Cryptology ePrint Archive: Report 2011/287

Algebraic cryptanalysis of the round-reduced and side channel analysis of the full PRINTCipher-48

Stanislav Bulygin

Abstract: In this paper we analyze the recently proposed light-weight block cipher PRINTCipher. Applying algebraic methods and SAT-solving we are able to break 8 rounds of PRINTCipher-48 with only 2 known plaintexts and 9 rounds under some additional assumptions. We show that it is possible to break the full 48-round cipher by assuming a moderate leakage of internal state bits or even just Hamming weights. Such a simulation side-channel attack has practical complexity. We investigate applicability of our method to cryptanalysis of the full PRINTCipher-48.

Category / Keywords: secret-key cryptography / Algebraic cryptanalysis, SAT-solving, PRINTCipher, MiniSAT, CryptoMiniSAT

Date: received 31 May 2011

Contact author: Stanislav Bulygin at cased de