Design of a Reliable XOR-XNOR Circuit for Arithmetic Logic Units

Mouna Karmani, Chiraz Khedhiri, Belgacem Hamdi, Amir-Mohammad Rahmani, Ka Lok Man, Kaiyu Wan

Design of a reliable XOR-XNOR Circuit for Arithmetic Logic Units

Mouna Karmani[1], Chiraz Khedhiri[1], Belgacem Hamdi[1], Amir-Mohammad Rahmani[2], Ka Lok Man[3] and Kaiyu Wan[3]

[1]Electronics & Microelectronics Laboratory, Monastir, Tunis University, Tunisia
[2]University of Turku, Finland and [3]Xi'an Jiaotong-Liverpool University, China

{mouna.karmani, chirazkhedhiri}@yahoo.fr, Belgacem.Hamdi@issatgb.rnu.tn, amir.rahmani@utu.fi, {ka.man,Kaiyu.Wan}@xjtlu.edu.cn

Abstract. Computer systems used in safety-critical applications like space, avionic and biomedical applications require high reliable integrated circuits (ICs) to ensure the accuracy of data they process. As Arithmetic Logic Units (ALUs) are essential element of computers, designing reliable ALUs is becoming an appropriate strategy to design fault-tolerant computers. In fact, with the continuous increase of integration densities and complexities ICs are susceptible to many modes of failure. Thereby, Reliable operation of ALUs is critical for high performance safety-critical computers. Given that XOR-XNOR circuits are basic building blocks in ALUs, designing efficient reliable XOR-XNOR gates is an important challenge in the area of high performance computers. The reliability enhancement technique presented in this work is based on using a Concurrent Error Detection (CED) based reliable XOR-XNOR circuit implementation to detect permanent and transient faults in ALUs during normal operation in order to improve the reliability of highly critical computer systems. The proposed design is performed using the 32 nm process technology.

Keywords: XOR-XNOR circuits, Concurrent Error Detection, fault-secure property, self-testing property, fault model.

1 Introduction

With the continuous increase of integration densities and complexities, IC design has become a real challenge to ensure the necessary level of quality and reliability especially for high performance applications [1-2]. Thus, computer systems used for instrumentation, measurement, and advanced processing in safety-critical applications like avionic, automotive and biomedical applications require high reliable ICs to

ensure the accuracy of analytical data they process [3]. In fact, a microprocessor is an internal hardware component that performs the mathematical calculations required for computers to run programs and execute commands while ALUs in microprocessors are combinatorial circuits allowing computers to add, subtract, multiply, divide and perform other logical operations at high speeds. Thanks to advanced ALUs, modern microprocessors are able to perform very complicated operations which make ALUs among the essential elements of computers. Consequently, designing efficient reliable ALUs is an important challenge in computer-based safety-critical systems [4]. Thus approaches and techniques to increase the reliability of these digital blocks are gaining more importance.

Interest in on-line error detection continues to grow as VLSI circuits increase in complexity [5]. The property of verifying the results delivered by a circuit during its normal operation is called Concurrent Error Detection (CED) [6]. Concurrent checking is increasingly becoming a suitable characteristic thanks to its ability to detect transient faults that may occur in a circuit during normal operation. CED also provides an opportunity for self-diagnosis and self-correction within a circuit design, especially in specific applications domains requiring very high levels of reliability [4]

Since XOR-XNOR circuits are basic building blocks in Arithmetic Logic Units, the performance and reliability of these digital circuits is affected by the individual performance of each XOR-XNOR included in them [7-8]. Thus, XOR-XNOR circuits should be designed such that they indicate any malfunction during normal operation. In this paper, we propose a CED based reliable new design XOR-XNOR circuit implementation using the 32 nm process technology. The circuit is analysed in terms of fault-secure and self-testing properties with respect to the set of fault models including logical stuck-at faults, transistor stuck-on and transistor stuck-open faults.

The organization of this manuscript is as follows: the CED based reliable circuits technique is first presented in Section 2, followed by the proposed XOR-XNOR circuit implementation in Section 3. Finally, the circuit's fault analysis with all parasitic is illustrated in Section 4.

2 The CED based reliable circuits

Concurrent error detection verifies the results delivered by a circuit during its normal operation. Concurrent error can be achieved by means of duplication and comparison. However, this technique requires more than 100% hardware overhead [9]. In fact, the CED technique presented in this paper is achieved by means of output duplication technique. The output of a circuit has a certain property that can be monitored by a checker. If an error causes a violation of the property, the checker gives an error indication signal [10]. The concurrent error detection property can be used for verifying the fault secure or/and the self-testing properties for circuits requiring high level of reliability and availability.

The Fault-Secure property: A circuit is fault-secure for a set of faults, if for any valid input code word and any single fault, the circuit either produces an invalid code word on the output or doesn't produce the error on the output [4]. In fact, ensuring the fault-secure property is essential for achieving safety and reliability in critical systems. Another useful property is the self-testing one.

The Self-Testing property: For each modelled fault there is an input vector occurring during normal operation that produces an output vector which do not belong to the output code. This property avoids the existence of redundant faults. If the circuit is both fault-secure and self-testing it is said Totally Self Checking (TSC property) [9]. The concept of TSC circuits was first proposed in [11] and then generalized and detailed in [12]. Thus, the combination of the fault secure and the self-testing properties offers the highest level of protection. The fault secure property is the most important one, since it guarantees error detection under any single fault, but it is also the most difficult to achieve [9].

3 The proposed XOR-XNOR circuit implementation

In this paper, a novel XOR-XNOR circuit designed in modified pass transistor logic is presented. This gate has dual inputs (A, A~, B and B~) and generates dual outputs (XOR, XNOR). The circuit implementation is performed with six MOS transistors. In the current XOR-XNOR circuit implementation, errors caused by faults will be detected only by checking the complementarity principle between the XOR and XNOR functions. The proposed XOR-XNOR circuit and the correspondent layout are respectively given by Fig. 1 and Fig. 2.

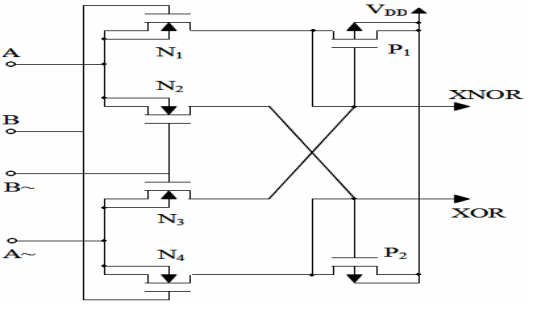

Fig. 1. The proposed XOR-XNOR circuit implementation

The XOR-XNOR circuit is implemented in full-custom 32 nm technology [13]. SPICE simulations of the circuit extracted from the layout, including parasitic, are used to demonstrate that the circuit has an acceptable electrical behaviour.

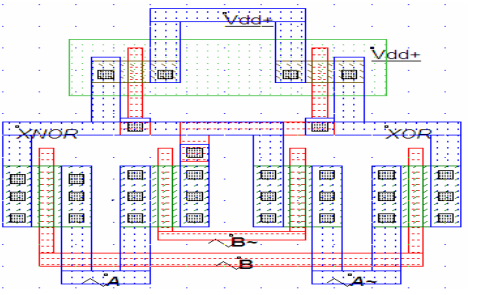

Fig. 2. Layout of the XOR-XNOR circuit in full-custom 32 nm process technology

SPICE simulation of the circuit without any fault is illustrated by Fig. 3.

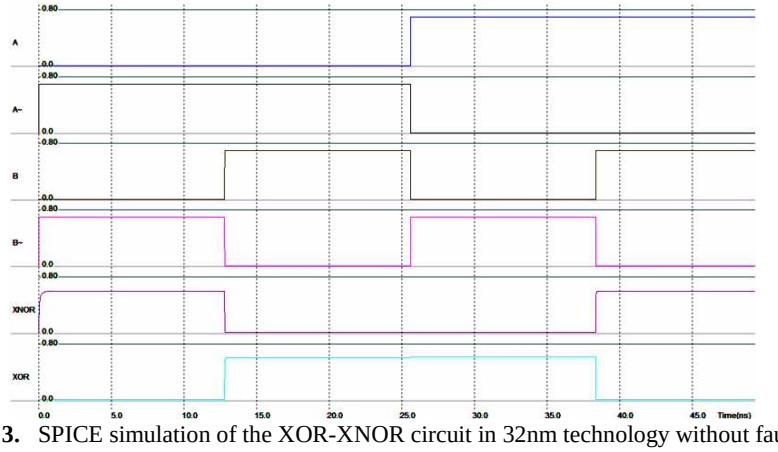

Fig. 3. SPICE simulation of the XOR-XNOR circuit in 32nm technology without faults

In Fig.3, we can remark that XOR and XNOR the outputs obtained by simulating the fault-free XOR-XNOR circuit are complementary.

4 The XOR-XNOR Circuit Fault Analysis

In the following sub-sections, we analyse the behaviour of the proposed XOR-XNOR circuit in terms of fault-secure and self-testing properties with respect to the set of fault models including logical stuck-at faults, transistor stuck-on and transistor stuck-open faults.

4.1 The stuck-at fault model

The most common model used for logical faults is the single stuck-at fault. It assumes that a fault in a logic gate results in one of its inputs or the output is fixed at either a

logic 0 (stuck-at-0) or at logic 1 (stuck-at-1) [14]. In the following, we analyze the behaviour of the XOR-XNOR gate shown in Fig. 1 in terms of fault secure and self-testing properties with respect to the logical stuck-at faults. For inputs, we consider the logical stuck-at fault model. Table 1 gives the response of the gate for all inputs combinations.

Table 1. The Gate Response for all inputs combinations.

A	A~	B	B~	XOR	XNOR	Conclusion
0	0	0	0	1	1	Multiple fault (detected)
0	0	0	1	0	0	Single fault (detected)
0	0	1	0	0	0	Single fault (detected)
0	0	1	1	0	0	Multiple fault (detected)
0	1	0	0	1	1	Single fault (detected)
0	1	0	1	0	1	Valid input
0	1	1	0	1	0	Valid input
0	1	1	1	0	0	Single fault (detected)
1	0	0	0	1	1	Single fault (detected)
1	0	0	1	1	0	Valid input
1	0	1	0	0	1	Valid input
1	0	1	1	0	0	Single fault (detected)
1	1	0	0	1	1	Multiple fault (detected)
1	1	0	1	1	1	Single fault (detected)
1	1	1	0	1	1	Single fault (detected)
1	1	1	1	1	1	Multiple fault (detected)

From Table 1, we can conclude that for primary logical stuck-at faults, all single and multiple faults on primary inputs will result in a non-valid code by producing no complementary outputs. In fact, each fault will be detected when there are non complementary (XOR, XNOR) outputs, because normally XOR and XNOR should be complementary data. Consequently, the proposed circuit is fault-secure and self-testing for single and multiple stuck-at faults.

In addition, by analyzing the table above we can remark that when a fault type stack-at occurs, in the major case, it will affect the XOR output. In fact, when such faults occur we will obtain a faulty XOR and a fault-free XNOR output for all cases if the input A is equal to the low level. Otherwise, if the input A is equal to the high level we will obtain a faulty XOR output only when the logic product A~B is equal to the

high level. Thereby, this remark can give us lots of ideas to consider when designing an error correction approach to ensure the fault tolerance property in the current XOR-XNOR circuit implementation. Next, we consider the stuck-on and stuck-open transistor fault model. We will examine all possible single transistor stuck-on and transistor stuck-open faults within the circuit of Fig. 1 in next two sub-sections.

4.2 The transistor stuck-on fault model

A transistor stuck-on fault may be modelled as a bridging fault from the source to the drain of a transistor [14]. In order to analyse the circuit behaviour in the presence of stuck-on faults with realistic circuit defects, we simulate the considered XOR-XNOR circuit in the presence of faults. Faults are manually injected in the circuit layout of Fig. 2.

Table 2. The Gate Response for Transistor Stuck-on faults.

Transistor Stuck-on	Input vectors detecting the fault A B	XOR	XNOR
N1	0 0	0	0
	1 0	1	1
N2	0 1	0	0
	1 1	1	1
N3	0 1	1	1
	1 1	0	0
N4	0 0	1	1
	1 0	0	0
P1	0 1	1	1
	1 0	1	1
P2	0 0	1	1
	1 1	1	1

From Table 2, we can conclude that for any valid input code word, any injected single stuck-on fault within the gate produces an invalid code word (non complementary (XOR, XNOR) outputs), therefore the Fault-Secure property is verified for this set of faults. On the other hand, the self-testing property signify that for each single stuck-on fault within the gate there is at least one input vector occurring during the circuit normal operation that detects it. In fact, by analysing the simulation results summarized in Table 2, we can say that the self-testing property is also verified for this set of faults. Thus, the combination of the fault-secure and the self-testing properties makes the circuit Totally Self Checking for the stuck-on fault model.

4.3 The transistor stuck-open fault model

A stuck-open transistor involves the permanent opening of the connection between the source and the drain of a transistor [14]. In order to analyse the circuit behaviour in the presence of stuck-open faults, faults are manually injected in the circuit layout

of Fig. 2. Let's examine the behaviour of the XOR-XNOR circuit under any single transistor open fault to make the proof that it is fault secure for this class of faults. Given that the XOR-XNOR circuit contains six transistors, there are six possible transistor open faults. SPICE simulation results of the circuit obtained by rendering the NMOS transistor N1 stuck-open are illustrated by Fig. 4.

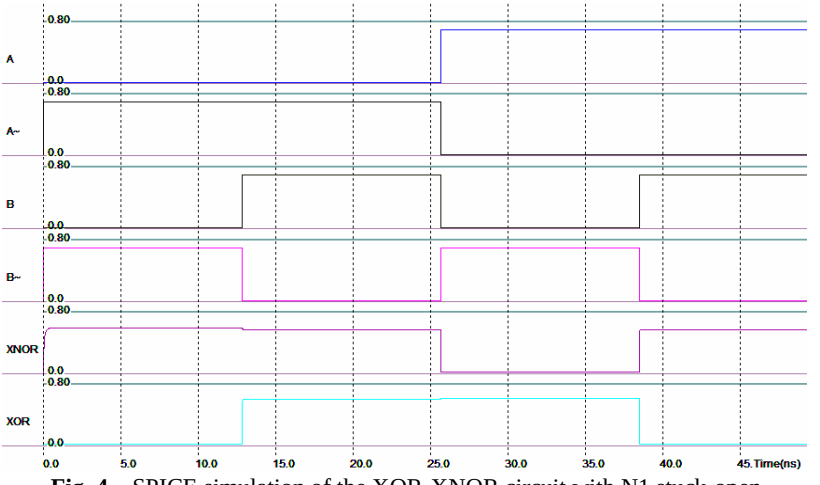

Fig. 4. SPICE simulation of the XOR-XNOR circuit with N1 stuck-open

In Fig. 4, we show that for the combination (0,0), (1,0) and (1,1) of the inputs (A,B) the circuit does not produce any error and both XOR and XNOR outputs are fault-free while for the combination (0,1) the circuit produce a fault-free XOR and a faulty XNOR. In fact, the Fault secure property require that for any valid input code word, any single transistor open fault within the gate produces an invalid code word on the output or does not produce an error on the output. Knowing that the considered fault will be detected because normally XOR and XNOR should be complementary data, we are sure that the fault secure property will not be lost. In the same way, we have simulated all possible single stuck-open faults within the XOR-XNOR circuit and simulation results show that the Fault-Secure property is verified for this set of faults.

Regarding the self-testing property, simulation results show that this property is verified for the NMOS transistors stuck-open. However, a stuck-open injected in any PMOS transistor (P1 or P2) don't produce any error in the circuit outputs and both XOR and XNOR outputs are fault-free. Thus, the fault will be undetectable because it has no effect on the circuit outputs. Theoretically, the self testing property is not ensured since a P1 or a P2 stuck-open transistor is undetectable but this is not catastrophic because firstly the fault-secure property is the most important one and secondly, we are sure that these two faults if they occur separately or even at the same time they have no effect on the outputs of the proposed circuit.

CONCLUSION

As modern processors and semiconductor circuits move into 32 nm technologies and below, designers face the major problem of process variations which affects the circuit performance and introduces faults that can cause critical failures. Therefore, integrated circuits are more and more required to guarantee reliability for safety-critical applications in the presence of permanent and transit faults. Thus, to cope with the growing difficulty of off-line testing, the concurrent error detection property is indispensable when designing complex nanometer VLSI circuits ALUs. This paper presents a new design 6-transistors XOR-XNOR circuit that can be used to ensure the on-line detection of faults occurring in computer systems during the manufacturing process. The proposed circuit, designed using the 32 nm CMOS technology, is analysed in terms of fault-secure and self-testing properties with respect to the set of fault models including logical stuck-at faults, transistor stuck-on and transistor stuck-open faults.

References

1. Bushnell, M., Agrawal, V.: Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits. (2002)
2. White, M., Chen, Y.: Scaled CMOS Technology Reliability Users Guide. NASA Electronic Parts and Packaging (NEPP) Program (2008)
3. Edward, W.: Performance and Reliability of Integrated Circuits within Computing Systems. EE Times design article (2011)
4. Hamdi, B., Chiraz, K., Rached, T.: Pass Transistor Based Self-Checking Full Adder. International Journal of Computer Theory and Engineering, Vol. 3, No. 5, pp. 608--616(2011)
5. Nicolaidis, M.: On-line testing for VLSI: state of the art and trends. Integration, the VLSI Journal, Vol 26, Issues 1-2, pp. 197--209 (1998)
6. Mouna, K., Chiraz, K., Belgacem, H., kalok, M., Lei, C., Lim, E.: A Concurrent Error Detection Based Fault-Tolerant 32 nm XOR-XNOR Circuit Implementation. In Proceedings of the IAENG International MultiConference of Engineers and Computer Scientists - IMECS'12, Hong Kong (2012)
7. Nicolaidis, M., Duarte, R.O., Manich, S., Figueras, J.: Fault-Secure Parity Prediction Arithmetic Operators. In IEEE Design & Test of computers, Vol. 14, pp. 60-71(1997)
8. Chowdhury, S.R., Banerjee, A., Roy, A., Saha, H.: A High Speed Transistor Full Adder Design using Novel 3 Transistor XOR Gates, In International Journal of Electronics, Circuits and Systems II, pp. 217--223 (2008)
9. Nicolaidis, M.: Carry Checking / Parity Prediction Adders and ALUs. IEEE Transactions on Very Large Scale Integration Systems, Vol.11, No.1, pp.121--128(2003)
10. Zeng, C., McCluskey, E.J.: Finite State Machine Synthesis with Concurrent Error Detection. Proc. International Test Conference, pp. 672--679(1999)
11. Anderson, D., Metze, G.: Design of totally self-checking check circuits for m-out-of-n codes. In IEEE Trans. on Computers, vol. 22, No. 3, pp. 263-269(1973)
12. Pradhan, K., Stiffler, J.: Error correcting codes and self-checking circuits in fault-tolerant computers. In IEEE Computer Magazine, Vol. 13, pp. 27--37(1980)
13. Etienne, S.: Microwind and Dsch version 3.1. INSA Toulouse, ISBN 2-87649-050-1(2006)
14. Lala, P.K.: An introduction to logic circuit testing. Morgan & Claypool, pp. 1--9(2009)