Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. Public-key encryption schemes are secure only if the authenticity of the public-key
Secure Key Transport in Symmetric Cryptographic Protocols using some Elliptic Curves over finite fields

is assured. Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptography (ECC) schemes including key exchange, encryption and digital signature. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead. In the present paper a new technique of secure key exchange using elliptic curve cryptography is proposed.

References

- V.Miller, “Uses of Elliptic curves in Cryptography”.In advances in Cryptography (CRYPTO 1985), Springer LNCS 218,417-4 26, 1985

Index Terms

Computer Science
Security

Keywords

Elliptic Curve Cryptography
Public-key
Secret key
Encryption
Decryption