Weekly Seminars on

Mathematical Aspects of Computer Science

Shahid Beheshti University, Department of Mathematics

Probabilistic Self-similarity Cryptanalysis

Hadi Soleimany

Cyberspace Research Institute - Shahid Beheshti University

94/8/26

Abstract

In this work we describe novel frameworks to enhance self-similarity cryptanalysis against some lightweight block ciphers in a probabilistic setting. The methods exploit some features from related-key cryptanalysis, differential cryptanalysis and also self-similarity cryptanalysis to build a particular differential characteristic which has potentially less active S-boxes than standard differential characteristics.

In particular, the presented techniques can overcome round-dependent constants which are the typical countermeasure against classical slide cryptanalysis and reflection cryptanalysis. To demonstrate the effect of the presented methods, we provide analyses of several well-known lightweight block ciphers LED-64, PRINCE-like cipher, ITUbee and Zorro This work shows that employing round constants is not always sufficient to provide security against a variant of self-similarity cryptanalysis but the relation between the round constants should also be taken into account.

1st term of 94-95/ Fall 2015,
Department of Mathematics,
Tuesday, 3-4 pm