue of low power has been appeared too. The rapidly extension of digital devices and the widely usage of them would create a major problem with the energy sources of the future due to the users growing power demands.

Architectures and methodologies for the desirable power reduction have been proposed at various levels [3], [4]. Low power designs are needed in all levels of a digital system design. In sectors of digital circuits with hard power specifications like wireless communications low power demand is very important too. Especially, components with broadly usage have to consume as less power as possible.

Shift registers are used widely in many applications. Especially, Bidirectional Shift Registers (BSRs) are basic parts of many well know encryption algorithms [5]. Hardware implementations of security systems for mobile communications, based on these algorithms, need low power BSRs with high speed performance [6]. On the other hand, reconfigurable computing techniques demand such of these registers too, in order to implement hard arithmetic operations [7].

Many low power designs for a one direction LFSR have been illustrated [8], [9]. Although, there are not many architectures for BSR published. The architecture that is used widely for BSR uses a set of a 4x1 multiplexers (Fig.1) [10]. In some other applications, the designers use two different one direction Linear Feedback Shift Registers (LFSRs) in order to achieve circular bidirectional shifting operations [11]. Of course these methods is not suitable for systems with low power and small covered area specifications.

In this paper, a new low power design for the implementation of a BSR is proposed. The proposed architecture is reconfigurable in the sense that can be programmed and configured for different wide of registers, depended on the user's needs.

The paper is organized as follows: the conventional architecture of a BSR is described in Section 2. In Section 3 the proposed architecture is presented in details. Experimental results, with power, area and time measurements are given in Section 4. Finally in Section 5 there are some useful conclusions about the advantages and the usability of the proposed architecture.

2. Conventional Architecture of a BSR

The conventional architecture for BSR uses a set of a 4x1 multiplexers [10]. This architecture is showed in Fig.1. For every used Flip/Flop (F/F) the design needs one 4x1 multiplexer. Due to the regularity, the four inputs of each multiplexer are similar. The first is the parallel input for data, the second is the preceding F/F output, the third is the following F/F output and the last input is the output of the F/F that the multiplexer forces.

The two signals Select0 and Select1 control the operation of the BSR. After the parallel shift register load the values of the two control signals determine the shift direction. Table 1 shows the control mode of each 4x1 multiplexer.

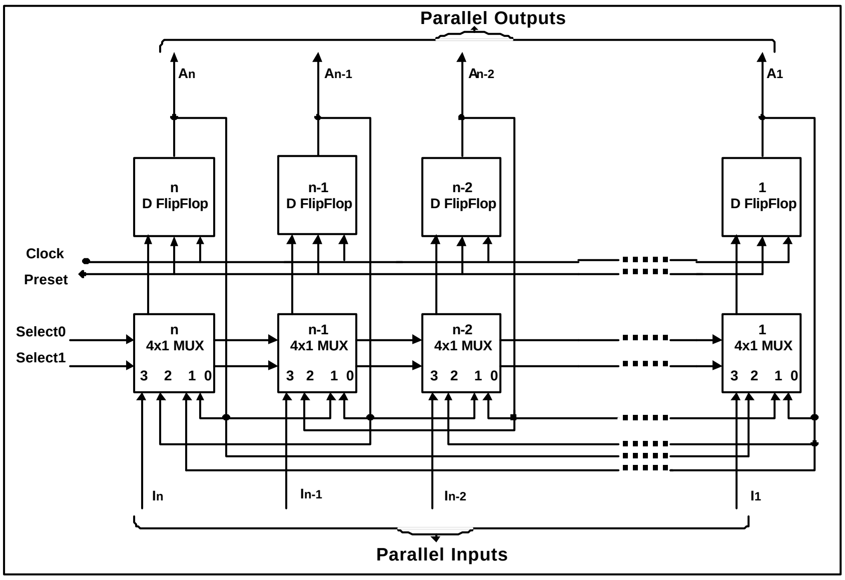

Fig. 1. Conventional bidirectional shift register architecture

Table 1. Control mode of each 4x1 multiplexer

Select1	Select0	Register Operation
0	0	No change
0	1	Shift Right
1	0	Shift Left
1	1	Parallel Load

It is obvious that this architecture is not suitable for applications with hard area specifications. When a large n-bit Shift Register is needed, this architecture demands n 4x1 multiplexers and the circuit's covered area increases with a linear function. At the same time the power consumption of the total design increases dramatically because of the large number of multiplexers. It has been measured that doubling the register's wide, results in doubling of the power consumption.

3. Proposed Architecture

The proposed architecture is based on the observation that a BSR can be constructed by using only one shift direction (right or left) [12]. So, although the F/Fs data are shifted in one direction the result is a right or left shift. Assume the data are shifted only to the right as shown in the proposed n-bit BSR of Fig. 2. A k steps left shift can be achieved by having n-k steps right shift.

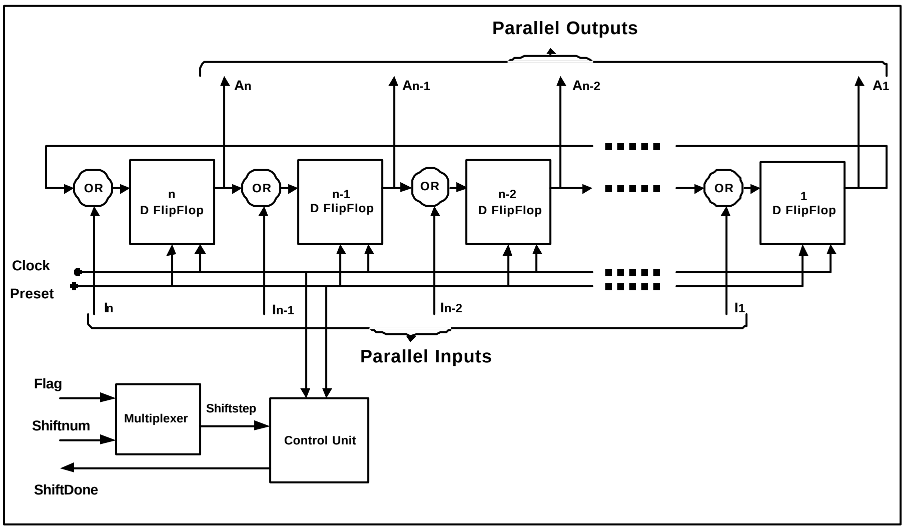

Fig. 2. Proposed bidirectional shift register architecture

Three are the main advantages of the proposed architecture: 1) the required logic reduction, 2) the power consumption reduction and 3) the system routing complexity minimization. As the above figure shows in details, the whole system consists of a Linear Feedback Shift Register (LFSR) of n F/Fs, a Multiplexer, and a Control Unit. It is obvious that the LFSR is n-bit wide, where n is the maximum n shift step positions. For example, if 16 shift step positions are required a 16-bit LFSR is needed. The design has n parallel inputs, one for each bit of the input data and n parallel outputs. For every F/F, one or-gate of two inputs is used in order to achieve the parallel load. In the next section the design's operation is analyzed in details.

Although someone can be arguing that the proposed design is slow when it operates in the opposite direction (left for the example of Fig. 2), this is not true. When the LFSR needs to shift n-k step positions, in order to achieve the same result as in the case of k shift left positions with k<n/2, it needs n-k periods of clock. In this case the conventional architecture of a BSR needs k periods (of course k is always less or equal to the LFSR wide n). This occurs for the half cases of shifting operation. In the other half, when k>n/2, the proposed design needs less clock periods than the conventional architecture. In the second case (k>n/2) the proposed designed is faster, with the same ratio compared to the cases that is slower when k<n/2. Of course when the number of shifting step positions is randomly chosen and all values of k appear with the same probability, the average performance speed of the two compared architectures is the same.

The operation of the proposed design starts with the initial parallel loading of the. This is the reason of using the or-gates. After, the input vector is forced equal to zero and the system starts to operate due to the user's commands. The Flag signal determines the desirable shift direction. If the user wants the input vector to be shifted in right direction, the flag indicator is equal to zero. Alternative for left direction, the Flag signal is one. The Shiftnum input signal specifies the user's desirable number of shifting positions. The output signal of the multiplexer, Shiftstep, defines the number of the real shifting steps that the LFSR should do. This means that if the desirable direction of shifting is right (Flag indicator is equal to zero) Shiftstep signal has the same value with the Shiftnum input. If the user needs the vector to be shifted in the opposite direction (left) the Shiftstep value is equal to {n-shiftnum}, where n is the number of F/Fs. The system's mode operation is given Table 2. Note that values A and B are less than n.

Table 2. Proposed design's truth table

Shifting Direction	**Flag**	**Shiftnum**	**Shiftstep**	**LFSR Shifting Steps**
Right	0	A	A	A
Left	1	B	n-B	n-B

When the Control Unit verifies that the appropriate shifting steps have been done, forces the Shiftdone output signal equal to one. This is a handshake signal, which shows to the user that the correct result is in the parallel outputs.

4. Experimental Results

The design has been implemented by using VHDL (VHSIC Hardware Description Language). All of the system components have been described with structural architecture. The architecture of the design has been synthesized using the available commercial tool of Mentor Graphic, Autologic. For the simulation of the system the tool Quicksim of the same company have been used. The power measurements of the system's power dissipation have been done by using an in-house plug-in to Mentor Graphics Framework [13], which automatically generates scripts, invokes the tools and parses their reports. For the measurements, a large number of randomly generated input vectors and for different shifting positions is used. All the measurements are made using a 0.7 um CMOS standard cell library.

In Table 3, the proposed design simulation and synthesis results and compared with results produced by using the conventional design.

Table 3. Simulation and synthesis results

Wide (n)	Number of Transistors	Estimation Area (mils^2)
	(Conventional Design / Proposed Design % Reduction)	
8	779 / 587 24.65%	52.85 / 42.71 19.19%
16	1398 / 1030 26.32%	94.18 / 74.65 20.74%
32	2425 / 1713 29.36%	162.26 / 124.60 23.21%
64	4434 / 3103 30.32%	296.94 / 225.20 24.16%
128	8452 / 5530 34.57%	563.28 / 401.05 28.85%

A significant reduction in the number of transistors and estimation area between the two cases are shown. The estimation area reduction reaches the values of 28.85 % (Fig.3).

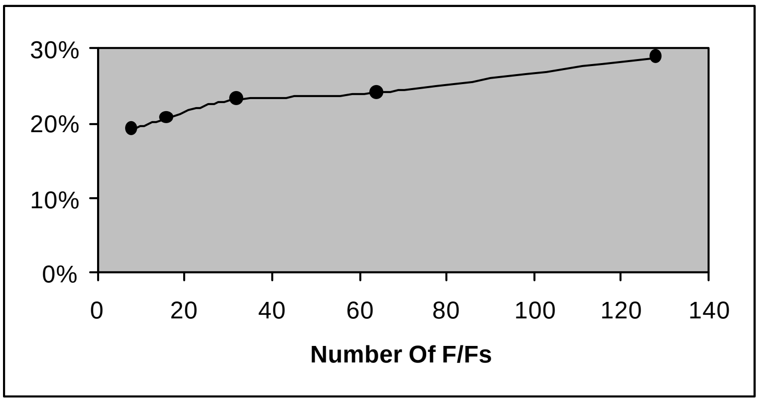

Fig 3. % Comparison of the estimation area of the proposed with the conventional design

The power consumption measurements are showed in Table 4. Different measurements for various values of n (number of F/Fs) were taken. Measurements for different number of shifting step positions are presented also in Table 4.

Table 4. Power measurements

Number Of F/Fs	Conventional Design (mW)			Proposed Design (mW)		
	n/4	n/2	3n/4	n/4	n/2	3n/4
8	0.000681	0.000768	0.00643	0.000572	0.000572	0.000512
16	0.001411	0.001543	0.001631	0.001139	0.001139	0.001220
32	0.002742	0.002250	0.002404	0.002056	0.002056	0.001616
64	0.005589	0.005781	0.005950	0.003654	0.003654	0.003717
128	0.011131	0.011382	0.011565	0.006784	0.006784	0.006506

In the next three figures (Fig. 4, 5, 6) the Table 4 data are shown graphically. The graph with the black colour is the plot of the conventional design (C.D.) and the gray one shows the measurements of the proposed design (P.D.). It is obvious that in all the three cases and for all the n-bit wide the proposed design power consumption measurements are much better (less) than these of the conventional design. So, the conventional design can be substituted by the proposed design in all the cases.

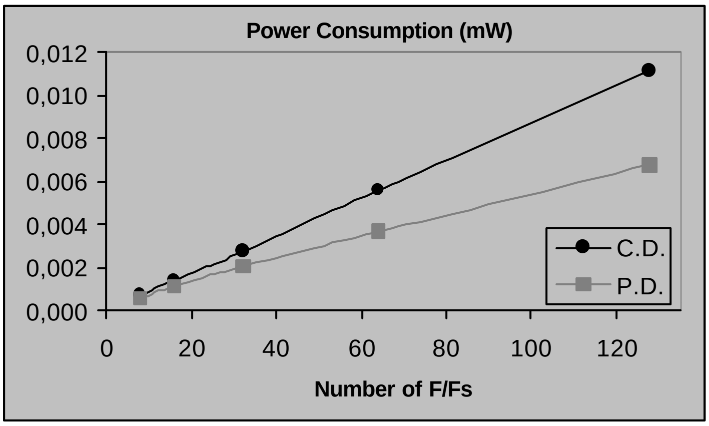

Fig.4. Power measurements for n/4 shifting positions

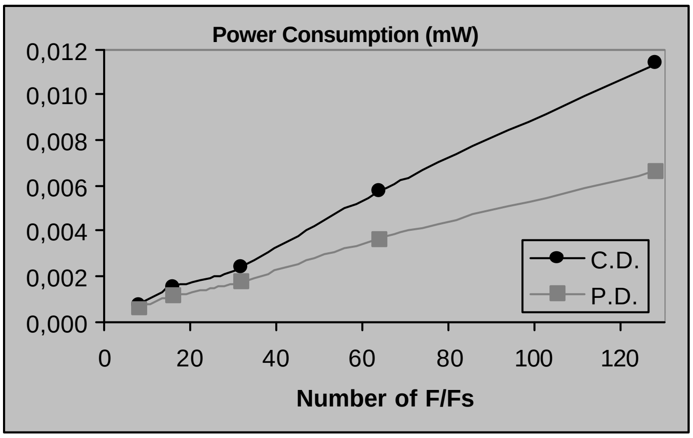

Fig. 5 Power measurements comparison for n/2 shifting positions

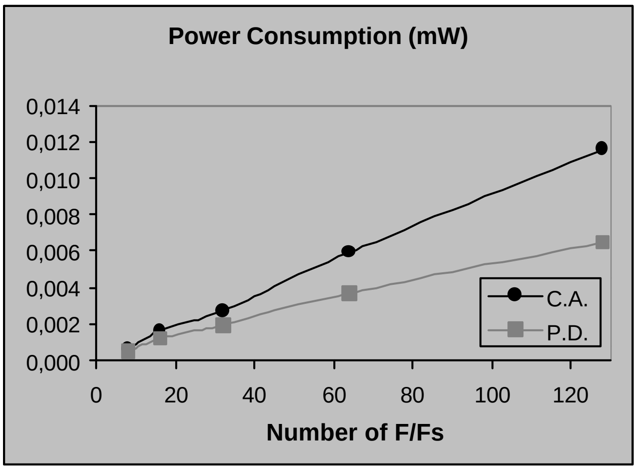

Fig. 6. Power measurements comparison for 3n/4 shifting positions

In Table 5 the comparisons of the proposed and conventional design power consumption measurements for the examined bit wide and shifting positions are shown. The table data represents the results from the formula:

$$\text{Power Reduction} = \frac{P_{CD} - P_{PD}}{P_{CD}} \text{ x } 100\% \qquad (1)$$

where P_{CD} is the power consumption of the conventional design and P_{PD} is the power consumption of the proposed design.

Table 5. Percentage comparisons of the power consumption measurements

Number Of F/Fs	Power Reduction (Shifting Positions n/4)	Power Reduction (Shifting Positions n/2)	Power Reduction (Shifting Positions 3n/4)	Average Value
8	15,93%	19,79%	20,30%	18,67%
16	19,29%	24,84%	25,22%	23,12%
32	25,01%	31,95%	32,76%	29,91%
64	34,62%	36,47%	37,52%	36,20%
128	39,05%	41,56%	43,74%	41,45%

From the power consumption measurements, power reduction from 19 to 42% between two cases is shown, in average units (Table 5). This is the major advantage of the proposed BSR design. The power reduction measurements also show that when the number of F/Fs is greater than n=32 the power consumption reduction reaches the maximum values of 30-42%. This shows that the proposed design fits better in applications that they need shift registers with wide greater to 32 bits.

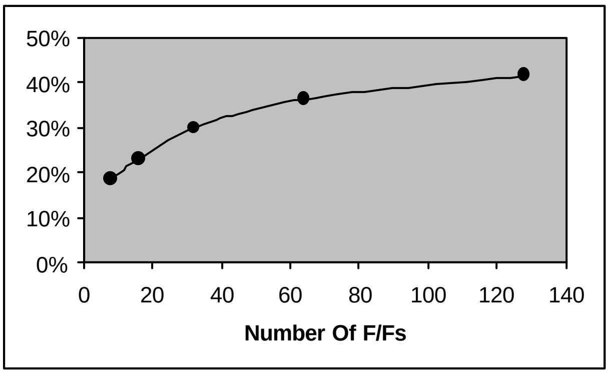

Fig 7. Average power dissipation reduction

The plot of the average value of the power dissipation reduction is given in Fig. 7. The average power dissipation reduction is almost an exponential function of the Bidirectional Register’s wide (number n of F/Fs).

Time measurements were taken too. In both designs, conventional and proposed, the maximum critical path is the F/Fs chain. Due to this event, the throughput of both designs appears to be the same, for the same number of the BSR wide (number n of F/Fs). For the library that we used, 1,16 nsec is the F/F delay time, so the BSR maximum throughput is 0,862 Gbps.

5. Conclusions

A low power VLSI Bidirectional Shift Register is proposed. This design can be used in cryptographic algorithms hardware implementations, especially for wireless communications. The presented design can also be a basic part of reconfigurable computing hardware designs, which support hard arithmetic operations. The introduced method achieves power consumption reduction with average values between 19% and 42%. The design's covered area is about 25% less than the conventional design. The two main characteristics of the proposed design are the power consumption and the covered area reduction. These major advantages prove the usability of the proposed architecture in today's implementations, which have hard power and covered area specifications.

References:

1.N. Weste and K. Eshraghian, "Principles of CMOS VLSI Design : A Systems Perspective", Addison-Wesley, Reading, MA, 1993.

2.W. Wolf, "Modern VLSI Design: A Systems Approach", Prentice-Hall, Eglewood Cliffs, NJ, 1994.

3.A.P.Chandrakasan, A. Burstein and R. W. Brodersen, "A Low Power Chipset for a Portable Multimedia I/O Terminal", IEEE Journal of Solid State Circuits, Vol 29, No 12, December 1994.

4. A.P.Chandrakasan, A. Burstein and R. W. Brodersen, " Low Power memory and arithmetic design for signal processing", IEEE Wkshp Low Power Electronics, Phoenix AZ, Aug. 25-26, 1993.

5.Bruce Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C", Second Edition, John Wiley and Sons, New York, 1996.

6.WAP Forum: "Wireless Transport Layer Security Protocol (WTLS)", 2000, http://www.wapforum.org

7.Behrooz Parhami, "Computer Arithmetic, Algorithms and Hardware Design",Hardcover, August 1999.

8.M. Brazzarola and Franco Fummi, "Power Characterization of LFSRs", Proc. IEEE International Symposium on Defect and Fault Tollerance in VLSI Systems, Albuqulrqul, New Mexico, November 1999.

9.M. E. Hamid and Chien-In Henry Chen "A Note to Low Power Linear Feedback Shift Registers", IEEE Transactions on Cicuits and Systems –II: Analog and Digital Signal Processing vol. 45, No 9, September 1998.

10. M. Morris Mano, "Digital Design", Second Edition, Prentice Hall Inc 1991.

11."Secure Hash Standard", Federal Information Processing Standards Publication 180-1,1995, http://www.itl.nist.gov/fipspubs/fip180-1.htm

12. J. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Transactions on Information Theory, Vol. IT-15, No1, January 1969.

13. N. Zervas, S. Theoharis, D. Soudris, C.E. Goutis, and A. Thanailakis "Generalized Low Power Design Flow", LPGD Project (ESPRIT 25256), Deliverable Report LPGD/WP2/UP/D1.3R1, pp. 11-15, Jan 1999.