Abstract

Finite field multiplication is one of the most important operation in the finite field arithmetic. This paper presents a study that compares the architectures and the performances of some of the major GF (2^m) multiplication algorithms. Hardware implementation on a reconfigurable circuit (FPGA) allowed assessment of the performance of architecture multipliers in terms of area and time complexities. Results show that serial/sequential multipliers require less area and lead to a small computational drawback, whereas parallel/combinational multipliers consume more area but are faster. Thus a trade-off between area and speed should be obtained using hybrid multipliers