

Andrej Dujella:

Applications of Elliptic Curves in Public Key Cryptography

Basque Center for Applied Mathematics and Universidad del Pais Vasco / Euskal Herriko Unibertsitatea, Bilbao, May 2011

Abstract:

The most popular public key cryptosystems are based on the problem of factorization of large integers and discrete logarithm problem in finite groups, in particular in the multiplicative group of finite field and the group of points on elliptic curve over finite field. Elliptic curves are of special interest since they at present allow much shorter keys, for the same level of security, compared with cryptosystems based on factorization or discrete logarithm problem in finite fields.

In this course we will briefly mention basic properties of elliptic curves over the rationals, and then concentrate on important algorithms for elliptic curves over finite fields. We will discuss efficient implementation of point addition and multiplication (in different coordinates), with special emphasis on fields of characteristic 2, which are important for applications in cryptography. Algorithms for point counting and elliptic curve discrete logarithm problem will be described. We intend to show how to use programs and program packages specialized for work with elliptic curves.

Factorization and primality testing and proving are very important topics for security of public key cryptosystems. Namely, the starting point in the construction of almost all public key cryptosystems is the choice of one or more large (secret or public) prime numbers. We will describe algorithms for factorization and primality proving which use elliptic curves.

Program:

1. Public Key Cryptography
 2. Elliptic curves over the rationals
 3. Elliptic curves over finite fields
 4. Implementation of operations
 5. Algorithms for determining the group order
 6. Elliptic Curve Cryptosystems
 7. Comparing elliptic curve with other types of cryptography
 8. Elliptic curve discrete logarithm problem
 9. Lenstra's elliptic curve factoring method
 10. Elliptic curve primality proving algorithm
-

Lecture Notes (working version)

References

1. I. Blake, G. Seroussi, N. Smart: [*Elliptic Curves in Cryptography*](#), Cambridge University Press, 1999.
 2. I. Blake, G. Seroussi, N. Smart (Eds): [*Advances in Elliptic Curve Cryptography*](#), Cambridge University Press, 2005.
 3. H. Cohen, G. Frey (Eds): [*Handbook of Elliptic and Hyperelliptic Curve Cryptography*](#), CRC Press, 2005.
 4. R. Crandall, C. Pomerance: *Prime Numbers. A Computational Perspective*, Springer, New York, 2001.
 5. D. Hankerson, A. Menezes, S. Vanstone: [*Guide to Elliptic Curve Cryptography*](#), Springer-Verlag, New York, 2004.
 6. N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag, Berlin, 1994.
 7. M. Rosing: [*Implementing Elliptic Curve Cryptography*](#), Manning, Greenwich, 1999.
 8. J. H. Silverman: *Elliptic curves and cryptography*, in: P. Garrett, D. Lieman (Eds.): *Public-Key Cryptography*, American Mathematical Society, Providence, 2005, pp.91-112.
 9. J. H. Silverman, J. Tate: [*Rational Points on Elliptic Curves*](#), Springer-Verlag, Berlin, 1992.
 10. N. Smart: [*Cryptography. An Introduction*](#), McGraw-Hill, 2002.
 11. D.R. Stinson: [*Cryptography. Theory and Practice*](#), CRC Press, 2005.
 12. L.C. Washington: [*Elliptic Curves: Number Theory and Cryptography*](#), CRC Press, Boca Raton, 2008.
-

Some useful links

- [High rank elliptic curves with prescribed torsion](#)
- [Infinite families of elliptic curves with high rank and prescribed torsion](#)
- [History of elliptic curves rank records](#)
- [John Cremona's home page](#)
 - [mwrank and related programs](#)
 - [Software packages of interest to number theory](#)
 - [Elliptic curve database and software](#)
- [Ian Connell's APECS](#)
- [PARI/GP home page](#)
- [SAGE Notebook](#)
- [KASH calculator](#)
- [MAGMA Calculator](#)

- [Algorithmic Number Theory: Tables and Links](#) (Noam Elkies)
 - [Joseph Silverman's home page](#)
 - [Jean-Francois Mestre's publications](#)
 - [Elliptic Curves and Cryptology](#) (people, books, theses, software)
 - [Elliptic Curves](#) (links by Franz Lemmermeyer)
 - [Certicom ECC Online Tutorial](#)
 - [Number Theory Web](#)
 - [Recommended readings for graduate students in number theory](#)
-

Web pages of some courses on elliptic curves

1. [Algorithms for Elliptic Curves](#) (Andrej Dujella)
 2. [Arithmetic of Elliptic Curves and Modular Forms](#) (Hossein Movasati)
 3. [Elliptic Curves](#) (Edray Goins)
 4. [Elliptic Curves](#) (Jim Milne)
 5. [Elliptic Curves](#) (Miles Reid)
 6. [Elliptic Curves](#) (Helena Verrill)
 7. [Elliptic Curves and Cryptography](#) (Alan Silvester)
 8. [Elliptische Kurven](#) (Franz Lemmermeyer)
 9. [Introduction to Elliptic Curves](#) (Ian Kiming)
 10. [Number Theory of Cubic Curves](#) (Jaap Top)
 11. [Rational Points on Elliptic Curves](#) (Daniel Rogalski)
 12. [Selected Topics in Number Theory](#) (Jerrold Tunnell)
 13. [Vorlesung über Elliptische Kurven und Kryptographie](#) (Wolfgang Ruppert)
-

[Andrej Dujella home page](#)