Galois Field Arithmetic Unit on FPGA

Sabbir Ahmed, Jeffery Osazuwa, Howard To, Brian Weber
E.F.Charles LaBerge, Professor of the Practice, Department of Electrical and Computer Engineering

In recent years, computer technology have developed so rapidly that almost all businesses and government's agency make use of it on a daily basis. Cryptology is a continuous concern for them to protect highly confidential data. Offenders will try to steal these data from businesses in order to make profits or use it to attack political enemies in order to achieve their goals. Galois Field, also known as finite field, refers to a field in which there exists finitely many elements. It is convenient to use Galois Field to represent computer data since computer data are stored as binary forms (0 or 1) which are the components in Galois field. Representing data as a vector in a Galois Field allows mathematical operations to scramble data easily and effectively; therefor, harder for the data going to the wrong hands. The Galois Field Arithmetic algorithm was programmed with a Hardware Description Language (VHDL) and will be programmed to a Field Programmable Gate Array (FPGA). We have developed and successfully simulated a 15-bit Galois Field arithmetic algorithm with the help of software.