CORR 2001-25

Fast Normal Basis Multiplication Using General Purpose Processors

Arash Reyhani-Masoleh*, & M.A. Hasan*

Abstract For cryptographic applications, normal bases have received considerable attention, especially for hardware implementation. In this document, we consider fast software algorithms for normal basis multiplication over the extended binary field $GF(2^m)$. We present a vector-level algorithm which essentially eliminates the bit-wise inner products needed in the conventional approach to the normal basis multiplication. We then present another algorithm which significantly reduces the dynamic instruction counts. both algorithms utilize the full width of the data-path of the general purpose processor on which the software is to be executed. We also consider composite fields and present an algorithm which can provide further speed-ups and an added flexibility toward hardware-software co-design of processors for very large finite fields.

Keywords Finite field multiplication, normal basis, software algorithms, ECDSA, composite fields.