Cryptology ePrint Archive: Report 2013/029

A Differential Fault Attack on MICKEY 2.0

Subhadeep Banik and Subhamoy Maitra

Abstract: In this paper we present a differential fault attack on the stream cipher MICKEY 2.0 which is in eStream's hardware portfolio. While fault attacks have already been reported against the other two eStream hardware candidates Trivium and Grain, no such analysis is known for MICKEY. Using the standard assumptions for fault attacks, we show that by injecting around $2^{16.7}$ faults and performing $2^{32.5}$ computations on an average, it is possible to recover the entire internal state of MICKEY at the beginning of the key-stream generation phase.

Category / Keywords: implementation / eStream, Fault attacks, MICKEY 2.0, Stream Cipher

Date: received 21 Jan 2013

Contact author: subho at isical ac in