Cryptology ePrint Archive: Report 2011/181

Security of Prime Field Pairing Cryptoprocessor Against Differential Power Attack

Santosh Ghosh, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury

Abstract: This paper deals with the differential power attack on a pairing cryptoprocessor. The cryptoprocessor is designed for pairing computations on elliptic curves defined over finite fields with large prime characteristic. The work pinpoints the vulnerabilities of such pairing computations against side-channel attacks. By exploiting the power consumptions, the paper experimentally demonstrates such vulnerability on FPGA platform. A suitable counteracting technique is also suggested to overcome such vulnerability.

Category / Keywords: implementation / Pairing Based Cryptography, Side-channel Analysis, Power Analysis Attack, DPA Attack, Prime Fields.

Date: received 7 Apr 2011

Contact author: santosh ghosh at gmail com

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20110408:134245 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]