ABSTRACT

The current era has seen an explosive growth in communications. Applications like on-line banking, personal digital assistants, mobile communication, smartcards, etc. have emphasized the need for security in resource constrained environments. Elliptic curve cryptography (ECC) serves as a perfect cryptographic tool because of its short key sizes and security comparable to that of other standard public key algorithms. However, to match the ever-increasing requirement for speed in today's applications, hardware acceleration of the cryptographic algorithms is a necessity. As a further challenge, the designs have to be robust against side channel attacks. The thesis therefore explores FPGA designs most important field primitives are multiplication and inversion. FPGAs are reconfigurable hard-ware platforms offering flexibility and lower costs like software programs. However, designing on FPGA platforms is challenging because of the large granularity, limited resources, and large routing delay. The smallest programmable entity in an FPGA is the look up table. The arithmetic algorithms proposed in this thesis maximizes the utilization of LUTs on the FPGA.A novel finite field multiplier based on the reconfigurable Architecture is proposed. The proposed multiplier combines two variants of reconfigurable, namely the general and the simple GF SPISO multipliers. The GF SPISO multiplier has a large gate count but for small sized multiplications is compact because it utilizes LUT resources efficiently. For large sized multiplications, the simple reconfigurable architecture is efficiently as it requires lesser gates