AIP Conference Proceedings, vol. 1522, 2013, pages 76-79

Improvement of signature scheme based on the hybrid of two problems

Abstract

This paper proposed an improvement of an existing signature scheme based on the hybrid of two problems. The security of this improved signature scheme is based on a hybrid of factorisation (FAC) and elliptic curve discrete logarithm problem (ECDLP). This improvement provides a higher level of security than the previous scheme. In the security evaluation, different aspects of attacks from adversaries are evaluated and the scheme showed that it is secured from those attacks. In the efficiency performance evaluation, the number of keys needed, the computational complexity and the communication cost are investigated. To date, these two problems have not yet been able to be solved simultaneously, making this signature scheme secure and efficient with minimal computational cost.

Keywords

ECDLP; FAC; Hybrid; Signature scheme