Signcryption is a relatively new technique in public key cryptography, that perform both the functions of digital signature and encryption in a single step, in a way that is more efficient than signing and encrypting separately. Signcryption scheme can achieve authentication and encryption simultaneously, it successfully prevents mutual cheating in message transmission. In this paper a Signcryption scheme is suggested which is based on Elliptic Curve Cryptography (ECC). Main benefit of the proposed scheme is that it uses only elliptic curve for both encryption and signature generation. Message transmission is in the form of a point P(m) embedded in Elliptic Curve and encrypted by point addition which is efficient and safe. In this paper a new signature generation technique has been introduced that requires less time as compared to signature generated by hashing scheme. The signature can be verified without decryption of the message thus, provides encrypted message authentication, and hence reduces the algorithm complexity. The aim of this paper is to specify signcryption schemes on elliptic curves over finite fields, and to examine the efficiency of such schemes. Signcryption scheme based on elliptic curves represents a remarkable saving in computational cost and in communication overhead.
Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation

References

- Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption)"