Abstract

The aim of this paper is to provide an overview for the research that has been done so far in signcryption area. The paper also presents the extensions for the signcryption scheme and discusses the security in signcryption and the practical application of signcryption in real life. Because the elliptic curve cryptography became the newest and most efficient method for public key cryptography, it is included in this paper the implementation of signcryption scheme for elliptic curves. The main contribution to this paper represents the implementation of the signcryption algorithm with the examples provided.
- Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption)