Cryptology ePrint Archive: Report 2013/141

Non-isomorphic Biclique Cryptanalysis and Its Application to Full-Round mCrypton

M. Shakiba and M. Dakhilalian and H. Mala

Abstract: Biclique attack, is a new cryptanalytic technique which brings new tools from the area of hash functions to the area of block cipher cryptanalysis. Till now, this technique is the only one able to analyze the full-round AES cipher in a single key scenario. In this paper, we introduce non-isomorphic biclique attack, a modified version of the original biclique attack. In this attack we obtain isomorphic groups of bicliques, each group contains several non-isomorphic bicliques of different dimensions. Actually, these bicliques are the results of an asymmetric key partitioning which is done according to two sets of key differences. Using this technique it is possible to get a chance to expand the length of bicliques or mount an attack with less data complexity. We found out the lightweight block cipher mCrypton is an appropriate candidate to be analyzed with this technique and bicliques up to five rounds can be constructed for this block cipher. Furthermore, we use two additional minor techniques, including pre-computation/re-computation in the bicliques construction and early abort technique in the matching stage, as well as a property observed in the diffusion layer of mCrypton to obtain more improvements for the complexity of our attacks on full-round mCrypton-96 and mCrypton-128.

Category / Keywords: Biclique cryptanalysis, Asymmetric key partitioning, Non-isomorphic bicliques, Block ciphers, mCrypton

Date: received 8 Mar 2013

Contact author: mshakiba_1360 at yahoo com