# Cryptology ePrint Archive: Report 2013/028

**More on linear hulls of PRESENT-like ciphers and a cryptanalysis of full-round EPCBC-96**

*Stanislav Bulygin*

**Abstract:** In this paper we investigate the linear hull effect in the light-weight block cipher EPCBC. We give an efficient method of computing linear hulls with high capacity. We then apply found hulls to derive attacks on the full 32 rounds of EPCBC--96 and 20 rounds of EPCBC-48. Using the developed methods we revise the work of J.Y. Cho from 2010 and obtain an attack based on multidimensional linear approximations on 26 rounds of PRESENT--128. The results show that designers of block ciphers should take seriously the threat coming from the linear hull attacks and not just limit themselves to proving bounds based solely on linear characteristics.

**Category / Keywords:** secret-key cryptography / PRESENT, EPCBC, linear cryptanalysis, linear hull, multidimensional linear cryptanalysis

**Date:** received 21 Jan 2013

**Contact author:** Stanislav Bulygin at cased de