# Cryptology ePrint Archive: Report 2011/093

### Linear Cryptanalysis Using Multiple Linear Approximations

*Miia Hermelin and Kaisa Nyberg*

**Abstract:** In this article, the theory of multidimensional linear attacks on block ciphers is developed and the basic attack algorithms and their complexity estimates are presented. As an application the multidimensional linear distinguisher derived by Cho for the block cipher PRESENT is discussed in detail.

**Category / Keywords:** secret-key cryptography / block ciphers, cryptanalysis, linear cryptanalysis, secret-key cryptography

**Date:** received 24 Feb 2011

**Contact author:** kaisa nyberg at aalto fi

**Available formats:** PDF | BibTeX Citation

**Version:** 20110228:223737 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]