{tag} {/tag} International Journal of Computer Applications

Number 5 - Article 18

Year of Publication: 2010

Authors:

Siddharth Shelly

Babu T Chacko

10.5120/114-229

{bibtex}pxc387229.bib{/bibtex}

Abstract

With significant advances in wired and wireless technologies and also increased shrinking in the size of VLSI circuits, many devices have become very large because they need to contain several large units. This large number of gates and in turn large number of transistors causes the devices to be more prone to faults. These faults especially in sensitive and critical applications may cause serious failures and hence should be avoided. In many cryptographic schemes, the most time consuming basic arithmetic operation is the finite field multiplication and its hardware implementation for bit parallel operation may require millions of logic gates. Some of these gates may become faulty in the field due to natural causes or malicious attacks, which may lead to the generation of erroneous outputs by the multiplier. New architectures are developed to detect erroneous outputs caused by certain types of faults in bit-serial polynomial basis multipliers and digit-serial normal basis multipliers over finite fields of characteristic two. In particular, parity prediction schemes are developed for detecting errors due to single and certain multiple stuck-at faults.

Reference

- S. Fenn, M. Gossel, M Benaissa, and D. Taylor, "On Line Error Detection for Bit Serial

Multipliers in GF(2m)." Journal of electronic Testing: Theory and Applications, vol.13, pp.29-40, 1998

- B. Sunar and C. K. Koc "An Efficient Optimal Normal Basis Type II Multiplier." IEEE Trans.Computers,50(1), 83-87,Jan.2001
- Siavash Bayat-Sarmadi and M. Anwar Hasan "On Concurrent Detection of Errors in Polynomial Basis Multiplication" IEEE transactions on very large scale integration (vlsi) systems, vol. 15, no. 4, April 2007
- G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard," IEEE Trans. Computers, special issue on cryptographic hardware and embedded systems, vol. 52, no. 4, pp. 492-505, Apr. 2003
- Arash Reyhani-Masoleh and M. Anwar Hasan "Low complexity bit parallel architectures for polynomial basis multipliers over GF(2m)."IEEE Trans.Computers,vol.53,no.8,pp.945-959,AUG.2004

Index Terms

Electronics

Digital Systems

Key words

Finite fields

Polynomial basis

Normal basis

Error detection