Cryptology ePrint Archive: Report 2011/672

Fast and Secure Root Finding for Code-based Cryptosystems

Falko Strenzke

Abstract: In this work we analyze five previously published respectively trivial approaches and two new hybrid variants for the task of finding the roots of the error locator polynomial during the decryption operation of code-based encryption schemes. We compare the performance of these algorithms and show that optimizations concerning finite field element representations play a key role for the speed of software implementations. Furthermore, we point out a number of timing attack vulnerabilities that can arise in root-finding algorithms, some aimed at recovering the message, others at the secret support. We give experimental results of software implementations showing that manifestations of these vulnerabilities are present in straightforward implementations of most of the root-finding variants presented in this work. As a result, we find that one of the variants provides security with respect to all vulnerabilities as well as competitive computation time for code parameters that minimize the public key size.

Category / Keywords: implementation / side channel attack, timing attack, implementation, code-based cryptography

Date: received 11 Dec 2011, last revised 7 Aug 2012

Contact author: fstrenzke at crypto-source de, fstrenzke@gmx de