Cryptology ePrint Archive: Report 2011/423

Linear Cryptanalysis of PRINTcipher --- Trails and Samples Everywhere

Martin Ågren and Thomas Johansson

Abstract: PRINTcipher is a recent lightweight block cipher designed by Knudsen et al. Some noteworthy characteristics are a burnt-in key, a key-dependent permutation layer and identical round keys. Independent work on PRINTcipher has identified weak key classes that allow for a key recovery --- the obvious countermeasure is to avoid these weak keys at the cost of a small loss of key entropy. This paper identifies several larger classes of weak keys. We show how to distinguish classes of keys and give a 28-round linear attack applicable to half the keys. We show that there are several similar attacks, each focusing on a specific class of keys. We also observe how some specific properties of PRINTcipher allow us to collect several samples from each plaintext--ciphertext pair. We use this property to construct an attack on 29-round PRINTcipher applicable to a fraction 2^{-5} of the keys.

Category / Keywords: secret-key cryptography / cryptanalysis, block cipher, linear cryptanalysis, finding samples, key bit distinguisher

Publication Info: Submitted

Date: received 5 Aug 2011, last revised 30 Sep 2011

Contact author: martin agren at eit lth se

Available formats: PDF | BibTeX Citation

Note: Substantially revised.

Version: 20110930:181043 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]