Abstract

Residue number systems bestow a first class means for exceptionally long integer arithmetic. Their carry-free operations make parallel implementations feasible. Some applications involving very long integers, such as information security, rely heavily on fast modulo reductions. Information Security is an extensive issue and covers a huge number of crimes. In its simplest form, it is concerned with making sure that curious people cannot read or modify messages anticipated for other recipients, and Fault-tolerant computing is the art and science of building computing systems that continue to operate adequately in the presence of faults. In this paper, a generalized information security and fault tolerant system using Redundant Residue Number System (RRNS) was proposed, the theoretical result show that our proposed scheme is out performed better compared with the state of the art in term of the computation time and space, called Delay and Area respectively and also provides more security to the data.

Index Terms

Computer Science
Security
Keywords

Residue Number System (RNS), Redundant Residue Number System (RRNS), Mixed-Radix Conversion (MRC), Chinese Remainder Theorem (CRT)