Analysis of Boomerang Differential Trials via a SAT-Based Constraint Solver URSA

Jun 12, 2015

Common previous applications of SAT solvers in cryptanalysis include directly encoding the cryptographic primitive into logical equations and then trying to solve such equations. The unknown variables are typically the secret key bits (or unknown message bits, in attempts to obtain a pre image of a hash function) and the equations are built using known plaintext/ciphertext or hash digest. Such attempts, however, typically go only through a small number of rounds of a cryptographic primitive, as the problem the SAT solver is given is equivalent to the problem of breaking the cryptographic primitive. In this work, we show that if we give up on attempting to use the SAT solver for direct cryptanalysis, SAT can still be a very useful tool in cryptanalysis, particularly, e.g., in the domain of differential/boomerang attack verification. Using an off-the-shelf constraint solver URSA (which translates C-like code into SAT equations), we analyze differential trails specified in previous literature and show that probabilistic analysis of several of these trails is flawed.

Abstract

Obtaining differential patterns over many rounds of a cryptographic primitive often requires working on local differential trail analysis. In the case of boomerang and rectangle attacks, merging two short differential trails into one long differential pattern is required. It was previously shown by Murphy that caution should be exercised as there is increased chance of running into contradictions in the middle rounds of the primitive. In this paper, we propose the use of a SAT-based constraint solver URSA as aid in analysis of differential trails and find that previous rectangle/boomerang attacks on XTEA, SHACAL-1 and SM3 primitives are based on incompatible trails. Given the C specification of the cryptographic primitive, verifying differential trail portions requires minimal work on the side of the cryptanalyst.

Presented at ACNS 2015 - Download.

design reviews, and tracking impactful developments in the space of academia and industry.