

Algebraic Curves in Cryptology

Andreas Enge, Pierrick Gaudry, François Morain
Laboratoire d'Informatique de l'École polytechnique
et INRIA Futurs

October 30, 2002

Number theory provides one of the most important sources of computationally hard problems which lay the foundations of modern cryptology: The security of RSA relies on the hardness of factoring a composite number, and the very first key-exchange algorithm in the setting of Diffie and Hellman requires the discrete logarithm problem in a finite field to be difficult. Over the past twenty years, however, there has been significant progress in factoring algorithms as well as in discrete logarithm computations. Furthermore, several security problems have been discerned related to the specific multiplicative structure of the RSA system.

It is to be expected that these first generation public key cryptosystems shall be replaced by more modern ones in the not too far future. In this mythic quest for a replacement of RSA, Europe has the unique chance of gaining technological leadership by joining its existant, already strong research competences.

Attractive candidates for replacement systems are provided by algebraic curves over finite fields, first introduced into cryptology in the form of elliptic curves by Koblitz and Miller fifteen years ago. More generally, the Jacobian, an abelian group associated to any algebraic curve, allows to implement all known discrete logarithm based cryptographic protocols. The maturity of the subject is demonstrated by the publication of several reference books [Men93, Eng99, BSS99, MOV97].

To devise robust and secure discrete logarithm based cryptosystems, for instance in Jacobians of algebraic curves, the following topics have to be addressed. Out of general security considerations, it is important to study the discrete logarithm problem itself in the class of proposed groups. Algorithms for the efficient and verifiable construction of secure problem instances have to be exhibited. Finally, efficient algorithms for realising the basic group operations are needed.

Overall security: To the best of our knowledge, the discrete logarithm problem on all but a negligible and well identified proportion of elliptic curves is of exponential complexity. For large genus hyperelliptic curves, Adleman, DeMarrais and Huang described an attack of heuristically subexponential complexity in $L(1/2)$. Further theoretical [Eng02, EG02] and practical [Gau00] analyses demonstrated that curves of genus larger than 4 should be avoided for cryptographic use.

It is thus an important task to establish an exhaustive list of classes of low genus curves. The implications of the Weil descent attack of [GHS02] on their security needs to be further studied in the light of subexponential algorithms for non-hyperelliptic curves. It is an open question whether the discrete logarithm problem on algebraic curves of high genus admits a subexponential solution of even lower complexity $L(1/3)$, as is the case for factoring.

Creation of secure curves: The main security parameter of an algebraic curve cryptosystem appears to be the group order of the Jacobian. It can be controlled by tailoring the curves via the complex multiplication method [AM93], or by counting the number of points on random curves. For elliptic curves in large characteristic, Schoof's polynomial algorithm with the improvements by Atkin and Elkies represents the state of the art [Sch95]. In small characteristic, Satoh's p -adic algorithm [Sat00] and its improvements allow computations well beyond the scope of practical cryptography. Other p -adic methods like Kedlaya's [Ked01] or Lauder and Wan's algorithms [LW01] seem to be best suited for higher genus curves.

Active fields of research include improvements of the p -adic counting algorithms, extensions of Schoof-like algorithms to higher genus curves and generalisations of the complex multiplication method to non-elliptic curves.

Implementation of the group operations: The group law on elliptic and hyperelliptic curves is well understood and can be efficiently implemented. For superelliptic and C_{ab} curves, polynomial time algorithms are described in [GPS00, Ari99, BEFG02]. It is essential to propose algorithms or even explicit formulae for all classes of curves identified as being of cryptographic relevance.

New generation algebraic curve cryptosystems: Innovative applications of algebraic curves to cryptography have been found recently, relying on structures proper to these curves for designing new cryptographic protocols. In particular, Weil and Tate pairings allow to realise identity based cryptosystems, for the first time in a secure and efficient way [cf. Nigel Smart's presentation].

Numerous problems, like the creation of secure problem instances, are only partially solved. Moreover, it may be fruitful to study further specific properties of curves with the aim of finding new paradigms and systems usable in cryptography.

References

- [AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, July 1993.
- [Ari99] Seigo Arita. Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions*, J82-A(8):1291–1299, 1999. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.
- [BEFG02] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel. Fast arithmetics for superelliptic cubics. Submitted, 2002.
- [BSS99] Ian Blake, Gadiel Seroussy, and Nigel Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1999.
- [EG02] Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 102(1):83–103, 2002.
- [Eng99] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography — An Introduction*. Kluwer Academic Publishers, 1999.
- [Eng02] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Mathematics of Computation*, 71(238):729–742, 2002.
- [Gau00] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34, Berlin, 2000. Springer-Verlag.
- [GHS02] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15:19–46, 2002.
- [GPS00] S. D. Galbraith, S. Paulus, and N. P. Smart. Arithmetic on superelliptic curves. To appear in *Mathematics of Computation*, 2000.
- [Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16(4):323–338, 2001.
- [LW01] Alan G. B. Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. Preprint, 2001.
- [Men93] Alfred Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, Boston/Dordrecht/London, 1993.
- [MOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.
- [Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, 2000.
- [Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.