Cryptology ePrint Archive: Report 2011/285

Exploiting Linear Hull in Matsui's Algorithm 1 (extended version)

Andrea Röck and Kaisa Nyberg

Abstract: We consider linear approximations of an iterated block cipher in the presence of several strong linear approximation trails. The effect of such trails in Matsui's Algorithm 2, also called the linear hull effect, has been previously studied by a number of authors. However, he effect on Matsui's Algorithm 1 has not been investigated until now. In this paper, we fill this gap and examine how to exploit the linear hull in Matsui's Algorithm 1. We develop the mathematical framework for this kind of attacks. The complexity of the attack increases with the number of strong linear trails. We show how to reduce the number of trails and thus the complexity using related keys. Further, we illustrate our theory by experimental results on a reduced round version of the block cipher PRESENT

Category / Keywords: secret-key cryptography / block ciphers, linear cryptanalysis, linear hull, key recovery, Matsui's Algorithm 1

Publication Info: This is a draft full version of the paper presented at WCC 2011.

Date: received 31 May 2011

Contact author: andrea rock at aalto fi