Centre for Research Training

Security analysis of Block ciphers with AI

Amirhossein Ebrahimi Moghaddam

Supervisors: Dr. Paolo Palmieri, Prof. Utz Roedig

School of Computer Science and Information Technology

University College Cork, Ireland

Introduction

- Block ciphers are cryptographic algorithms that can provide confidentiality by encrypting sensitive data.
- They are widely used in many protocols like SSL and SSH.
- For their vast application, it is vital to evaluate the security of block ciphers.
- There are some statistical techniques, which is called cryptanalysis, that can attack one algorithm to get a measure of their security.
- These attacks' main idea is to find a statistical method to distinguish between a random permutation and a block cipher, called a distinguisher attack.
- In differential distinguisher attack, which is the main focus of this research, the attacker tries to observe a block cipher's behavior under a specific input difference
- If the system's resultant output differences show any non-random behavior, a differential distinguisher is obtained.
- These techniques usually need a massive amount of data and memory to be implemented.
- There are many types of research to automate these cryptanalysis methods.
- One of these research areas is using Machine Learning (ML) to attack a block cipher.
- In 2019 Gohr presented an ML/AI based cryptanalysis on SPECK cipher that was better than previous attacks.
- It was illustrated that by using deep learning, a differential distinguisher could be achieved in an automated way and with less data than other attacks.
- The key recovery stage of the attack also needs much less data, so the whole process of the cryptanalysis can be implemented on a personal computer.

PROBLEM

It is enough to distinguish a cipher from a random permutation to break the security of it. This research aims to train a deep neural network to do this classifying problem. However, some challenges may make the training phase difficult.

Challenges:

The main challenges are:

(i) *Data complexity:*

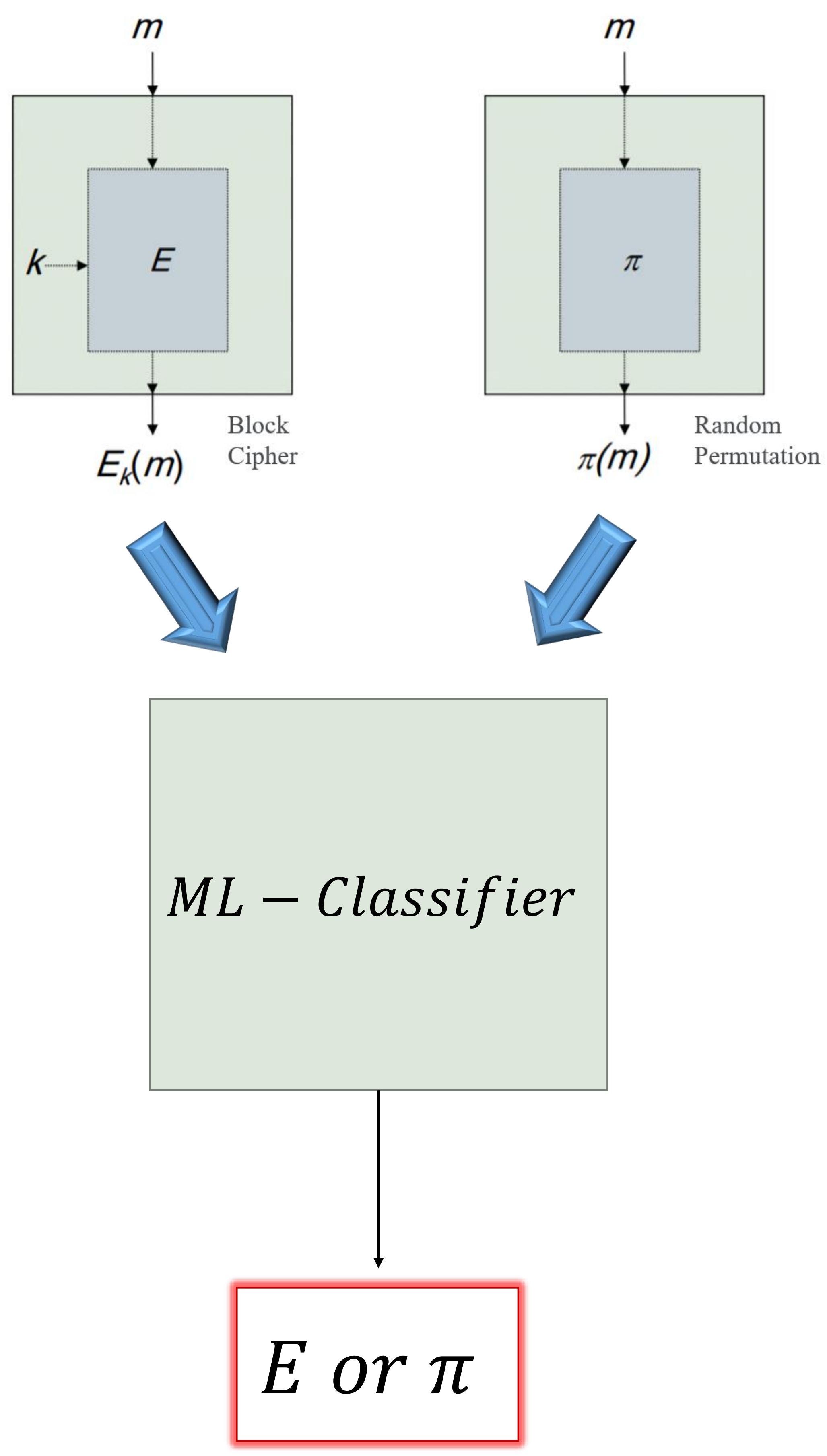
In traditional attacks, the amount of needed data could be as large as possible until it is not more than brute force.

PROBLEM (Cont.)

However, in the deep learning method, for one workstation, the memory only can have data around 2^{40}, which is not enough in most cases.

(ii) *Randomness of ciphers:*

Block ciphers try to hide messages from attackers, so they make a plaintext as random as possible. As a result, in the output, we have lots of pseudo-random generated data, making it hard for a machine to find any meaningful pattern in it.



METHODOLOGY

- We review current methods to create an machine based distinguisher for a cipher.
- We explore different "differential analysis" techniques such as truncated-differential for the proposed challenges in the current distinguisher to compare their performance
- We explore different cryptanalysis like "linear attacks" to see the performance of machines that are trained.

Discussion & Future works

Using ML to evaluate the safety of block ciphers can make this task more convenient. However, we need to deploy new techniques in order to increase the accuracy of these machines. Also, it is good to examine if ML-distinguishers could be as good as "differential attack" for other attacking scenarios. Moreover, using transfer learning techniques may allow us to transfer the knowledge obtained from cryptanalysis on a cipher to another encryption design. Finally, ML-distinguishers make it possible to check the effect of each bit of plaintext/ciphertext pairs during the cipher's security analysis, so we have a better understanding of the cryptosystem's behavior.

Host Institution