**Rasoolzadeh, Shahram**; **Raddum, Håvard**

**Improved multi-dimensional meet-in-the-middle cryptanalysis of KATAN.** (English)

Zbl 1436.94089
Tatra Mt. Math. Publ. 67, 149-166 (2016).

Summary: We study multidimensional meet-in-the-middle attacks on the KATAN block cipher family. Several improvements to the basic attacks are explained. The most noteworthy of these is the technique of guessing only non-linearly involved key bits, which reduces the search space by a significant factor. The optimization decreases the complexity of multidimensional meet-in-the-middle attacks, allowing more rounds of KATAN to be efficiently attacked than previously reported.

**MSC:**

94A60 Cryptography



**Keywords:**

lightweight; block cipher; KATAN; meet-in-the-middle; reducing complexity.

**Software:**

KATAN; KTANTAN

**Full Text:** DOI

**References:**

[1] ISOBE, All subkeys recovery attack on block ciphers : extending meet - in - the - middle approach in : Selected Areas in Cryptography SAC th eds Lecture Notes in Springer Verlag pp, Int Conf Comput Sci 12 pp 7707– (2012)

[2] CANNIÈRE, DE KATAN and KTANTAN a family of small and efficient hardware - oriented block ciphers in Hardware and The th eds Lausanne Lecture Notes in Springer Verlag pp, Cryptogr Embed Syst Int Comput Sci 09 pp 5747– (2009)

[3] DIFFIE, Exhaustive cryptanalysis of the NBS data encryption standard IEEE, Comp Soc 10 pp 74– (1977) · Zbl 05332334 · doi:10.1109/C-M.1977.217750

[4] ZHU, Multidimensional meet - in - the - middle attack and its applications to KATAN Cryptogr, Commun 6 pp 32– (2014)

[5] KNELLWOLF, Conditional differential cryptanalysis of NLFSR - based cryptosystems in in Crypt ASIACRYPT th on the Theory and of Crypt and ed Lecture Notes in Springer Verlag pp, Adv Int Conf Appl Inform Sec Comput Sci 10 pp 6477– (2010)

[6] FUHR, Match box meet - in - the - middle attack against KATAN in Workshop on Fast Software Encr FSE Lecture Notes in Springer Verlag pp, Int Comput Sci 14 pp 8540– (2015)

[7] ALBRECHT, An all - in - one approach to differential cryptanalysis for small block ciphers in : Selected Areas in Cryptography SAC th eds Lecture Notes in Springer Verlag pp, Int Conf Comput Sci 12 pp 7707– (2012)

[8] ISOBE, Improved all - subkeys recovery attacks on FOX KATAN and SHACAL block ciphers in Workshop on Fast Software Encr FSE Lecture Notes in Springer Verlag pp, Int Comput Sci 14 pp 8540– (2015)