Cryptology ePrint Archive: Report 2013/097

Biclique Cryptanalysis of the Full-Round KLEIN Block Cipher

Zahra Ahmadian and Mahmoud Salmasizadeh and Mohammad Reza Aref

Abstract: In this paper we present a biclique attack on the newly proposed block cipher KLEIN-64. We first introduce some weaknesses of the diffusion layer and key schedule of this algorithm. Then we exploit them to present a full round attack on KLEIN-64 using an asymmetric biclique. The (worst case) computations and data complexity of this attack are 2^{62.84} and 2^{39}, respectively. A modified version of this attack is also presented which is slightly faster at the expense of the data required.

Category / Keywords: secret-key cryptography / lightweight cryptography, biclique attack, KLEIN family

Date: received 21 Feb 2013

Contact author: zahraahmadian at yahoo com