Abstract

Currently, short signature is receiving significant attention since it is particularly useful in low-bandwidth communication environments. In this paper, a short signature scheme is proposed from weil pairing. The proposed scheme is efficient as lesser number of cost effective pairing operations involved. We analyze security and efficiency comparison of the proposed scheme with other short signature schemes.

References

Scheme From Bilinear Pairings. Journal of telecommunication and information technology.


Index Terms

Computer Science

Pattern Recognition

Keywords

short signature; elliptic curve cryptosystem; weil pairing