ABSTRACT

In the present scenario of growing need of security for data, both confidentiality and authentication services of public key cryptosystems as well as the shared key methods have gained greater importance. The algorithms for shared key generation and authentication that are described in the literature are mainly extensions of some basic public key cryptosystems. However, any extension of the existing public key cryptographic algorithms to the shared key context can take large amounts of computational time and may also require high computational capabilities. Hence they must be improved a great deal before they can be used for real time applications such as smart cards and RFID's. In this work, some of these algorithms are improved using fast multiplication methods such as Montgomery multiplication and truncated polynomials. Applications of Montgomery methods with truncated polynomials, wherever appropriate, can further increase the speed of these algorithms.

In this work, some of the shared key algorithms based on RSA have been improved. A shared key version of NTRU, is given with a specific implementation based on truncated polynomials. In all these implementations and improvements Montgomery methods have been extensively used.

Apart from providing efficient methods for confidentiality, the work also focuses on methods for improving authentication. The framework for the study of authentication algorithms in this thesis is Zero knowledge protocols. The algorithm described by Fiege, Fiat and Shamir is one of the first algorithms based on zero-knowledge protocols. Montgomery methods are applied for speeding up the process of authentication. Deterministic method of authentication based on digital signature
using truncated polynomials is designed and implemented along with the probabilistic methods of zero knowledge protocols.

These new methods on shared key concepts have been illustrated with an application of data base security.