Cryptology ePrint Archive: Report 2011/709

Fault Attack against Miller's algorithm

Nadia El Mrabet

Abstract: We complete the study of [23] and [27] about Miller's algorithm. Miller's algorithm is a central step to compute the Weil, Tate and Ate pairings. The aim of this article is to analyze the weakness of Miller's algorithm when it undergoes a fault attack. We prove that Miller's algorithm is vulnerable to a fault attack which is valid in all coordinate systems, through the resolution of a nonlinear system. We highlight the fact that putting the secret as the rst argument of the pairing is not a countermeasure. This article is an extensed version of the article [15].

Category / Keywords: public-key cryptography / Pairing Based Cryptography, Side Channel Attacks, Fault attacks

Publication Info: Extended version of citation [15].

Date: received 29 Dec 2011

Contact author: elmrabet at ai univ-paris8 fr

Available formats: PDF | BibTeX Citation

Version: 20111231:155223 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]