# Cryptology ePrint Archive: Report 2011/417

**New Data-Efficient Attacks on Reduced-Round IDEA**

*Eli Biham and Orr Dunkelman and Nathan Keller and Adi Shamir*

**Abstract:** IDEA is a 64-bit block cipher with 128-bit keys which is widely used due to its inclusion in several cryptographic packages such as PGP. After its introduction by Lai and Massey in 1991, it was subjected to an extensive cryptanalytic effort, but so far the largest variant on which there are any published attacks contains only 6 of its 8.5-rounds. The first 6-round attack, described in the conference version of this paper in 2007, was extremely marginal: It required essentially the entire codebook, and saved only a factor of 2 compared to the time complexity of exhaustive search. In 2009, Sun and Lai reduced the data complexity of the 6-round attack from 2^{64} to 2^{49} chosen plaintexts and simultaneously reduced the time complexity from 2^{127} to 2^{112.1} encryptions. In this revised version of our paper, we combine a highly optimized meet-in-the-middle attack with a keyless version of the Biryukov-Demirci relation to obtain new key recovery attacks on reduced-round IDEA, which dramatically reduce their data complexities and increase the number of rounds to which they are applicable. In the case of 6-round IDEA, we need only two known plaintexts (the minimal number of 64-bit messages required to determine a 128-bit key) to perform full key recovery in 2^{123.4} time. By increasing the number of known plaintexts to sixteen, we can reduce the time complexity to 2^{111.9}, which is slightly faster than the Sun and Lai data-intensive attack. By increasing the number of plaintexts to about one thousand, we can now attack 6.5 rounds of IDEA, which could not be attacked by any previously published technique. By pushing our techniques to extremes, we can attack 7.5 rounds using 2^{63} plaintexts and 2^{114} time, and by using an optimized version of a distributive attack, we can reduce the time complexity of exhaustive search on the full 8.5-round IDEA to 2^{126.8} encryptions using only 16 plaintexts.

**Category / Keywords:** secret-key cryptography / IDEA, Meet in the middle

**Date:** received 2 Aug 2011, last revised 5 Nov 2011

**Contact author:** orr dunkelman at weizmann ac il