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

M. Poolakkaparambil[1], J. Mathew[2], A. Jabir[1], & S. P. Mohanty[3]
Oxford Brookes University[1], University of Bristol[2]
University of North Texas[3]
Email: 09137484@brookes.ac.uk[1], jimson@cs.bris.ac.uk[2],
ajabir@brookes.ac.uk[1], saraju.mohanty@unt.edu[3]

Presented by
Oghenekarho Okobiah, University of North Texas.

Overview

- Motivation
- Novel Contributions
- Prior Research
- CNTFETs and QCAs
- CED over Emerging Technologies
- Experimental Results
- Conclusion & Future Work

Motivation

- Viable solution for fault tolerance is vital in critical applications.
- Requirements for fault tolerance in emerging technologies:
  - Feature size continued to decrease.
  - Critical node and operational voltage are more prone to faults.
  - Manufacturing faults is additional fault notion.
  - No deterioration in normal circuit performance.
- Fault injection based attacks in cryptography related arithmetic circuits is a major concern.
  - Emerging technologies are not safe from classical faults, hence fault tolerance is important.

Contributions of this paper

- Concurrent Error Detection (CED) with emerging technologies.
- Realization of Galois Filed (GF) circuits in both CNTFET and QCA technology.
- First known approach has been made to compare GF CED circuits on the emerging technologies and comparison with CMOS equivalent.
- Both behavioral and geometrical level implementation has been made.
- Comparison if critical parameters such power and delay with CMOS counterpart design.

Prior related research

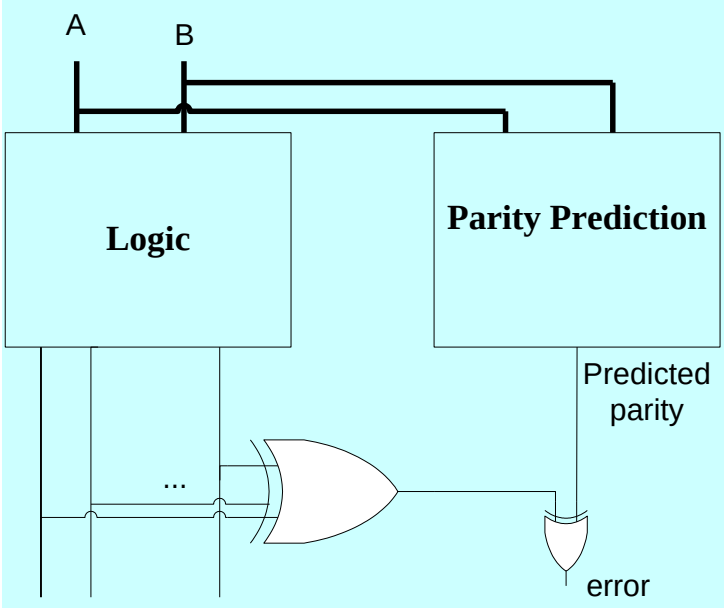


Fig 1. CED based on Parity

Ref: M. Nicoliadis , "**Carry checking/parity prediction adders and ALUs** ", IEEE Trans. VLSI Systems, vol. 11, Oct. 2003

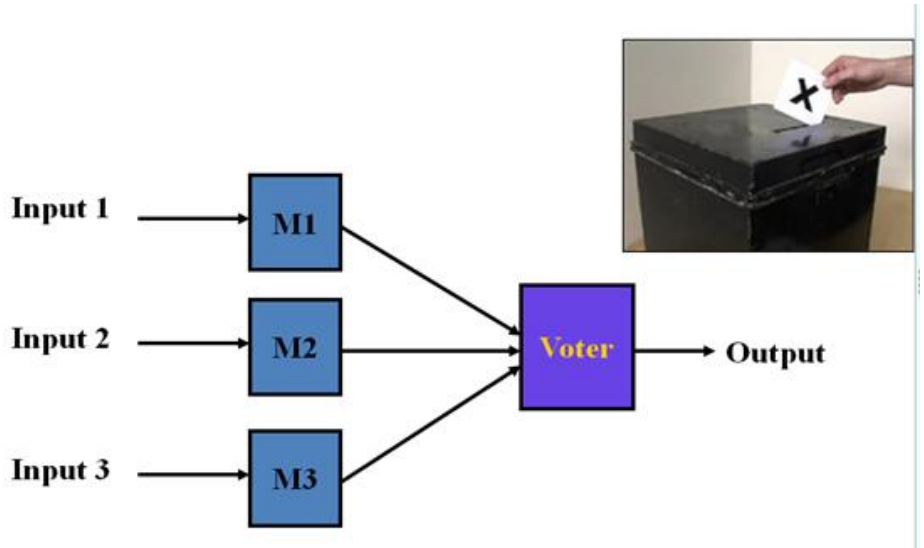


Fig 2. Triple Modular Redundancy

Error propagation in GF arithmetic circuits

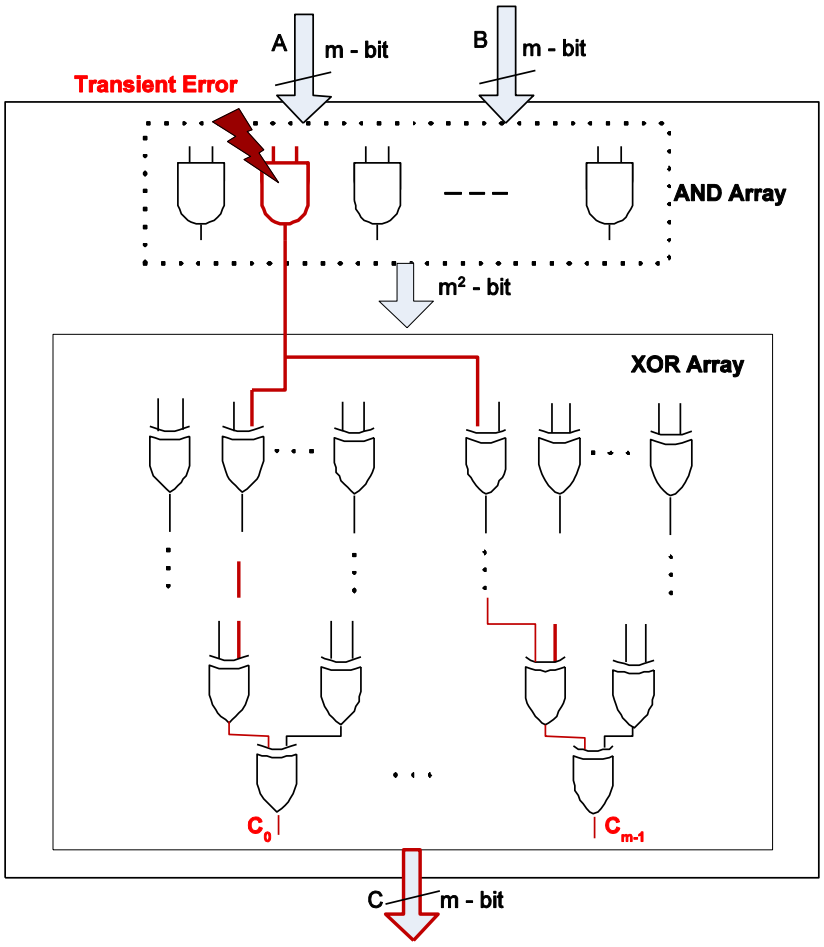


Fig 3. NB GF multiplier structure

- Natural or malicious fault on a critical node propagates to multiple outputs.
- Crypto-arithmetic circuits faces fault based attacks and manufacturing faults.
- Malicious radiation based transient attacks are more predominant in minute architecture using CNTFETs and QCAs.
- CED is the simplest way of multiple error detection.

Emerging technologies (CNTFET)

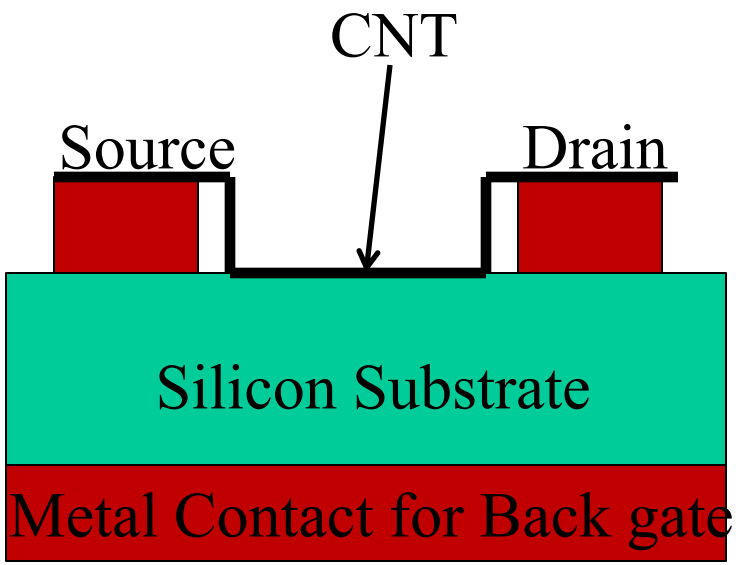


Fig 4. CNTFET

- CNTFETs are similar to CMOS except the CNT channel.
- CNT properties helps the FET to further follow Moore's law.
- Considered to be a potential replacement for CMOS.
- Less leakage power compared to CMOS counterpart.

Emerging technologies (QCA)

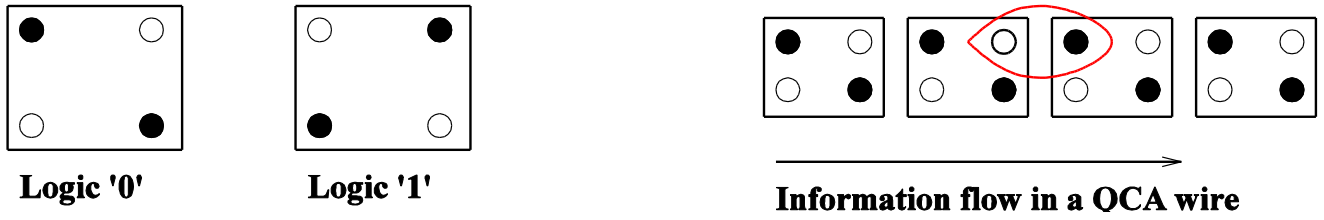


Fig 5. QCA logic and QCA wire

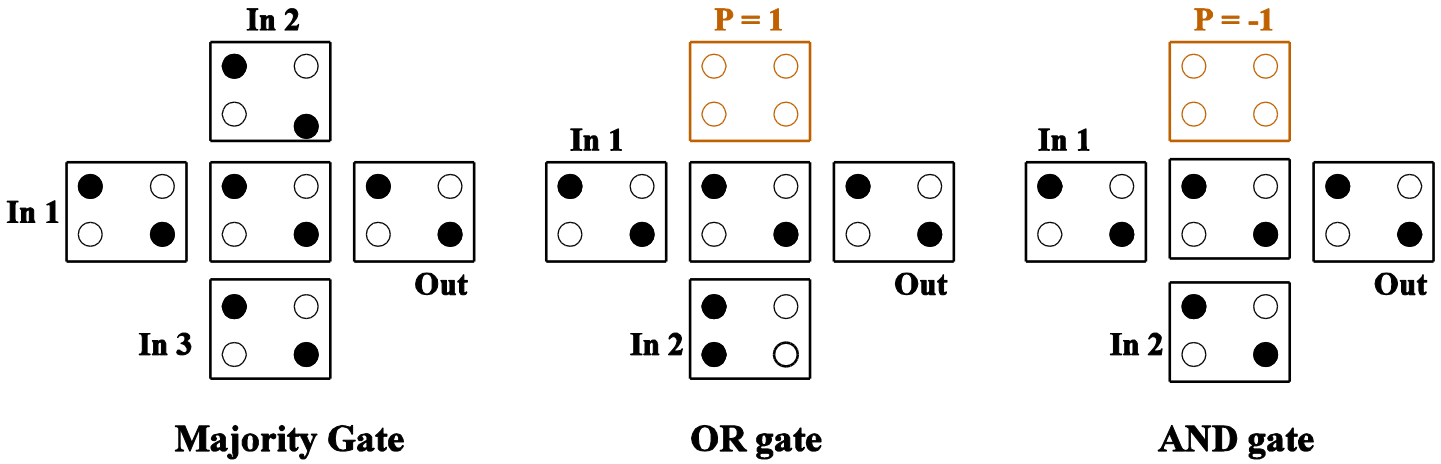


Fig 6. QCA logic gates

GF circuits uing QCA

Fig 7. 2-bit NB GF multiplier using QCA

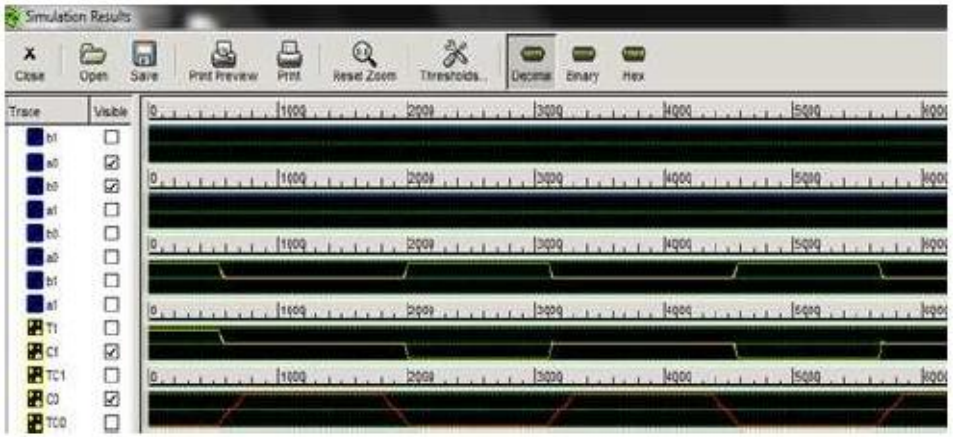
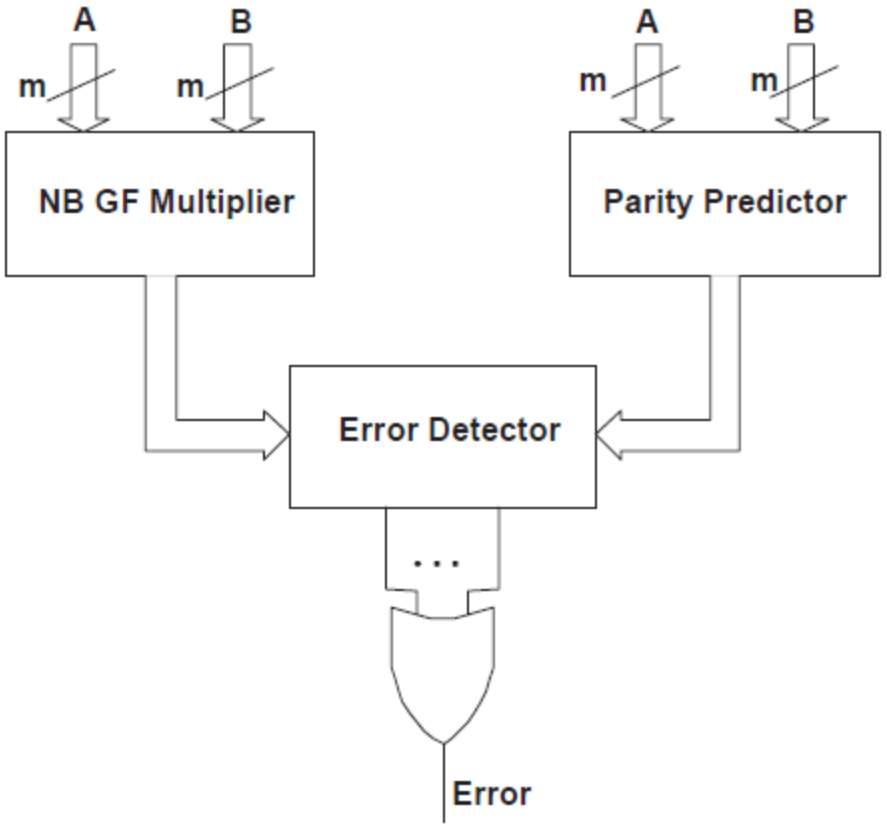


Fig 8. Functional simulation of 2-bit NB GF multiplier using QCA

Faults in Emerging Technologies

- Faults in CNTFETs are generally same as that in CMOS.
- Additional fault in CNTFETs are due to the nature of the CNT fabricated (Metallic or Semi-conducting).
- In QCA technology all components including interconnects are realized using ACA cells.
- Cell misplacements and columbic interactions of neighboring cells produce faults in QCA.
- All these notions are apart from the known existing fault sources.
- Better technology means adding more fault sources.

CED in Emerging Technologies



- NB GF multiplier is considered as a test bench circuit.
- Parity is predicted using hamming codes.
- Error detector is used to compare the prediction Vs actual computation.
- Error signal is flagged when it is appeared.

Fig 9. Concurrent error detection architecture

CED in Emerging Technologies (QCA)

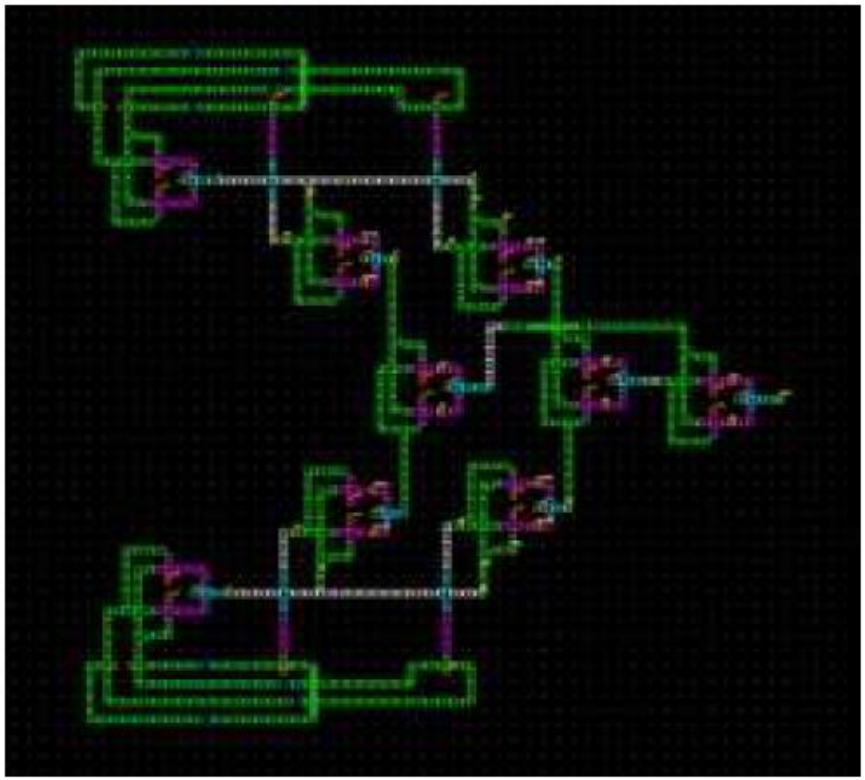


Fig 10. 2-bit NB GF multiplier with CED using QCA

Experimental Results

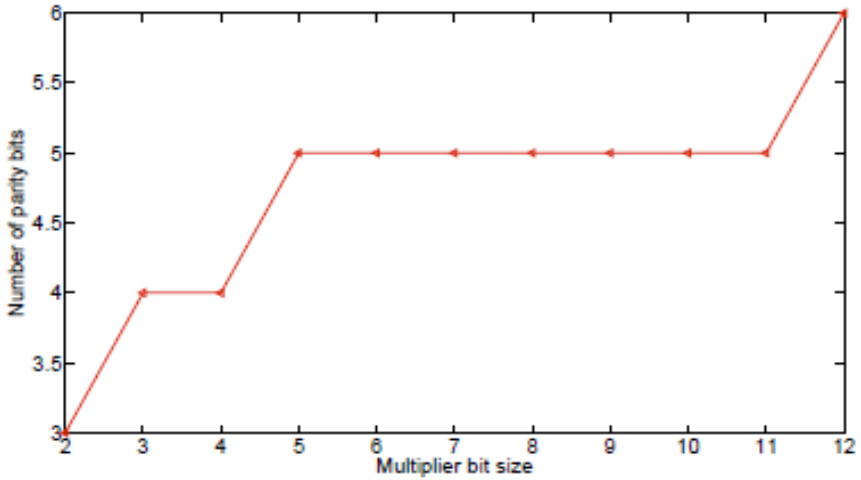


Fig 11. Parity prediction block complexity w.r.t multiplier size

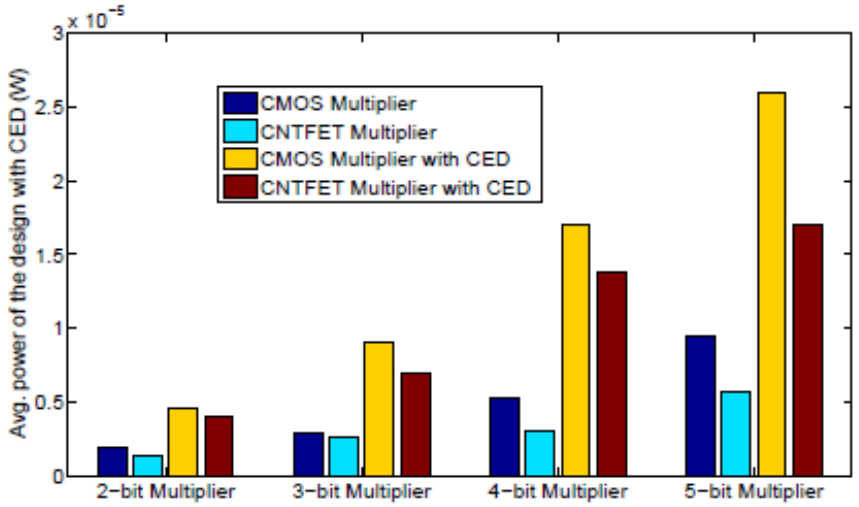


Fig 12. Average power dissipation comparison of NB multipliers in CMOS and CNTFET with or without CED.

Experimental Results

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	$1.41 * 10^{-11}$	$7 * 10^{-10}$

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	$5.1 * 10^{-11}$	$2.73 * 10^{-9}$

Conclusions

- A CED based multiple error detection scheme has been investigated over emerging technologies such as CNTFETs and QCAs.
- Hamming based error scheme is implemented for multiple error detection.
- The design is functionally verified using SPICE simulator and QCA design tool.
- Emerging technologies have been compared with CMOS in terms of power and speed.
- Though there are only small circuits designed over CNTFET and QCA, they prove to be potential followers of CMOS.
- This is the first ever reported work that initiated investigation of fault tolerant architectures for GF circuits implemented using CNTFET and QCA.
- Future work include investigation of fault tolerant schemes on other GF arithmetic circuits with increasing complexity.
- Multiple error correcting schemes will be investigated for the emerging technologies.

Thank you…

The presentation is available at:

http://www.cse.unt.edu/~smohanty/Presentations/Presentations.html