Cryptology ePrint Archive: Report 2013/191

Improved Differential Fault Analysis on ARIA using Small Number of Faults

Yuseop Lee, Kitae Jeong, Jaechul Sung, Seokhie Hong

Abstract: In [15], Li et al. firstly proposed a differential fault analysis on ARIA-128. This attack requires average 45 random byte fault injections. In 2012, Park et al. proposed the improve DFA by using 33 random byte fault injection. Also Kim proposed differential fault analysis based on multi byte fault model. In this model, the number of fault injections is reduce to 13 and If access to the decryption oracle is allowed, only 7 faults are required. In this paper, we propose improved differential fault analysis on ARIA. Based on random byte fault model, the proposed attacks can recover the secret key of ARIA-128/192/256 by using 6 fault injections within a few minutes. Moreover, in cases of ARIA-128 and ARIA-256, it is possible to recover the secret key using only 4 fault injections under a fault assumption where an attacker can induce some faults during both encryption and decryption process, respectively. Our results on ARIA-192/256 are the first known DFA results on them.

Category / Keywords: secret-key cryptography / Differential fault analysis, Block cipher, ARIA, Cryptanalysis

Date: received 2 Apr 2013

Contact author: yusubi at korea ac kr