ABSTRACT

This thesis proposes the design of an area-efficient compact optimal normal basis field arithmetic unit (FAU) utilizing the common parts between the Massy-Omura multiplier and the Itoh - Tsugii inverter. The field arithmetic operations include addition, multiplication, and inversion. Addition can be easily implemented as an XOR of the corresponding vectors. Multiplication typically requires more computational time than addition, and it has more circuit complexity. Multiplicative inversion can be conducted by repeatedly applying the multiplication squaring algorithm. The design showed decreased hardware complexity and a decrease in the number of inputs compared to the standard approach, which makes the design very attractive when implementing elliptic curve cryptosystems in resource-constrained devices such as, smart cards, radio-frequency identification (RFID), and wireless sensor networks. The design was initially run on 173-bit input; it was then adjusted to run on 233, 350, and 515-bit inputs. The proposed design was coded using VHDL on Xilinx's ISE design suit 14.5 and simulated on an Artix7 XC7A200T field-programmable gate array (FPGA).