Automatic differential cryptanalysis of symmetric ciphers

Matteo Rossi

Abstract

Symmetric cryptography plays a key role in our daily lives, securing the vast array of devices and applications we utilize, facilitating secure and fast communications, as well as safeguarding data at rest. Motivated by the pursuit of enhanced efficiency and robustness, researchers recently have worked on novel designs for symmetric ciphers. A notable example is NIST's call in 2019, which introduced 56 candidates for the standardization of lightweight symmetric ciphers. The evolution of these designs inevitably leads to the emergence of new attack vectors, giving cryptanalysts two primary objectives: crafting specialized methods to break novel designs, and developing automated frameworks for fast blackbox analysis of symmetric ciphers to uncover possible weaknesses. This thesis focuses on the latter aspect, drawing inspiration from Aron Gohr's pioneering work presented at CRYPTO 2019. Gohr demonstrated an attack on the SPECK cipher improving the existing state of the art, employing neural networks with minimal prior knowledge on the cipher structure.

Expanding Gohr's contributions, we first analyze what we can expect from neural networks in symmetric cryptanalysis. Subsequently, we analyze why Gohr's approach excelled in the case of the SPECK cipher but encountered limitations with other designs. This investigation results in the formulation of a comprehensive framework for analyzing symmetric ciphers in the context of differential cryptanalysis by means of neural networks. The concluding segment of the thesis explores algorithmic methods for the same purpose, presenting a novel approach based on Monte Carlo tree search.