Cryptology ePrint Archive: Report 2011/619

Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2

Bo Zhu and Guang Gong

Abstract: This paper investigates a new approach to analyze symmetric ciphers by dividing the algorithms to consecutive sub-ciphers and then evaluating them separately. This attack is suitable for ciphers with simple key schedules and having block sizes smaller than key lengths. We have successfully applied this multidimensional approach to the block ciphers, GOST and KTANTAN32/48/64, and found attacks with time complexities less than all existing results. An attack on full Hummingbird-2 faster than exhaustive search but requiring large memory is also constructed by using this method. Most importantly, a security requirement for lightweight block cipher designs is proposed, which shows, for example, GOST is as secure as claimed only when its number of rounds is larger than or equal to 40.

Category / Keywords: Multidimensional Meet-in-the-Middle, cryptanalysis, GOST, KTANTAN, Hummingbird

Date: received 17 Nov 2011, last revised 17 Feb 2012

Contact author: bo zhu at uwaterloo ca

Available formats: PDF | BibTeX Citation

Note: added authors' names to the noname version

Version: 20120218:000951 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]