Exploring Automatic Search of Differential Characteristics in Symmetric Ciphers

Tan Jun Xiong (U2140233A)

Abstract:

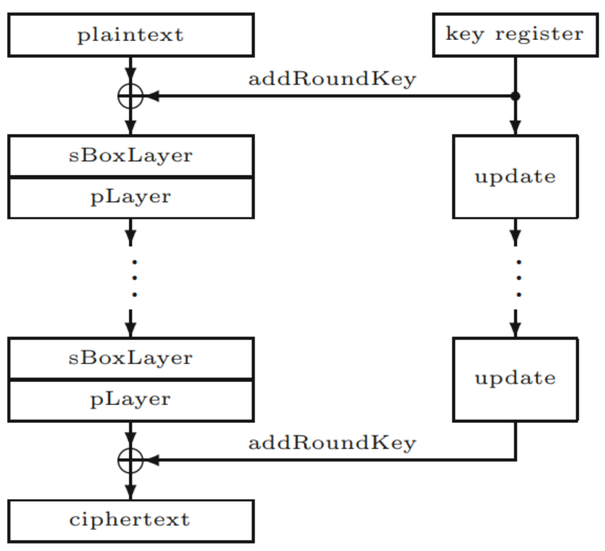
Differential cryptanalysis is one of the most powerful techniques to understand symmetric-key ciphers. However, obtaining the differential characteristic of a modern cipher can be very computationally taxing, and practically impossible when using a brute-force approach. In this summer, I learnt about the structure of Substitution-Permutation Network (SPN) ciphers, the fundamentals of a differential attack, and employ the automatic search of a differential characteristic on PRESENT-80 using Mixed Integer Linear Programming (MILP).

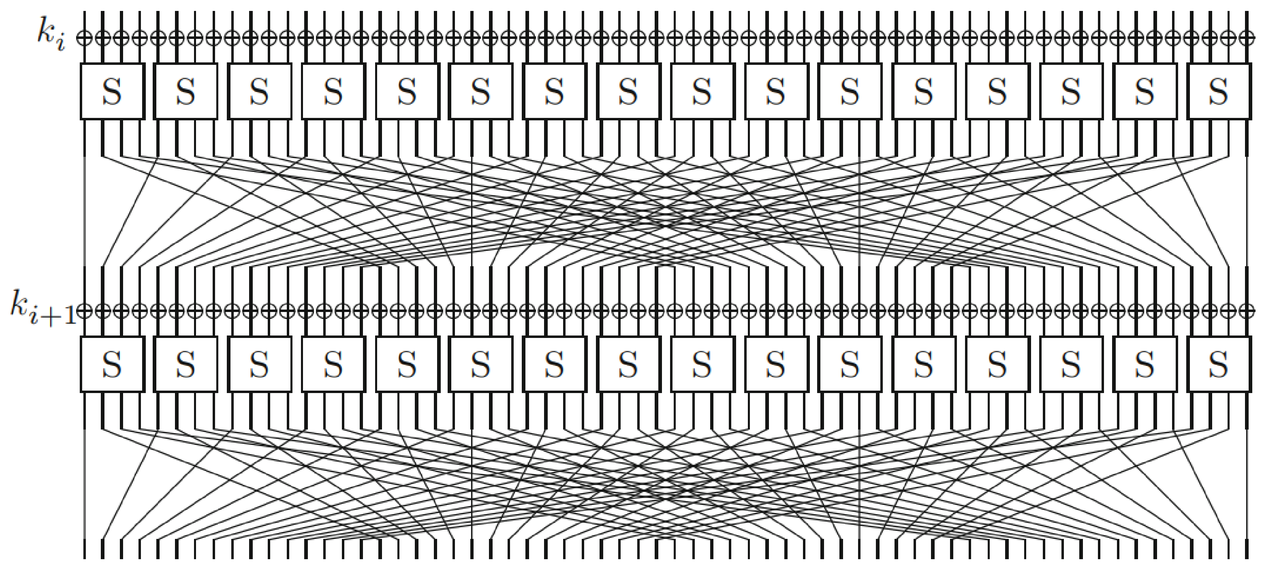
Image by Anthony Brown, taken from Adobe Stock

PRESENT-80:

PRESENT-80 is a lightweight, bit-oriented SPN block cipher. 64-bits of data are first pushed through 4 x 4 S-boxes. The bits are then permutated before being XOR-ed against a round key. This process is repeated for 31 rounds, each round using a unique round key, calculated using a base key of 80-bits and a key scheduler.

generateRoundKeys()
for $i = 1$ to 31 **do**
  addRoundKey(STATE, K_i)
  sBoxLayer(STATE)
  pLayer(STATE)
end for
addRoundKey(STATE, K_{32})





Diagrams taken from "Encyclopedia of Cryptography and Security" by Van Tilborg et. al.

Understanding the Differential Attack:

Differential cryptanalysis is a chosen plaintext attack. The difference between strings of data is equal to the strings XOR-ed against each other. In an ideal cipher, the probability that a particular output difference occurs given a particular input difference is 1 in 2^n, where n is the number of bits in each block of data. This would also require each pair of S-box inputs to return a unique output difference. However, such an ideal S-box is mathematically impossible. The attack aims to exploit the pair of input and output differences with a significantly higher probability of occurrence. This output difference is known as the ***differential characteristic***. Furthermore, intermediate round keys have no influence on the output difference of a cipher, making differential cryptanalysis a powerful tool.

Using MILP with the convex hull of S-box:

Clearly, some differentials cannot exist as outputs of a given S-box. These ***impossible differentials*** have 0 probability of occurring. The space of possible differentials of the cipher exist as vertices in GF(2^n) as a convex polytope. The set of solutions can be described as a set of linear constraints. This is known as the half-space representation. By modelling each operation as a set of constraints, all constraints can be put together to find the convex hull of differentials. The objective is to obtain the highest probabilistic differential from this set. We can also set the objective function to be the least number of active S-boxes during the entire encryption.

Results:

Differential trail obtained for 3 rounds of PRESENT-80:

```
Probability of Differential Characteristic:  0.00390625
 - One in 256
```

Differential trail obtained for 5 rounds of PRESENT-80:

```
Plaintext Difference:
        .... .... 1111 .... .... .... .... .... .... .... .... .... .... .... 1111 ....

S-Box I/O:
 I:     .... .... 1111 .... .... .... .... .... .... .... .... .... .... .... 1111 ....
 O:     .... .... ..1. .... .... .... .... .... .... .... .... .... .... .... ..1. ....
_____________________________________PERMUTATE_____________________________________
 I:     .... .... .... .... .... .... .... .... .... .... 1..1 .... .... .... .... ....
 O:     .... .... .... .... .... .... .... .... .... .... ..1. .... .... .... .... ....
_____________________________________PERMUTATE_____________________________________
 I:     .... .... .... .... .... .... .... .... .... .... ..1. .... .... .... .... ....
 O:     .... .... .... .... .... .... .... .... .... .... 1.1. .... .... .... .... ....
_____________________________________PERMUTATE_____________________________________
 I:     .... .... .... .... .... .... .... .... ..1. .... ..1. .... .... .... .... ....
 O:     .... .... .... .... .... .... .... .... 1.1. .... 1.1. .... .... .... .... ....
_____________________________________PERMUTATE_____________________________________
 I:     ..1. .... ..1. .... .... .... .... .... ..1. .... ..1. .... .... .... .... ....
 O:     1.1. .... 1.1. .... .... .... .... .... 1.1. .... 1.1. .... .... .... .... ....
_____________________________________PERMUTATE_____________________________________

Ciphertext Difference:
        1.1. .... 1.1. .... .... .... .... .... 1.1. .... 1.1. .... .... .... .... ....

Probability of Differential Characteristic:  9.5367431640625e-07
 - One in 1048576
```

Supervisor: Asst. Prof. Jian Guo
Special Thanks to Poon Zong Wei, Julian