Preface

Nowadays, the modern cryptography uses the methodology of provable security. This methodology requires to first clearly setting out a formal model for the security of the concrete scheme. Next a “reductionist” proof is needed to show that the only way to break the scheme with a significant probability is to solve a computationally hard mathematical problem.

Another major advance in modern cryptography is pairing based cryptography. Pairings are bilinear mappings defined over groups wherein the discrete logarithm problem is hard. For the last 10-12 years, they have been found to provide plenty of applications in the design of cryptographic protocols. The most salient examples were probably the appearance of tripartite key agreement protocols and identity-based cryptography.

Note that in general, the notion of combination is very important. The combination can be performed in many ways. For example, one can simply concatenate two or more primitives (i.e. performing the first and then the second). However, in cryptographic research such simple combination is not obvious, since the combination may not preserve the security properties of each of the components. Signcryption is a one such combination of two cryptographic primitives’ signature and encryption. The original motivation for “signcryption” was to gain efficiency, namely to allow both actions to be done more efficiently than just a serial composition of the two components. This combination is naturally in numerous applications for examples secure ATM networks, secure routing in mobile ad hoc networks, encrypted email authentication by firewalls and mobile grid web services etc. Thus signcryption get much attention by researches and developed very fast in recent years. Many signcryption schemes with different mathematical basis and with additional properties are proposed. This thesis contains some developments in the research area of identity based signcryption and its variants.

Organization of the work: This thesis is divided into three parts consisting nine chapters.

Part I is Introduction, divided in three chapters. Chapter 1 gives an introductory idea about cryptography and includes the description of three important
cryptographic primitives i.e. Encryption, Digital Signature and Signcryption in public key infrastructure. In this chapter we also summarize the method of Provable Security and its ingredients. Definitions of various hard problems and intractability assumptions on which the security of our cryptographic schemes relies are also included. Chapter 2 deals with the Identity Based Cryptography. In this chapter we give definitions, various security models and concrete schemes for encryption, signature and signcryption in identity based setting related to our work. Chapter 3 contains review of literature. Many variants of identity based signcryption have been proposed in literature. We discuss these variants and their development in this chapter.

Part II is Generalized Signcryption. It contains two chapters Chapter 4 and Chapter 5 both deals with a recently proposed cryptographic primitive generalized signcryption. In Chapter 4 we discuss identity based generalized signcryption schemes and propose two new schemes. In the first scheme we give the generalization of Barreto et al. [BLMQ05] signcryption scheme. Further we simplify the security models for identity based generalized signcryption scheme and proposed most efficient scheme secure under the simplified model. In the Chapter 5 we study certificateless generalized signcryption. We review the Ji et al. [JHZ10] certificateless generalized signcryption scheme and showed that it is not insider secure. We also propose the first provable secure certificateless generalized signcryption.

Part III is other contributions. It is divided in the four chapters, deals with the different variants of identity based signcryption. In Chapter 6, we propose an efficient identity based public verifiable signcryption scheme. In Chapter 7, we review the Zhang [Zha10] and Jin et al. [JWD10] identity based signcryption schemes without random oracles and give attacks on them. Also in this chapter we propose a provably secure identity based signcryption scheme without random oracles and include public verifiability and third party verification in it and proposed first identity based signcryption scheme without random oracles with these property. In Chapter 8, we propose a new variant of identity based signcryption i.e. anonymous identity based signcryption scheme for multiple receivers. In Chapter 9, we propose an efficient and public verifiable multi signcryption scheme and we extend it for multiple receivers. We give heuristic security of these schemes.