

Cryptology ePrint Archive: Report 2011/683

Timing Attacks against the Syndrome Inversion in Code-based Cryptosystems

Falko Strenzke

Abstract: In this work we present the first practical key-aimed timing attack against code-based cryptosystems. It arises from vulnerabilities that are present in the inversion of the error syndrome through the Extended Euclidean Algorithm that is part of the decryption operation of these schemes. Three types of timing vulnerabilities are combined to a successful attack. Each is used to gain information about the secret support, which is part of the code-based decryption keys: The first allows recovery of the zero-element, the second is a refinement of a previously described vulnerability yielding linear equations, and the third enables to retrieve cubic equations.

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

Date: received 16 Dec 2011, last revised 7 Aug 2012

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

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20120807:144920 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]