Abstract for Poster Session at ANTS 2006, TU Berlin
(Peter Birkner, Technical University of Denmark)

Poster title: Efficient Arithmetic on Binary Hyperelliptic Curves

Since hyperelliptic curve cryptosystems (HECC) gain similar attention as their elliptic counterparts, it is very interesting to investigate, whether ideas and methods can be transferred from the elliptic to the hyperelliptic case. The most important operation used by elliptic curves cryptosystems (ECC) is scalar multiplication which is composed of point addition, doubling and sometimes halving. These operations are well investigated and it is likely that the present formulae are the most efficient ones. For HECC explicit formulae for addition, doubling and hence scalar multiplication of divisor classes are also known [1, 3].

The poster features a family of genus two curves over binary fields. We cover the following topics:

1. An overview of hyperelliptic curves,
2. Addition and doubling formulae for divisor classes,
3. An efficient divisor class halving algorithm for hyperelliptic curves of genus two over binary finite fields,
4. Inversion-free doubling formulae.

The main part of the presentation consists of a new efficient halving algorithm for divisor classes and of inversion-free doubling formulae. So we explain this more detailed:

Efficient halving of divisor classes offers the possibility to improve scalar multiplication on hyperelliptic curves and is also a step towards giving HECC all the features that ECC have. Halving a divisor class of a hyperelliptic curve is the reverse operation to doubling, i. e. given a divisor class D one computes another divisor class E such that $2E = D$ or slightly informal written: $\frac{1}{2}D = E$. On this poster we present an efficient divisor class halving algorithm for hyperelliptic curves of genus two over finite fields of characteristic two. Covering a large family of curves, that are of cryptographic interest, our algorithm can beat previously known techniques [2] by a factor of 2. We also show an improved version of the algorithm that can be used for repeated halving (e. g. in a halve-and-add algorithm). The proposed halving method is based on explicit doubling formulae [4] that we use to develop the halving formulae.

So far known doubling formulae for divisor classes contain at least one inversion. So, taking into account the costs of a hardware implementation of hyperelliptic curves cryptosystems it is preferable to avoid an hardware inverter. To achieve this we propose inversion-free formulae to perform the doubling operation on divisor classes.

References

[1] Roberto Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[2] Izuru Kitamura, Masanobu Katagi, and Tsuyoshi Takagi. A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two. In *Information Security and Privacy – ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 146–157. Springer-Verlag, 2005.

[3] Tanja Lange. Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328, 2005.

[4] Tanja Lange and Marc Stevens. Efficient Doubling for Genus Two Curves over Binary Fields. In *Selected Areas in Cryptography – SAC 2004*, volume 3357 of *Lecture Notes in Computer Science*, pages 170–181. Springer-Verlag, 2005.