Abstract

Identification protocols have an important role for building secure communications amongst two or more entities over the internet. In this paper we introduce a new identification scheme (or money transaction protocol) based on the elliptic curve Diffie - Hellman problem. We show that our protocol meets the security attributes under the assumption that the elliptic curve discrete logarithm problem is secure.

References

- N. Koblitz, 1992. CM – Curves with good cryptographic properties, Proceedings of crypto’ 91, Santa Barbara, USA.

Index Terms

Computer Science
Security

Keywords
Identification schemes  elliptic curve Diffie – Hellman problem  secure communication  discrete logarithm problem