Overview of Cryptanalysis Projects

Table of Contents

Retracing Boomerang Attack on AES I

- The retracing boomerang attack is a refined form of the boomerang attack used in differential cryptanalysis to extract information about a block cipher's secret key, particularly when no strong differential spans the entire cipher.
- The project in [Retracing Boomerang Attack] implements retracing boomerang attack on 5 round AES. The procedure is as follows
  - Identify the plaintext pair that that exhibits better differential characteristics across 5 rounds of AES using yoyo distinguisher.
  - Generate the 1034 friend pairs. Friend pairs are the plaintext pairs that retain the differential characteristic.
  - For each friend pair, generate an equation where the coefficients are the MixColumns bytes and the unknown variables are the pre-MixColumns bytes.
  - Perform the guassian elimination to find the rank of the matrix.

  The project performs the following tests

Retracing Boomerang Attack on AES II

  - Retracing Boomerang Attack on 5 round AES using for 100 random keys.
  - Yoyo distinguisher for 10 times and check whether it returns good pair of plaintexts or not.
  - AES encryption with various plaintext ciphertext pairs.
- Future Work: Recover the pre-Mix Column bytes by solving the system of linear equations. Apply inverse Shift rows and SubBytes to obtain the partial key bytes.

Differential Linear Cryptanalysis I

- Differential-Linear Attack is a hybrid cryptanalysis technique that combines differential cryptanalysis and linear cryptanalysis to attack symmetric-key block ciphers.
- The differential-linear attack uses a differential characteristic on the first rounds and a linear approximation on the last rounds.
- To find the good differential linear characteristic, a Differential Linear Connectivity Table (DLCT) is needed.
- The project in [DLCT] presents the DLCT for the s-boxes of DES, Midori cipher and PRESENT cipher.
- For DES, it performs the following steps.
  1. Extract s-box input bits for the row and the column index.
  2. For every input difference, compute outputs of the S-box for pairs of inputs differing by that difference.
  3. Construct the DLCT table by comparing the output mask of the two S-box outputs.

Differential Linear Cryptanalysis II

For Midori and PRESENT cipher, the DLCT is constructed similar to step 2 and step 3.

- The input s-boxes is given as a part of the program and the output tables are stored DLCT_tables.txt

Future Work: By analyzing the DLCT of the DES S-boxes, the DL attack can be performed on reduced round DES.

Boomerang Connectivity Table I

- The boomerang attack is a cryptanalytic technique used to break block ciphers by combining two short differential characteristics that apply to different halves of the cipher.
- The Differential Distribution Table (DDT) of an S-box shows how often input difference leads to the specific output difference.
- The Boomerang Connectivity Table (BCT) for an S-box records how often a specific input difference δ_{in} combined with a specific output difference δ_{out} satisfies a boomerang relation.

The project in [BCT] constructs the DDT and BCT for AES and TWINE S-boxes. The procedure is as follows:

- Choose the AES s-box or TWINE s-box for the DDT and BCT construction.
- For each pair of inputs, compute the input difference and output difference of the chosen s-box and construct the DDT.

Boomerang Connectivity Table II

- For each input difference δ_{in} and the output difference δ_{out}, compare

$$S^{-1}(S(x) \oplus \delta_{out}) \oplus^{-1} (S(x \oplus \delta_{in}) \oplus \delta_{out}) == \delta_{in}$$

  If the condition is satisfied, update the BCT.
- It counts the frequency of each value in DDT and BCT.
- The input S-boxes are given as seperate files and the output is stored in ddt.csv and bct.csv files.

Future Work: Boomerang Attack can be performed using the BCT to the Deoxy-BC and SKINNY Cipher.

Matsui Linear Cryptanalysis

- It is a known plaintext attack.
- It was first introduced by Mitsuru Matsui in the early 1993.
- Attackers identify a linear expression relating bits of plaintext, ciphertext, and key that holds with probability biased away from 0.5.
- Matsui proposed two algorithms:
  - Distinguishing Attack: Distinguishes cipher from random permutation.
  - Key Recovery Attack: Recover partial key bits using a linear approximation of $n-1$ rounds of cipher.

Matsui Atttacks on DES I

The Project present in [Matsui] implements the following attacks.

- Distinguishing Attack on 3-round DES with 75 plaintext-ciphertext pairs, 0.56/8 bias and a specific 5 bits are set for input and output mask. The procedure of the attack is as follows:
  - Generate 75 random (plaintext-ciphertext) pairs.
  - For each plaintext–ciphertext pair, apply the input mask (after the initial permutation) to the plaintext, and apply the output mask (after the inverse final permutation) to the ciphertext.
  - Count the number of pairs satisfying the linear equation and calculate the expected bias.
  - If the expected bias matches with the theoretical bias, it returns 0. Otherwise, return 1 indicating the approximation does not hold and data is a random permutation.

Matsui Attacks on DES II

- Key Recovery attack on 4 round DES with 50 plaintext-ciphertext pairs and 0.56/8 bias. The procedure of the attack is as follows:
    - Find the active S-boxes and and determine the total number of key bits to be guessed.
    - Generate partial round keys for every combination of guessed bits.
    - Identify the correct partial round key by exploiting linear biases.

  The input s-boxes and the keys are given as a part of the test program.

Future Work: The key recovery attack needs to be fully implemented. The Key Schedule algorithm needs to be implemented.

THANK U