Algorithms for implementing fast arithmetic for cryptographic applications

Dr. Roberto M. Avanzi

June 28, 2004

The aim of this short course is to provide an introduction to the algorithms which are used to implement "small large-integer arithmetic", i.e. computation with the quantities of the sizes encountered in modern curve based cryptography. Most results will be presented without proofs, in order to keep the course limited to about 20-24 45-minute lessons.

Topics

1. Basic operations for large integer arithmetic.
2. Modular arithmetic and prime fields.
   (a) Residue representation of elements.
      i. Arithmetic operations.
      ii. Multiplication: Schoolbook, Comba, Karatsuba, Toom-Cook.
      iii. Lazy reduction.
      iv. Division and inversion: GCD algorithms.
   (b) Montgomery's modular multiplication without trial division,
      i. Arithmetic operations.
      ii. REDC.
      iii. Variations...
3. Fields of middle characteristic.
4. Even characteristic. Square Root.

If time permits, a short introduction to integer recordings and addition chains will be made.

Bibliography

Books

1. H. Cohen: *A Course in Computational Algebraic Number Theory.* Springer Verlag.

2. D. Hankerson, A. Menezes, and S. Vanstone: *Guide to Elliptic Curve Cryptography.* Springer Verlag 2004.

3. D. Knuth: *The art of computer programming, vol II: Seminumerical Algorithms.*

Papers (selection)

1. R. Avanzi and P. Mihăilescu: *Generic Efficient Arithmetic Algorithms for PAFFs and related algebraic structures.* Proceedings of SAC 2003. Springer Verlag 2004.

2. R. Avanzi: *Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations.* Proceedings of CHES 2004. Springer Verlag 2004.

3. C. Doche: *Redundant polynomials for binary fields.* A manuscript, 2004.

4. K. Fong, D. Hankerson, J. Lopez and A. Menezes. *Field inversion and point halving revisited.* Available from `http://www.cs.siu.edu/~kfong/research/ECCpaper.ps`. Unpublished Manuscript.

5. D. Hankerson, J. Lopez-Hernandez, and A. Menezes. *Software Implementatin of Elliptic Curve Cryprography over Binary Fields.* In: *Proceedings of CHES 2000.* LNCS 1965, pp. 1–24. Springer, 2001.

6. J. Lopez and R. Dahab: *High-Speed software multiplication in* F_{2^m}. Proceedings of INDOCRYPT 2000. 203–212.

7. P. L. Montgomery: *Modular Multiplication Without Trial Division.* Mathematics of Computation, 44(170):519–521, April 1985.