Cryptology ePrint Archive: Report 2011/178

Differential Fault Analysis of AES: Toward Reducing Number of Faults

Chong Hee KIM

Abstract: Differential Fault Analysis (DFA) finds the key of a block cipher using differential information between correct and faulty ciphertexts obtained by inducing faults during the computation of ciphertexts. Among many ciphers AES has been the main target of DFA due to its popularity. DFA of AES has also been diversified into several directions: reducing the required number of faults, applying it to multi-byte fault models, extending to AES-192 and AES-256, or exploiting faults induced at an earlier round. This paper deals with the first three directions together, especially giving weight to reducing the required number of faults. Many previous works show that the required numbers of faults are different although the same fault model is used. This comes from lack of a general method of constructing and solving differential fault equations. Therefore we first present how to generate differential fault equations systematically and reduce the number of candidates of the key with them, which leads us to find the minimum number of faults. Then we extend to multi-byte fault models and AES-192/256.

Category / Keywords: secret-key cryptography / Cryptanalysis, Side channel attacks, Differential fault analysis, Block ciphers, AES

Publication Info: Full version of the paper will be published at Information Sciences (2012).

Date: received 5 Apr 2011, last revised 20 Feb 2012

Contact author: chhkim7 at gmail com

Available formats: PDF | BibTeX Citation

Version: 20120220:101532 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]