Function Field Sieve Revisited

Tony Mack Robert EZOME MINTSA (Laboratoire de Recherche en Mathématiques et Applications (LAREMA), Ecole Normale Supérieure (ENS), Gabon)

Abstract: The Function Field Sieve (FFS) is an algorithm that computes discrete logarithms in a finite field extension Fqn /Fq by using intersection theory on algebraic or arithmetic surfaces. In the literature, some surfaces have been exploited to improve the original FFS for some values of the degree n. This talk aims to explain the contribution of new surfaces in order to enlarge the range of good n.