©2010 International Journal of Computer Applications (0975 – 8887)
Volume 1 – No. 5

Fault Detection Multipliers in Polynomial and Normal Basis

Siddharth Shelly
ECE Department
Viswajyothi College of Engineering and Technology
Vazhakulam, Muvattupuzha, Ernakulam, Kerala, India.

Babu T Chacko
EEE Department
Viswajyothi College of Engineering and Technology
Vazhakulam, Muvattupuzha, Ernakulam, Kerala, India.

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.