Applications of finite fields in cryptography

Abstract

Attila Pethő

Department of Computer Science, University of Debrecen,
H-4002 Debrecen, P.O. Box 400, HUNGARY

Modern cryptography started in 1976 with the Diffie-Hellmann key exchange protocol, which is based on the difficulty of discrete logarithm computation. Since then finite fields play prominent role in cryptography, mainly, but not exclusively in asymmetric cryptography. In this survey talk we present algorithms and protocols based on finite fields and on elliptic as well as on hyperelliptic curves over finite fields. We discuss the state of the art of the computation of discrete logarithm and discrete elliptic logarithm, and compare the results with international standards. Proposals for post quantum cryptographic algorithms and protocols will be presented too.