Cryptology ePrint Archive: Report 2011/032

Corrigendum to: The Cube Attack on Stream Cipher Trivium and Quadraticity Tests

Piotr Mroczkowski and Janusz Szmidt

Abstract: In 2008 I. Dinur and A. Shamir presented a new type of algebraic attack on symmetric ciphers named cube attack. The method has been applied to reduced variants of stream ciphers Trivium and Grain- 128, reduced variants of the block ciphers Serpent and CTC and to a reduced version of the keyed hash function MD6. Independently a very similar attack named AIDA was introduced by M. Vielhaber. In this paper we develop quadraticity tests within the cube attack and apply them to a variant of stream cipher Trivium reduced to 709 initialization rounds. Using this method we obtain the full 80-bit secret key. In this way it eliminates the stage of brute force search of some secret key bits which occured in previous cube attacks. In this corrigendum to our previous paper the indexing of cubes and key bits was reversed making it consistent with other papers.

Category / Keywords: secret-key cryptography / cube attack, quadraticity tests

Date: received 18 Jan 2011

Contact author: p mroczkowski at wil waw pl