# Abstract

In the current age of information communication, security is one of the most important concern which is attracting a lot of attention from the research community. Cryptography is a pivotal method to offer security to communication of various information. Authentication and key establishment protocols are cryptographic techniques that are the first steps to set up a secure communication by authenticating the users involved and establishing a secure key among them. The key can subsequently be used to offer various security services. In this thesis various new protocols for authentication and key establishment are proposed in order to enhance efficiency and security of communication.

In the design of key establishment protocols, the use of cryptographic primitives requiring less computations are preferred to increase efficiency. Particularly, due to the popularity of applications in heterogeneous environments, protocols having less computational burden on the low power users have become essential. One of the design goals of the protocols proposed in the thesis is to provide an asymmetric computational pattern to enhance the overall efficiency. The security analysis of the protocols have been performed under provable security model.

The contributions of the thesis can be classified into three parts. In the first part, we are concerned with the analysis and design of server based two-party protocols, where a common weakness in the key control of three existing protocols has been discussed. Then a set of protocols having varying key control properties is proposed using one way hash functions. The protocols have better efficiency property compared to the existing ones.

In the second part, we have proposed a novel authenticated and contributory key agreement protocol. The protocol provides truly contributory key agreement using a polynomial interpolation based key construction. Then we have extended the protocol for communication between a set of resource constrained users connected to one/more powerful node. The protocol follows an asymmetric computation pattern and achieves better efficiency and security compared to the existing works. In order to enhance the scalability of the protocol, it has also been extended to hierarchy.

Finally, we have analyzed the security protocols for third generation GSM and CDMA mobile networks and summarized their corresponding threats. We have complemented the threats by proposing new authentication and key agreement protocols for the next generation mobile networks.

**Keywords:** Cryptography, Authentication, Key establishment protocols, Heterogeneous environment.