ABSTRACT

The need for high speed processing has been increasing as a result of expanding signal processing and cryptography applications. To achieve this objective, high speed multipliers and adders (which form the core modules) are required. In addition, the different types of applications demand different performance measures such as scalability, reconfigurability, high speed, low power consumption, regularity of layout and less area or a combination of one or more of these features.

The modular exponentiation, is a common operation used in scrambling and public-key cryptosystems and involves repeated iterative application of modular multiplication. The performance of public key cryptosystems is primarily determined by the implementation efficiency of the modular multiplication and exponentiation operations. There are various reported algorithms to perform modular multiplications. The most prominent ones are Karatsuba – Ofman Algorithm, Booth Algorithm, Barrett Reduction Method, Montgomery Algorithm. In particular, Karatsuba-Ofman algorithm is considered as one of the fastest ways to multiply long integers. It is based on a divide and conquer strategy.

Vedic Mathematics is the ancient Indian Vedic System of Mathematics, rediscovered recently. The system is based on sixteen Vedic Sutras or aphorisms, which are actually word formulae describing natural ways of solving a whole range of mathematical problems. Identifying the
correct Vedic Sutras and performing multiplication operation based on the Sutra selected, can improve the speed of the multiplier significantly.

In this thesis, in the first phase, certain Vedic Sutras have been identified and applied to the existing multiplication schemes. In the second phase, the same Sutra is applied to Karatsuba Ofman modular multiplication algorithm and the performance is analysed. The FPGA implementation is carried out and the results show that Vedic Mathematics have increased speed and decreased power consumption and improved scalability.