Bafghi, Abbas Ghaemi; Safabakhsh, Reza; Sadeghiyan, Babak
Finding the differential characteristics of block ciphers with neural networks. (English) Zbl 1283.94047

Summary: We have developed a model to represent the differential operation of block ciphers in order to help finding differential characteristics. Through this model, the whole space of differential characteristics for a block cipher is represented by a multi-level weighted directed graph. In this way, the problem of finding the best differential characteristic for a block cipher reduces to the problem of finding the minimum-weight multi-branch path between two known nodes in the proposed graph. In this paper, we use recurrent neural networks to find such a path in the differential operation graph of a block cipher. The path is found through minimization of the network cost function. We use the Hopfield network and the Boltzmann machine with and without chaos to minimize the cost function. Chaos is introduced to assist the network to escape from the local minima of the cost function. Experimental results indicate the usefulness of the approach and comparison of the performance of the used techniques shows that the Boltzmann machine algorithm incorporating simulated annealing produces the best result.

MSC: 94A60 Cryptography

Keywords: differential cryptanalysis; block cipher; differential operation model; hopfield network; chaotic Hopfield; Boltzmann machine; chaotic Boltzmann machine; simulated annealing

Software: Serpent

Full Text: DOI

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.