Wissenschaftliche Publikationen (bis 2012)

Abschlussarbeiten

Elliptic Curves, Studienarbeit an der University of Edinburgh, 1998,

Das diskrete Logarithmusproblem auf elliptischen Kurven mit einem Endomorphismenring kleiner Klassenzahl, Diplomarbeit, 1999, Johann Wolfgang Goethe-Universität Frankfurt

Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation, Promotion, 2001, Universität GH Essen

Veröffentlichungen

Hyperelliptic CM-curves of genus 3, Journal of the Ramanujan Mathematical Society 16, No. 4, 2001, pp.339-372

Constructing hyperelliptic curves using complex multiplication, Conference Proceedings of the Millenial Number Theory Conference (2000), 2002, Part III, pp. 385-396

On group orders of rational points of elliptic curves, Quaestiones Mathematicae 25 (2002), p.513-525

Constructing hyperelliptic curves of genus 2 suitable for cryptography, Math. Comp. (72), 2003, p. 435-458;

Extensions and Improvements for the CM method for genus two, Fields Institute Comm., Volume 41, 2004, 379-389

Weak Fields for ECC, (mit A. Menezes und E. Teske), Topics in Cryptology -- CT-RSA 2004, LNCS 2964, p.366-386, Springer 2004

Construction of CM-Picard curve, (mit K. Koike), Math. Comp. (72), 2005, p. 499-518

Quotients of Fermat curves and a Hecke character, (mit B.v. Geemen und K. Koike), Finite Fields and Applications 11, 2005, p. 6-29

Primzahltests - von Eratosthenes bis heute (mit J. Steuding), Mathematische Semesterberichte 51, 2005, 231-252

On the number of prime divisors of the order of elliptic curves modulo p, (mit J. Steuding), Acta Arithm. 117, 2005, p. 341-352

Elliptic curves suitable for pairing based cryptography (mit F. Brezing), Design, Codes and Cryptography 37, 2005, 133-141

Point counting on Picard curve in large characteristic, (mit M. Bauer und E. Teske), Math. Comp. (74), 2005, p. 1983-2005

Generation of random Picard curves for crytography, Design, Codes and Cryptography, Volume 38, No. 3, p. 383-393, 2006

Computing generators of the tame kernel of a global function field, Journal of Symbolic Computation, Volume 41, No. 9, p.964-979, 2006

The p-adic CM-method for genus 2 curves with application to cryptography, (mit P. Gaudry, Th. Houtmann, D. Kohel, C. Ritzenthaler), Asiacrypt 2006, Lecture Notes of Computer Science 4284, p. 114-129

Das Schlüsselaustauschverfahren von Diffie und Hellmann im Unterricht, MU, Der Mathematikunterricht, Jahrgang 52, Heft 5, 2006, p. 15-29

Skripten

Ellliptische Kurven und komplexe Multiplikation (SS 2002)

Kryptographie (SS 2004)

Summary on abelian varieties with complex multiplication (Lectures at IHP, 2004)

Operations Research (2010)