

An attack on the elliptic curve discrete logarithm problem

Ayan Mahalanobis

INDIAN INSTITUTE OF SCIENCE EDUCATION

Abstract

In this talk we describe a new attack that we developed in last few years on the elliptic curve discrete logarithm problem.