

# Cryptology ePrint Archive: Report 2011/619

## Multidimensional Meet-in-the-Middle Attack and Its Applications to KATAN32/48/64

*Bo Zhu and Guang Gong*

**Abstract:** This paper investigates a new approach to analyze symmetric ciphers by guessing intermediate states and dividing algorithms to consecutive sub-ciphers. It is suitable for ciphers with simple key schedules and block sizes smaller than key lengths. A thorough theoretical analysis of this multidimensional method is given, and new attacks on the block cipher family KATAN are proposed by applying this method, which can attack 175-round KATAN32, 130-round KATAN48 and 112-round KATAN64 faster than exhaustive key search.

**Category / Keywords:** Multidimensional, meet-in-the-middle, cryptanalysis, KATAN

**Date:** received 17 Nov 2011, last revised 12 Nov 2012

**Contact author:** bo zhu at uwaterloo ca

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Note:** The time complexities in previous versions were not calculated correctly.

**Version:** 20121113:051402 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]