Jens Gamst 05.04.2011

Literatur zum AℓZAGK-Seminar

SS 2011

R.A. Avanzi/N.Thériault: „Index Calculus“, Ch 20 in „Handbook of Elliptic and Hyperelliptic Curve Cryptography“
H. Cohen, G. Frey eds, Chapman Hall 2006

C. Diem: „On arithmetic and the discrete logarithm problem in class groups of curves“, Habil. Schrift 2008

C. Diem: „A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties“, Diss. 2001

C. Diem: Vortragsfolien „What is Index Calculus?“ (homepage)

Kevin S. McCurley: „The discrete logarithm problem“
in „Cryptology and Computational Number Theory“,
Proc. Symp. App. Math. 42, AMS 1990

A.M. Odlyzko: „Discrete logarithms in finite fields and their cryptographic significance“ LN Computer Science 209, p 224-314 (Euro crypt 84)

C. Pomerance: „Discrete Logarithms“ (Vortragsfolien homepage)

C. Pomerance: „Elementary Thoughts on Discrete Logarithms“
in „Algorithmic Number Theory“, MSRI 44, Cambridge UP 2008

C. Pomerance: „Fast, rigorous factorization and discrete logarithm algorithms“ in „Discrete Algorithms and Complexity“, Japan-US joint-seminar 1986, Academic Press 1987.