Abstract

Electronic Mail or E-mail is an important development in the communication world. Therefore, the email security and efficiency has become a critical issue. Most of the existing email systems use either S/MIME (Secure/Multipurpose Internet Mail Extensions) or PGP (Pretty Good Privacy) which depend on Public Key Infrastructure (PKI) or Identity-Based Cryptography (IBC) and use inefficient signature-then-encryption techniques. Each one of these techniques has its own drawbacks. Recently, Certificateless Cryptography (CLC) and Elliptic Curve (EC) based signcryption which combines both signature and encryption in logically one step are developed to overcome these drawbacks with efficient methods. In this paper, a CLC-EC- signcryption based secure E-mail system is proposed. To make the system more efficient, the encryption key is hidden in the transmitted ciphertext itself. The system is highly secure as it uses multi-factor authentication technique includes IP address, password and fingerprint for registration and login. It provides all the security services: confidentiality, integrity, authentication, non-repudiation and forward secrecy with high efficiency compared with other recently existing
schemes. Also, it is optionally for the user to send his email in clear form or signcrypted. Finally, it is practically implemented by C# programming language and it can work on the real network system without changing in the existing network architecture.

References

5. Ays¸e G¨ul Karatop and Erkay Savas¸, "An Identity-Based Key Infrastructure Suitable for Messaging Applications" Faculty of Engineering and Natural Sciences Sabancı University Istanbul, Turkey.
22. Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)