Cryptology ePrint Archive: Report 2011/282

An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware

Itai Dinur and Tim Güneysu and Christof Paar and Adi Shamir and Ralf Zimmermann

Abstract: In this paper we describe the first single-key attack which can break the full version of Grain-128 for arbitrary keys by an algorithm which is considerably faster than exhaustive search (by a factor of about 2^{38}). It uses a new version of a cube tester, which uses an improved choice of dynamic variables to eliminate all the previously made assumptions on the key, to speed up the attack, and to simplify the final key recovery. Since it is extremely difficult to mathematically analyze the expected behavior of such attacks, we implemented it on RIVYERA, which is a new massively parallel reconfigurable hardware, and tested its main components for dozens of random keys. These tests experimentally verified the correctness and expected complexity of the attack. This is the first time a complex analytical attack is successfully realized against a full-size cipher with a special-purpose machine. Moreover, it is also the first attack that truly exploits the configurable nature of an FPGA-based cryptanalytical hardware.

Category / Keywords: secret-key cryptography / Grain-128, stream cipher, cryptanalysis, cube attacks, cube testers, RIVYERA, experimental verification.

Publication Info: Accepted to ASIACRYPT'11

Date: received 30 May 2011, last revised 18 Sep 2011

Contact author: itaid at weizmann ac il