Cryptology ePrint Archive: Report 2011/388

Modulus Fault Attacks Against RSA-CRT Signatures

Eric Brier and David Naccache and Phong Q. Nguyen and Mehdi Tibouchi

Abstract: RSA-CRT fault attacks have been an active research area since their discovery by Boneh, DeMillo and Lipton in 1997. We present alternative key-recovery attacks on RSA-CRT signatures: instead of targeting one of the sub-exponentiations in RSA-CRT, we inject faults into the public modulus before CRT interpolation, which makes a number of countermeasures against Boneh et al.'s attack ineffective.

Our attacks are based on orthogonal lattice techniques and are very efficient in practice: depending on the fault model, between 5 to 45 faults suffice to recover the RSA factorization within a few seconds. Our simplest attack requires that the adversary knows the faulty moduli, but more sophisticated variants work even if the moduli are unknown, under reasonable fault models. All our attacks have been fully validated experimentally with fault-injection laser techniques.

Category / Keywords: implementation / Fault Attacks, Digital Signatures, RSA, CRT, Lattices

Publication Info: An extended abstract will appear in the proceedings of CHES 2011. This is the full version.

Date: received 18 Jul 2011, last revised 28 Jul 2011

Contact author: mehdi tibouchi at normalesup org

Available formats: PDF | BibTeX Citation

Version: 20110728:132622 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]