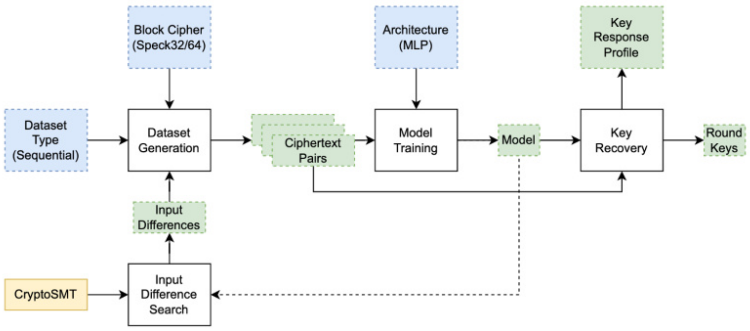
Hessisches Kompetenzzentrum
für Hochleistungsrechnen

Investigating the Machine Learning-based Cryptanalysis of Lightweight Block Ciphers



Project Manager
Moritz Huppert

Principal Investigator
Prof. Dr. Marc Fischlin

Project Term
2023 - 2023

Clusters
Lichtenberg II Cluster Darmstadt

Software
PyTorch

Additional Software
CryptoSMT

Institute
Cryptography and Complexity Theory

University
Technische Universität Darmstadt

Introduction

Lightweight Cryptography is about developing and analyzing algorithms that provably obtain security goals, such as Confidentiality and Integrity, in resource-constrained environments. In these environments, computing devices are restricted in their memory and computational capabilities, which prevents the operation of well-established cryptographic algorithms, such as the Advanced Encryption Standard. The Internet of Things is a prominent instance of such an environment that largely consists of low-cost, smallscale computing devices. In the last decade, the increasing importance of Lightweight Encryption has been reflected in the NSA publishing two Lightweight Cipher families and NIST initiating a standardization process for Lightweight Ciphers. Considering the efficient performance of these Ciphers, their practical security needs the be closely examined by employing Cryptanalysis. One type of Cryptanalysis – Differential Cryptanalysis – recently was combined with Deep Learning, which yielded powerful attacks against Lightweight (Block) Ciphers. Further, it started an active field of research that combines recent advances in Machine Learning research with cryptanalytic attacks. Due to the variety and amount of recently published ideas in the field of Machine Learning-based Cryptanalysis, it is challenging to conceive the current state of knowledge. Hence, we summarize, implement, and compare recent work in a transparent and reproducible manner. Moreover, we extend the research by successfully applying new Machine Learning models to cryptanalytic attacks and by developing a new training setup, which impacts how the models can be utilized in a partial (Round-)Key Recovery, as proposed in previous research. Further, we have implemented a lightweight SMT-solver-based search for well-suited input differences: an essential component of cryptanalytic attacks. In all of our experiments, we trained artificial neural networks on a large set of training data in a supervised setting, for which we used the GPUs provided by the Lichtenberg cluster.

Methods

We have developed a modular, highly vectorized Python framework for Machine Learningbased Cryptanalysis that served as the basis for our experiments. The Pytorch-based framework simulates cryptanalytic games in which an artificial neural network performs a binary classification task based on the observed behavior of an encryption oracle. The neural distinguisher is trained on 10^7 and tested on 10^6 game instances. We plan to publish the framework in the near future, which can be used to reproduce our experiments, apply new Machine Learning models, and extend the attacks to new ciphers and types of Cryptanalysis. All of the experiments were conducted for the (Lightweight) Speck32/64 and the Present64/80 Block Ciphers. We compared the impact of different model architectures, data requirements, and manual input preprocessing on the neural distinguishers.

Results

Based on our benchmarking, we have adapted new Machine Learning architectures that obtain competitive accuracies to the well-established models from the literature. The lightweight SMT-based search reliably produces cryptographic distinguishers with high accuracy and even found input differences, which were previously not mentioned in the literature concerned with Machine Learning-based Cryptanalysis. Our proposed training setup impacts the learned Key Response of neural distinguishers, which was previously assumed to be immutable.

Discussion

Our framework aims to lower the barrier to entry for researchers that are interested in the exciting new field of Machine Learning-based Cryptanalysis. We plan to technically extend the framework to offer distributed training capabilities on multiple GPUs and Cupy support for further performance enhancements. Similarly, we plan to extend the number of supported ciphers, Machine Learning models, and cryptanalytic techniques in collaboration with the research community. The insights from our benchmarking, the adapted architectures, and the new training setup might allow future work to extend the scope of existing cryptanalytic attacks.

Figures

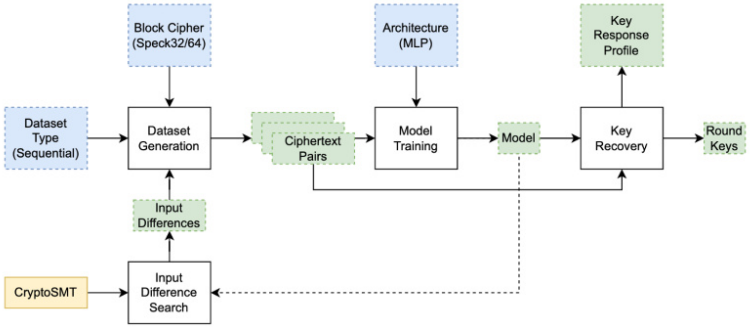


Figure 1: An overview of the framework architecture. The white boxes represent the modules, the blue boxes represent possible configurations, the yellow boxes represent external modules, and the green boxes represent the module artifacts.

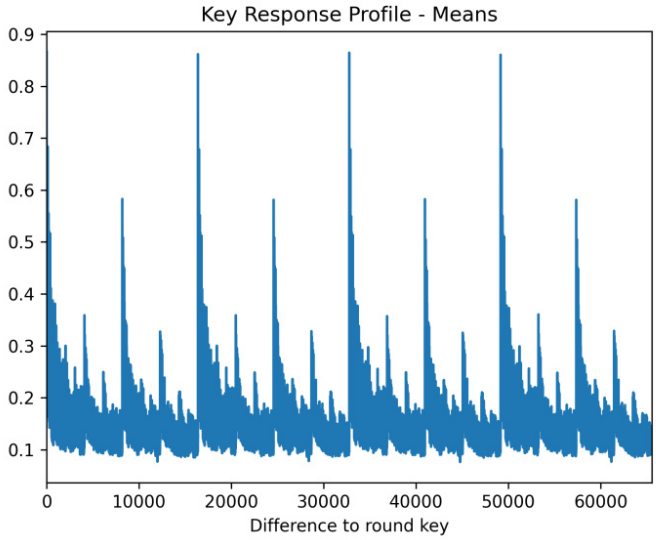


Figure 2: The Key Response Profile of a trained (neural) cryptographic distinguisher. The profile depicts the output score of the distinguisher with respect to ciphertext pairs that have been decrypted for one round with right/false round keys.

Last Update: 2023-08-27 15:51