Cryptology ePrint Archive: Report 2011/683

Timing Attacks against the Syndrome Inversionin Code-based Cryptosystems

Falko Strenzke

Abstract: In this work we present new timing vulnerabilities that arise in the inversion of the error syndrome through the Extended Euclidean Algorithm that is part of the decryption operation of code-based Cryptosystems. We analyze three types of timing attack vulnerabilities theoretically and experimentally: The first allows recovery of the zero-element of the secret support, the second is a refinement of a previously described vulnerability yielding linear equations about the secret support, and the third enables to retrieve non-linear equations about the secret support. Furthermore, we analyze theoretically the limitations applying to actual attacks based on the information gained in such manner.

Category / Keywords: implementation / ide channel attack, timing attack, post quantum crypto-graphy, code-based cryptography

Date: received 16 Dec 2011

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

Available formats: PDF | BibTeX Citation

Version: 20111218:214747 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]