Cryptology ePrint Archive: Report 2011/589

Impact of Intel's New Instruction Sets on Software Implementation of $GF(2)[x]$ Multiplication

Chen Su and Haining Fan

Abstract: PCLMULQDQ, a new instruction that supports $GF(2)[x]$ multiplication, was introduced by Intel in 2010. This instruction brings dramatic change to software implementation of multiplication in $GF(2^m)$ fields. In this paper, we present improved Karatsuba formulae for multiplying two small binary polynomials, compare different strategies for PCLMULQDQ-based multiplication in the five $GF(2^m)$ fields recommended by NIST and conclude the best design approaches to software implementation of $GF(2)[x]$ multiplication.

Category / Keywords: implementation / $GF(2)[x]$ multiplication, Karatsuba Algorithm, SSE, AVX, PCLMULQDQ

Date: received 30 Oct 2011, last revised 22 Mar 2012

Contact author: sochat88 at gmail com

Available formats: PDF | BibTeX Citation

Note: Source code appended

Version: 20120322:084222 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]