Cryptology ePrint Archive: Report 2011/500

Biclique Cryptanalysis of the Block Cipher SQUARE

Hamid Mala

Abstract: SQUARE, an 8-round substitution-permutation block cipher, is considered as the predecessor of the AES. In this paper, inspired from the recent biclique attack on the AES by Bogdanov et al., we present the first single-key attack on full SQUARE. First, we introduce a biclique for 3 rounds of SQUARE using the independent related-key differentials. Then, we present an attack on the full round of this cipher with a data complexity of about 2^48 chosen plaintexts and a time complexity of about 2^126 encryptions.

Category / Keywords: secret-key cryptography / Block cipher, cryptanalysis, biclique, differential, SQUARE

Date: received 14 Sep 2011, last revised 14 Sep 2011

Contact author: hamidmala2003 at yahoo com