

Hyperelliptic Cryptosystems in Practice

Christof Paar and Jan Pelzl and Thomas Wollinger

Communication Security Group — COSY
Ruhr Universität Bochum
Germany

The Hyperelliptic curve cryptosystem is one of the emerging cryptographic primitives of the last years. This system offers the same security as established public-key cryptosystems, such as those based on RSA or elliptic curves, with much shorter operand length. However, until recently the common belief in industry and in the research community was that hyperelliptic curves are out of scope for any practical application.

We were able to show the practical use of hyperelliptic curve cryptosystems (HECC) by narrowing the performance gap between elliptic curve (EC) and hyperelliptic curve cryptosystems. The complexity of the group operation for small genus hyperelliptic curves was reduced and efficient algorithms have been proposed [PWGP03, PWP03]. We developed a new metric to compare different cryptographic primitives based on the atomic operations of a processor and our theoretical comparison between elliptic curve and hyperelliptic curve cryptosystems, as well as our software and hardware implementations show that the performance of both cryptographic primitives are in the same range [P02]. Surprisingly, the hyperelliptic curve cryptosystems even outperform elliptic curves using certain curve parameters. We implemented these cryptosystems on general purpose processor and on a variety of different embedded processors, and build even a prototype implementation of a hyperelliptic curve coprocessor on FPGAs [WPWPSK04, Wol04].

References

- [Wol04] Thomas Wollinger. *Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems* Ph.D., Ruhr-University Bochum, Bochum, Germany July 2004.
- [PWGP03] Jan Pelzl and Thomas Wollinger and Jorge Guajardo and Christof Paar. *Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves* *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2003* September 2003.
- [PWP03] Jan Pelzl and Thomas Wollinger and Christof Paar. *Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves* *Tenth Annual Workshop on Selected Areas in Cryptography - SAC 2003* August 2003.
- [P02] Jan Pelzl. *Hyperelliptic Cryptosystems on Embedded Microprocessors* Diplomarbeit, Ruhr-Universität Bochum September 2002.
- [WPWPSK04] Thomas Wollinger and Jan Pelzl and Volker Wittelsberger and Christof Paar and Gokay Saldamli and Cetin Koc. *Elliptic and Hyperelliptic Curves on Embedded uP* *Special issue on Embedded Systems and Security of the ACM Transactions in Embedded Computing Systems (TECS)*