An Investigation of Concurrent Error Detection over Binary Galois Fields in CNTFET and QCA Technologies

M. Poolakkaparambil[1], J. Mathew[2], A. M. Jabir[3] and S. P. Mohanty[4]
1, 3 Dept. of Comp. Sci. & Electronics, Oxford Brookes University, UK
2 Department of Computer Science, University of Bristol, UK
4 Department of Computer Science, University of North Texas, USA

Abstract— **Permanent and temporary transient faults are the main concern in modern very large scale integrated circuits (VLSI). The main reason for such high vulnerability of the modern integrated circuit is their high integration density. Miniaturization of devices resulted in scaling their properties along with their size and thus making them a subject to induced faults and permanent faults. As the research progresses towards shrinking the technology even further to 15nm or below with potential CMOS replacement strategies such as carbon nano-tube field effect transistors (CNTFET) and quantum cellular automata (QCA) cells, the notion of fault susceptibility increases even further. Owing to these facts, this paper investigates the performance of standard concurrent error detection (CED) scheme over CNTEFETs and QCA technologies using normal basis (NB) finite field multiplier circuit as a test bench. The results are then compared with their CMOS equivalents which are believed to be the first reported attempt to the best of the authors' knowledge. The detailed experimental analysis of CMOS with CNTFET design proves that the emerging technologies perform better for error tolerant designs in terms of area, power, and delay as compared to its CMOS equivalent.**

Keywords: Finite Field, Concurrent Error Detection (CED), Normal Basis (NB) Multiplier, Carbon Nano-Tube Field Effect Transistor (CNTFET), Quantum Cellular Automata (QCA), Transient Error.

I. Introduction

Cryptography is a potential area where one needs secure and fast computation. The advancements in CMOS technology driven my Moore's law was a benefit to the crypto hardware designers until its integrity and reliability was questioned because of its susceptibility to transient and permanent faults. However, since the high integration is a much desired factor in digital ICs, its high reliability should be ensured. According to ITRS-2009 surveys, it is evident that further scaling in CMOS devices is limited by the adverse performance of the devices beyond 20nm geometry. According to the survey, the potential candidates for overcoming the scaling limitation of CMOS are CNTFETs and QCA circuits. However, the high level of device scaling in such devices makes them even more prone to the malicious transient fault based attacks and other permanent faults such as stuck-at faults. This is an unavoidable aspect in areas such as cryptography where high end reliability and integrity should be paramount [7].

Cryptography and hence the crypto hardware is an inevitable part of modern digital VLSI circuits spanning from bank transactions, digital rights management, TV set top box, smart cards, mobile communications, etc. [6]. The primary goal of crypto processor hardware is to perform encoding and decoding of secure data using one of the many crypto algorithms. The encoding and decoding operations generally contain a series of arithmetic addition, multiplication and inversion over finite fields. It has been reported that cryptography hardware dedicated in critical applications can become faulty either by deploying in natural radiation prone environment or by radiation induced attacks by someone with malicious intent. As the multiplier circuit is arguably the most complex and predominant arithmetic module in the crypto processor [8], it is likely to be the targeted part of the chip. As the scaling of devices in CNTFETs and QCAs increases even further, they will be no exception from such faults. These faults, either natural or malicious, can result in multiple bit errors at the output of the functional block. In either case, the end result may be catastrophic. The eavesdropping is done by observing the chips behavioural changes due to the transient faults. From this kind of observation, the attacker can gain a good understanding of the internal of the chip. The main advantage of doing this is that, the attacker is not permanently tampering or damaging the chip but only making it perform faulty in the presence of radiation [9].

Thus it is evident that error tolerant schemes are inevitable even in future technologies. This paper thus investigates the performance figures such as power and delay of multiple error detecting schemes over bit parallel Normal Basis (NB) GF multiplier implemented using emerging technologies such as CNTFET and QCA.

The remainder of the paper is organized as follows. Section II explains the related recent research and other radiation tolerant techniques. Section III presents the fundamental notion of error sources in finite field arithmetic circuits. Section IV introduces the promising emerging technologies that may be replacements for existing CMOS technology. A Hamming code based concurrent multiple error detection scheme is explained in Section V. Section VI presents experimental results of the CNTFET and QCA based designs and their performance compared to the CMOS counterpart. The conclusions and the future extensions of the proposed research is presented in Section VII.

II. Prior Research

This section details the state of the art multiple error correction schemes in GF multipliers and other GF circuits mainly targeted for CMOS technology. We also briefly review the fault tolerant research in CNTFET and QCA circuits.

Most of the existing approaches for detecting erroneous calculations in GF circuits are based on space redundancy. This implies replicating the functional block multiple times and checking for the correctness of the operations with the help of a voter. One example of such a space redundant scheme is the Triple Modular Redundancy (TMR). In TMR, the actual functional block is replicated three times and the output is compared for correctness with a voter [10]. If two out of three circuits agree to one result to be correct, the voter considers that as the correct result of the circuit output. The major drawback of TMR is that, the hardware overhead is at least 200%. Another drawback is that the entire reliability depends on the voter, which is not triplicated; as well as the assumption that the errors happen only in one functional block out of three. The design complexity of the voter is also non-trivial.

Another well known approach for error detection, termed as Concurrent Error Detection (CED), is based on time redundancy [11],

[12]. In CED, an additional error monitoring block is attached to the actual circuit that flags the occurrence of an error. Once the error flag is active, the functional block will roll back and recompute. This introduces a high delay penalty to the calculation that maybe unsuitable for many applications. There are also approaches reported for double error detection and single error correction known as the SEC/DED schemes. The SEC/DED schemes are based on Hamming or LDPC codes that can correct only single bit errors in the calculations [13]. But analysis shows that transient error occurring at a critical node can cause multiple output errors due to large fan-out in most practical systems. Also [13] deals with errors that occur only within the functional block whereas our scheme takes care of errors both in the functional block as well as the redundant bit generation block.

Other known but less explored approaches are based on the inherent properties of the functional block itself. One such error detection method is based on implications. It is well known that implications exist in any circuit and their violation can be used to detect error occurrences [7]. An in depth analysis of such schemes on any practically applicable circuit is not reported so far.

There has been little research done on faults and fault tolerant designs for QCA. The technique of [2], [3], [4] reports some of the causes of faults and fault tolerance in QCA based circuits. The primary cause of faults and errors in QCA seems to be due to the cell displacements and unwanted inversion during propagation. But to the best of our knowledge, this is the first effort that has been made to analyze the classical Hamming code based CED schemes in both CNTFET and QCA based designs.

III. Effect of Faults in Reliability of Galois Field Circuits

The effect of faults and their impact on the finite field circuits are investigated in this section. Normal Basis multipliers over binary extension field are considered as test bench circuits for the case study. The classical bit parallel NB multiplier structure can be considered as AND-XOR logic structure divided into two main parts. The first part generates the m^2 product terms realized with AND gates and second stage produces the multiplication result by performing XOR operations over the product terms. The final result generally has m^2 AND gates and (m^2-1) XOR gates with product terms shared between m outputs. Sharing of the AND gates depends on the primitive polynomial that is used to generate the field. Different primitive polynomial chosen for the same field can result in different multiplier structure and hence different AND gates being shared. Due to the sharing of gates, the shared product term forms a critical node of fault. A transient fault induced on such critical node thus propagates the erroneous calculation to multiple outputs thus providing a wrong computation value. Targeting such critical nodes for deliberate error injection and observations of the functional block's response can give the attacker a clue about the secret information within the chip.

For better understanding of the critical nodes and the propagation of the faults in NB multipliers, a generic NB multiplier example is shown in Fig. 1. This diagram shows the AND array and XOR array that performs the NB multiplication. Due to the modular reduction operation performed with the primitive polynomial, one or more AND gate may be shared and which in turn is part of multiple output terms. Thus by inducing fault in one of such critical shared gate can cause multiple output bits erroneous. The red highlighted path in Fig. 1 shows the erroneous critical AND gate and the multiple error caused by inducing error at that node.

The general NB multiplication can be represented as,

$$C(x) = a(x)b(x) mod P(x) \quad (1)$$

where, $a(x)$, $b(x)$ are the multiplication inputs over GF(2^m) and $P(x)$ is the primitive polynomial that defines structure of the Galois field under consideration. The multiplicands $a(x)$ and $b(x)$ are represented in NB as [16],

$$a(x) = \sum_{i=0}^{m-1} a_i \alpha^{2i} \quad (2)$$

$$b(x) = \sum_{i=0}^{m-1} b_i \alpha^{2i} \quad (3)$$

In this paper, we have considered bit-parallel NB multiplier defined over binary extended field by a trinomial primitive polynomials of the form $P(x) = x^m + x^k + 1$. In general a bit parallel NB multiplier has m^2 two input AND gates and (m^2-1) two input XOR gates. Due to their ease of implementation, they are widely used in Elliptic Curve Cryptography (ECC) processors which are well known for ensuring high security with lesser key-lengths. The interesting property of the NB multiplication is that the squaring operation is very simple in NB as it is just the shift operation [1]. As the shift operation is almost cost free in hardware, it has highly useful in much complex inversion circuits.

Fig. 2 shows the basic block diagram of the Hamming CED scheme that is used to detect multiple errors in the test bench NB multiplier circuits. In this design, we have used an additional parity bit in order to increase the Hamming distance to detect up to 3-bit errors.

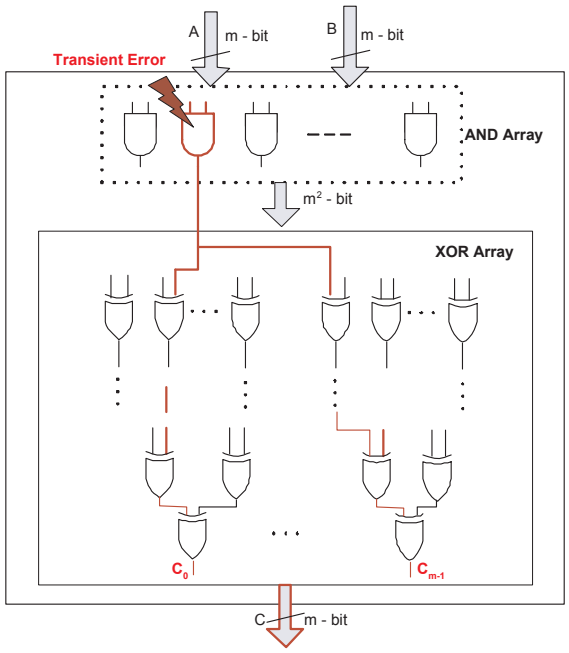

Fig. 1. Effect of transient fault in a bit-parallel NB multiplier.

Due to the limitations of the available present day EDA tools for synthesis of CNTFET and QCA circuits, the implementation results have been limited to circuits of smaller sizes and complexities.

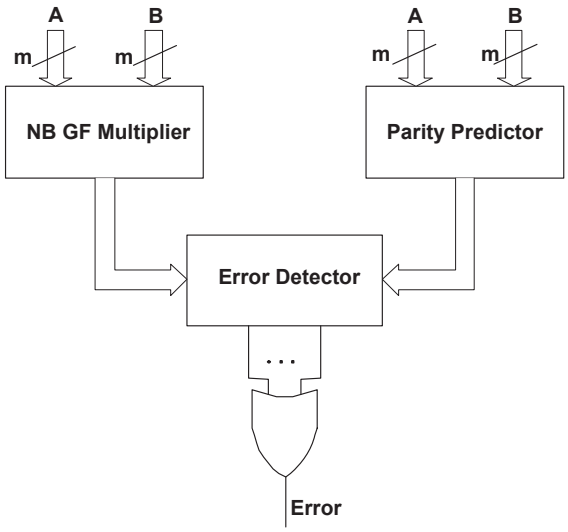

Fig. 2. Block diagram of parity based CED

However, theoretically, the designs can be extended to more complex and effective multiple error correcting architectures, e.g. in [6].

IV. Emerging Technologies

This section explores the two potential technologies that are considered to be the future replacement for the CMOS technology. The primary candidates seem to be CNTFETs and QCA. They are predominantly considered over other technologies due to their capabilities of maintaining high integration density, lower power consumptions, and lower chip area requirements.

A. CNTFET

CNTFET based circuits are reported to be high performance alternative to the existing CMOS technology in terms of area, power and speed. The first CNTFET device is manufactured in 1998 and has been widely researched to check its adaptability to replace the CMOS circuits. The CNTFET devices are preferred over CMOS devices due to many reasons. One of the reasons is the less increase NRE cost in the fabrication of such devices. This is because of the fact that, CNTFETs are similar to that of MOSFETs in physical structure except that of the conducting channel material. In CNTFETs, the bulk silicon channel material of the MOSFET is replaced by a single carbon nano-tube or by array of tubes. The in depth detail of CNTFET device properties are not discussed in this paper. The physical properties and features of CNTFETs are explained in [14].

The fundamental idea of CNTFET based circuits is to continue with the aggressive scaling in order to achieve high integration density. Typically the technology nodes for these devices are expected to be 30nm or less, potentially making the logic circuits using the CNTFETs far more susceptible to reliability compared to its CMOS equivalent. Hence, this makes the fault mitigating methods inevitable in such nano scale arithmetic logic circuits realized with CNTFET.

B. Quantum Dot Cellular Automata

Quantum Dot Cellular Automata (QCA) is another emerging technology that uses quantum cells (with cell size less than 20nm) to propagate and process information. In QCA the interconnection between the QCA logic gates is done by quantum wires that are again realized using QCA cells as compared to the metallic wires in CNTFET and CMOS technologies.

In QCA the logic is propagated because of the Coulombic interaction between the driver QCA cell and its neighboring cells. The binary logic representation and logic propagation in QCA is shown in Fig. 3. Here the black thick dots represent the electrons and void circles represent the holes or quantum dots. In Fig. 3, the thick dots on the left diagonal of the quantum cell represents logical '0' (Polarity $= -1$) and the thick dots on the right diagonal represents logical '1' (Polarity $= 1$).

Fig. 3. QCA binary logic and QCA wire.

As shown in the information flow part of Fig. 3, the electrons will try to settle down as far as possible w.r.t to its neighboring cell as a result of the electrostatic repulsion of the same polarity charge carriers. In QCA, the data flow in a circuit is controlled by QCA clocking. The QCA clocking generally has 4 stages, namely, release, relax, switch, and hold respectively. These four stages are shown in Fig. 4. In the release stage, the tunneling barrier begins to increase. In the relax stage the tunneling barrier will be high; in the switch stage the barrier starts to reduce and it will be low in the hold stage so that the logic information will be retained by the QCA cell in that particular zone.

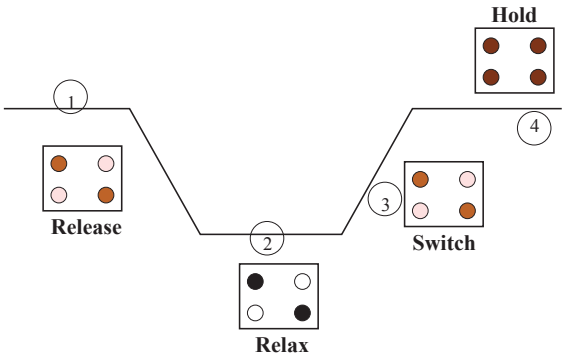

Fig. 4. QCA clocking.

The AND-XOR-OR logic gates using QCA are realized using QCA majority gates. The majority gate in principle acts as a voter that gives output as the majority of the input logic. The majority with one input set to fixed polarity $P = 1$ acts as an OR gate and as an AND gate if $P = 0$. A Majority-OR-AND gate in QCA is as shown in Fig. 5.

The XOR gate in QCA can be realized using three QCA AND gates and two inverters as shown in Fig. 6.

V. Concurrent Error Detection in Emerging Technologies

From the discussion so far, it is evident that critical application hardware such as a crypto processor is prone to transient error based attack. Fig. 1 depict a generic example to show how error or fault at one critical node may cause multiple bit errors at the output. Owing

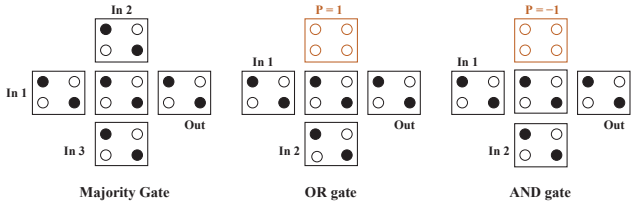

Fig. 5. QCA Gates.

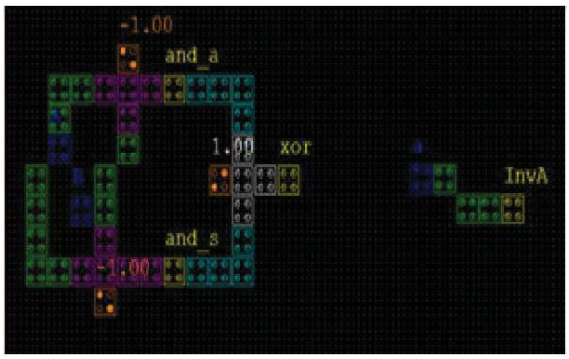

Fig. 6. QCA XOR and simple NOT gate.

to these facts, this paper investigates the performance of the error detection schemes in the potential emerging technologies. Since the emerging technologies are still under research level, there are hardly any EDA tools available for constructing complex designs. Hence this paper is limited to investigation over smaller design examples. However these may be extended to large circuits in the near future with the availability of more capable CAD tools.

A. Error Source in CNTFET Design

In CNTFET based designs, the main expected source of faulty operation can be similar to its CMOS counterpart. They are, stuck-at faults due to minute particle deposition during manufacturing, stuck-open faults due to the electron migration, or aging. There also faults that result from the third party intrusion using highly energized particle. Possibilities of such attacks are mainly reported in digital circuits used in critical applications such as cryptography where an intruder is keen on leaking out the hidden information such as a secret key.

B. Faults in Quantun Cellular Automata Designs

Even though there are designs and logic circuits that have been designed using QCA, it is not always easy and straightforward to realize all digital circuits in QCA due to unwanted cross talks and other faults in QCA cells.

As discussed in previous sections, the information carriers in QCA design are wires that are realized using QCA cells themselves. It is observed in prior research that the polarization of a QCA cell not only depends on just its adjacent cells but also on its surrounding cells. This often gives rise to unwanted data manipulation while propagation especially in wire cross overs in complex designs. The other sources of faults can be be due to the QCA cell displacement while manufacturing. A slight movement to the cell from its intended position can give rise to incorrect data. These fault sources are in addition to the error sources that we discussed in case of CNTFETs. The highly energetic radiation can also introduce transient errors in quantum dot designs [15].

These investigations hence prove that fault tolerant techniques are inevitable in current and emerging technologies. The following section explores the simple Hamming code based CED technique and its implementation in emerging technologies.

C. CED using Predicted Parity

The Hamming codes are well known and easy to implement error detecting codes generally known as single error correcting and double error detecting codes (SEC/DED). However, the Hamming codes can also detect an extra bit error if we increase the Hamming distance by adding an extra parity. In this paper 4-bit error detecting Hamming codes are considered. In practice, to detect multiple bit errors, we generate check bits (parity) from the primary input to compute the checksum for the functional block (NB multiplier) as shown in Fig. 2.

The 4 bit Hamming parity for a 4-bit multiplier circuit is as given below,

$$P1 = C0 \oplus C2 \oplus C3 \quad (4)$$

$$P2 = C0 \oplus C1 \oplus C3 \oplus C4 \quad (5)$$

$$P3 = C0 \oplus C1 \oplus C4 \quad (6)$$

$$P4 = C0 \oplus C1 \oplus C2 \oplus C4 \quad (7)$$

The generated parities and the multiplier functional block outputs are then passed on to the decoder to generate syndromes that detect the occurrence of an error. This scheme can however be easily scaled to a single error correctable scheme by just adding the Hamming decoding part.

VI. Experimental Results

This section explains the experimental results of the performance of CED in emerging technologies as compared to their CMOS equivalent. For fair comparison, CED schemes are implemented over NB multipliers of various sizes namely 1, 2, 3 and 4-bit multipliers. The circuits are modeled at gate level using 45nm CNTFET library from Stanford University and simulated for power and delay using the HSPICE simulator. For comparison purpose, we have also implemented the equivalent CMOS implementation.

The QCA based circuits are designed using QCADesigner tool from the Walus group of British Columbia University. However the tool is still under development and only functional simulation is possible with the current version of the tool. A 2-bit NB multiplier has been designed using the QCADesigner tool and CED scheme has been embedded with it as shown in Fig. 9 and Fig. 11 respectively.

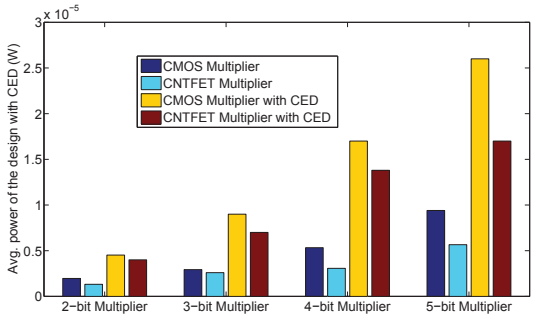

Fig. 7. Average power dissipation comparison of NB multipliers in CMOS and CNTFET with or without CED.

The power dissipation comparison of the multiplier with and without CED of the NB GF multiplier is shown in Fig. 7. The figure shows power dissipation profile of CMOS circuits with CNTFET equivalent. It clearly shows that the CNTFET based technology is significantly superior to the CMOS based implementation with lower power requirements.

Fig. 8 shows the variation of complexity of the parity prediction block as the multiplier size increases. The trend shows a considerable increase in the parity bits required as the multiplier size increases. This diagram shows the number of parity bits required for each multiplier size for a 3-bit error detection.

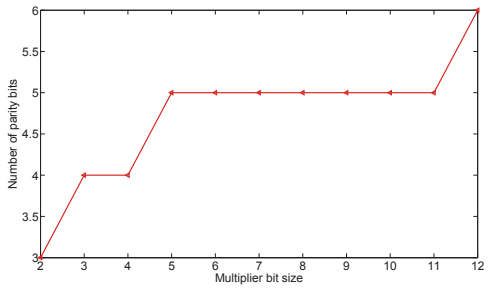

Fig. 8. Parity prediction block complexity w.r.t multiplier size.

For analysis, a QCA version of the 2-bit NB GF multiplier has been designed as shown in Fig. 9. The implementation is achieved using AND-XOR logic based on the QCA majority gates. The inverters used in the layout are the simple inverter logic as shown in Fig. 6.

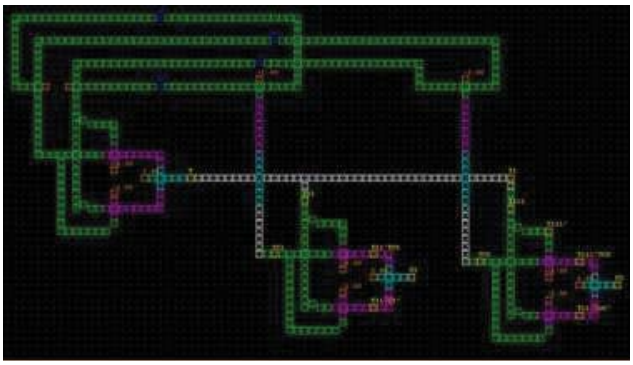

Fig. 9. 2-bit NB multiplier using QCA.

Fig. 11 shows the extended error detectable version of the Fig. 9. The various colors in the layout represent the various clocking zones of the QCA. Fig. 10 shows the functional simulation result for the 2-bit NB multiplier for one of the 4 input combination.

TABLE I
DELAY INFORMATION OF VARIOUS NB MULTIPLIERS.

No. of bits	CNTFET (sec)	CMOS (sec)
2	$1.33 * 10^{-11}$	$5.5 * 10^{-10}$
3	$1.4 * 10^{-11}$	$5.6 * 10^{-10}$
4	$1.4 * 10^{-11}$	$6.7 * 10^{-10}$
5	$1.41 * 10^{-11}$	$7 * 10^{-10}$

Fig. 10. Example Simulation of a NB QCA Multiplier.

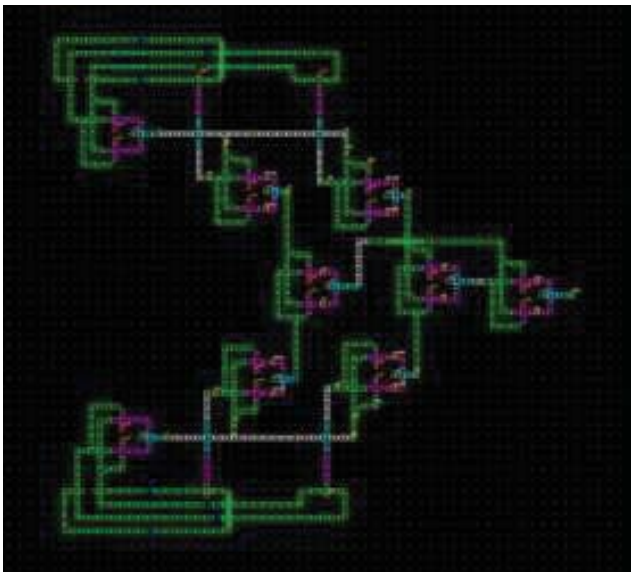

Fig. 11. 2-bit NB multiplier with CED using QCA.

The critical path delay comparison of the NB multipliers implemented in both CMOS and CNTFETs' are presented in Table I and Table II. In general the hardware complexity remains the same for any bit parallel GF multiplier circuit as they have m^2 AND gates and (m^2-1) XOR gates in general.

VII. CONCLUSIONS

Owing to the substantial scaling of devices, it is evident that the future technologies under 15nm technology may be more vulnerable towards the transient faults as it is today. VLSI circuits for critical applications such as crypto hardware realized using emerging miniature devices in CNTFETs' and QCA cells hence need to me made fault tolerant. Hence this paper investigated the performance of well known

TABLE II
DELAY INFORMATION OF NB MULTIPLIERS WITH CED.

No. of bits	CNTFET (sec)	CMOS (sec)
2	$3.2 * 10^{-11}$	$1.7 * 10^{-9}$
3	$3.65 * 10^{-11}$	$1.81 * 10^{-9}$
4	$4.15 * 10^{-11}$	$2.33 * 10^{-9}$
5	$5.1 * 10^{-11}$	$2.73 * 10^{-9}$

concurrent error detection approach in both CNTFET and WCA based NB GF circuits. To this end the paper explored error detection with CED in NB GF multipliers. The multiplier circuits were chosen for the experiments as they can be the vital and critical component for malicious attacks. As a start up phase, simple NB multiplier structures were designed over 45nm CMOS and CNTFET technologies for a fair comparison. Their power and delay are compared for the understanding of the performance of CED scheme in the emerging technologies. The scheme has also been implemented over the QCA technology to evaluate the logic performance. Due to the limitations of the available present day EDA tools for synthesis of CNTFET and QCA circuits, the implementations over CNTFET and QCA have been limited to circuits of smaller sizes and complexities. In addition, we were only able to implement the error detection capabilities owing to these limitations. Our future work include extension of the reported circuits into more complex circuits and finally towards a fault tolerant crypto processor. This includes also investigations of other fault tolerant technologies such as LDPC, multiple error correcting schemes such as BCH codes etc.

REFERENCES

[1] A. R. Masoleh and M. A. Hasan, "Efficient Digit-Serial Normal Basis Multiplier over Binary Extension Fields", ACM Trans. Embedded Computing Systems, Vol. 3, No. 3, pp. 575–592, August 2004.

[2] M. Crocker, X. Sharon Hu, M. Niemier, "Defects and Faults in QCA-Based PLAs". ACM Journal on EmergingTechnologies in Computing Systems",Vol. 5, No. 2,Article 8, 2009.

[3] X. Ma, F. Lombardi, "Fault Tolerant Schemes for QCA Systems", IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems", pp. 236–244. IEEE 2008.

[4] M. Dalui, B. Sen, B. K. Sikdar, "Fault Tolerant QCA Logic Design With Coupled Majority-Minority Gate", International Journal of Computer Applications,Vol. 1, No. 29, pp. 90–96, 2010.

[5] D. K. Pradhan, "A Theory of Galois Switching Functions", IEEE Trans. Computers, vol. 27, no. 3, pp.239–248, 1978.

[6] M. Poolakkaparambil, J. Mathew, A. Jabir, D. K. Pradhan, "BCH Code Based Multiple Bit Error Correction in Finite Field Multiplier Circuits", In Proc. IEEE/ACM Int. Symp. Quality Electronic Design ISQED 2011, pp.1–6, 2011.

[7] N. Alves, "State-of-the-art techniques for Detecting Transient Errors in Electrical Circuits", IEEE Potentials, pp.30-35, 2011.

[8] A. R. Masoleh, M. A. Hasan, "Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF(2^{m}", IEEE Trans. Computers, pp. vol. 53, no. 8, pp. 45–959, 2004.

[9] G. B. Ratnapal, R. D. Williams, T. N. Blalock, "An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks", IEEE Trans. Dependable Sec. Comput, vol. 1, No. 3, pp. 179–189, 2004.

[10] J. F. Wakerly, "Microcomputer reliability improvement using triple-modular redundancy", IEEE Proceedings, vol. 64, pp. 889–895, 1976.

[11] K. Wu, R. Kari, G. Kuznetsov, M. Gossel, "Low Cost Concurrent Error Detection for the Advanced Encryption Standard", Proceedings of the International Test Conference", pp. 1242–1248, 2004.

[12] O. Keren, "One to Many: Context Oriented Code for Concurrent Error Detection", Journal of Electronic Testing, Vol. 26, No. 3, pp. 337–353, 2010.

[13] J. Mathew, A. M. Jabir, H. Rahman, D. K. Pradhan, "Single Error Correctable Bit Parallel Multipliers Over GF(2^{m}", IET Comput. Digit. Tech., Vol.3, No.3, pp. 281–288, 2008.

[14] S. Lin, Y. B. Kim, F. Lombardi, "CNTFET-Based Design of Ternary Logic Gates and Arithmetic Circuits", IEEE Trans. Nanotechnology, Vol. 10 , Issue. 2, pp. 217–225, 2011.

[15] K. Kim, K. Wu, R. Karri, "The Robust QCA Adder Designs Using Composable QCA Building Blocks", IEEE Trans. CAD, Vol. 26 , No. 1, pp. 176–183, 2007.

[16] C. C. Wang, T. K. Truong, H. M. Shao and L. J. Deutsch, "VLSI Architectures for Computing Multiplications and Inverses in $GF(2^m)$", TDA Progress Report, pp. 52–64, July 1983.