Fundamenta Informaticae 114 (2012) 309–318
DOI 10.3233/FI-2012-631
IOS Press

The Cube Attack on Stream Cipher Trivium and Quadraticity Tests*

Piotr Mroczkowski , Janusz Szmidt
Department of Cryptology
Military Communication Institute
ul. Warszawska 22A, 05-130 Zegrze, Poland
p.mroczkowski@wil.waw.pl; j.szmidt@neostrada.pl

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. Previously, a very similar attack named AIDA was introduced by M. Vielhaber, in 2007. 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.