Cryptology ePrint Archive: Report 2013/043

Differential Fault Attack on the PRINCE Block Cipher

Ling Song and Lei Hu

Abstract: PRINCE is a new lightweight block cipher proposed at the ASIACRYPT'2012 conference. In this paper two observations on the linear layer of the cipher are presented. Based on the observations a differential fault attack is applied to the cipher under a random nibble-level fault model. The attack uniquely determines the 128-bit key of the cipher using less than 7 fault injections averagely. In the case with 4 fault injections, the attack limits the key to a space of size less than 2^{18} statistically.

Category / Keywords: secret-key cryptography / lightweight cipher, PRINCE block cipher, differential fault attack

Date: received 28 Jan 2013

Contact author: lsong at is ac cn

Available formats: PDF | BibTeX Citation

Version: 20130129:224722 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
