Hyperelliptic Curve Cryptography

Adam Ibrahim
ai@cs.ucsb.edu

Abstract

The use of elliptic-curve groups in cryptography, suggested by Miller [1] and Koblitz [2] three decades ago, provides the same level of security for the Discrete Logarithm Problem as multiplicative groups, with much smaller key sizes and parameters. The idea was refined two years later by Koblitz, who worked with the group formed by the points of the Jacobian of hyperelliptic curves to implement Hyperelliptic Curve Cryptography (HECC) as an improvement on Elliptic Curve Cryptography (ECC) [3]. In this project we give a short introduction to hyperelliptic curves as the generalisation of elliptic curves to higher genera, define divisors and their Mumford representation, and give the group laws with Cantor's algorithm for curves of genus 2. We then show as an example how hyperelliptic curves can be used in the Digital Signature Algorithm, before discussing the advantages and drawbacks of HECC in terms of implementation and security, as well as a novel idea that strives to reap the benefits of both ECC and HECC: hyper-and-elliptic curve cryptography [4].

References

[1] V. Miller, "Use of elliptic curves in cryptography," pp. 417–426, 1986.
[2] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.
[3] N. Koblitz, "Hyperelliptic cryptosystems," *Journal of cryptology*, vol. 1, no. 3, pp. 139–150, 1989.
[4] D. J. Bernstein and T. Lange, "Hyper-and-elliptic-curve cryptography," *LMS Journal of Computation and Mathematics*, vol. 17, no. A, pp. 181–202, 2014.