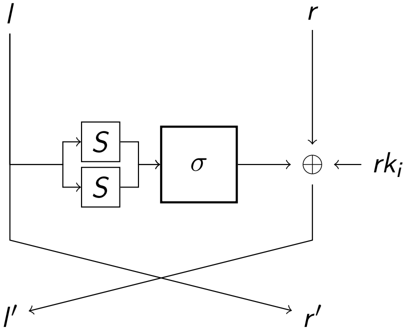
Differential Cryptanalysis

April 10, 2019

Last week's exercise

Solution on whiteboard.

TC05 (mini)



With Sbox:

$$S = (\mathtt{E},\ \mathtt{B},\ \mathtt{4},\ \mathtt{6},\ \mathtt{A},\ \mathtt{D},\ \mathtt{7},\ \mathtt{0},\ \mathtt{3},\ \mathtt{8},\ \mathtt{F},\ \mathtt{C},\ \mathtt{5},\ \mathtt{9},\ \mathtt{1},\ \mathtt{2})$$

and bit permutation:

$$\sigma = \left(\begin{array}{cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 0 & 1 & 7 & 2 & 4 & 5 & 3 \end{array}\right)$$

TC05 sbox DDT

	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	4	0	2	0	4	0	0	0	2	2	0	0	0
2	0	0	0	0	4	0	0	0	0	0	2	2	2	6	0	0
3	0	0	0	0	0	0	0	4	4	0	4	0	0	0	0	4
4	0	2	0	2	2	0	6	0	0	0	0	0	0	0	4	0
5	0	4	0	2	2	0	0	0	0	0	2	0	0	6	0	0
6	0	0	2	0	0	2	0	0	0	2	4	4	0	0	2	0
7	0	2	0	0	0	0	2	0	0	6	0	0	4	0	2	0
8	0	0	2	2	2	0	2	0	0	0	2	2	0	2	0	2
9	0	2	0	2	0	2	2	0	6	2	0	0	0	0	0	0
A	0	2	2	0	0	0	0	4	0	2	0	2	0	0	2	2
B	0	0	2	0	2	4	0	0	2	0	0	0	4	0	2	0
C	0	0	2	0	2	4	0	0	2	2	0	2	2	0	0	0
D	0	0	2	0	0	0	2	4	0	0	0	2	0	0	4	2
E	0	4	0	0	2	2	0	0	2	2	0	0	0	0	0	4
F	0	0	2	4	0	0	2	0	0	0	2	0	2	2	0	2

Key recovery

- Differential Characteristic gives distinguisher.
- We can use distinguishers to recover round keys.
- Say we have a r round distinguisher, then we can attack $r + i$ rounds by decrypting i rounds and checking for the distinguisher. If distinguisher holds, key is probable.
- For Differential Cryptanalysis there exists another key recovery attack.

Key recovery (Feistel network)

Let

$$P_1 \oplus P_2 = \Delta_{\mathtt{in}} = \Delta_0 \text{ and } C_0 \oplus C_1 = \Delta_{\mathtt{out}} = \Delta_r$$

.
We know the differences

$$\Delta_0, \Delta_1, \ldots, \Delta_{r-1}, \Delta_r.$$

Now if for a key guess k

$$F(F(C_0^r) \oplus C_0^l \oplus k) \oplus F(F(C_1^r) \oplus C_1^l \oplus k) \oplus \Delta_r^r = \Delta_{r-2}^r$$

We know for which values, a, b we have $F(a) \oplus F(b) = \Delta_r^r \oplus \Delta_{r-2}^r$
Which allows us to compute a set of k's.

Key recovery (Feistel network)

- Only active S-boxes can be used for key recovery.
- In practice this means we need several characteristics to recover the full key.
- The key is only probable (often you will find a couple of keys).
- After finding a probable key we can unroll one round and repeat.

Questions

- What property can we use of AES like ciphers (TC03) to find more characteristics?
- Does TC05 (mini) have this property?

Key recovery appending rounds

- Appending rounds
  - Given an r round distinguisher from $\Delta_{\texttt{in}} \rightarrow \Delta_{\texttt{out}}$
  - Given a set of plaintext ciphertext pairs $(p_1, c_1, p_2, c_2) \in P$ such that $p_1 \oplus p_2 = \Delta_{\texttt{in}}$
    - Guess partial key k s.t. we can decrypt i rounds.
    - Initialize a counter $C_k = 0$
    - Construct the set $P' = (p_1, D_i(c_1, k), p_2, D_i(c_2, k))$ for $(p_1, c_1, p_2, c_2) \in P$.
    - Now for every pair $(p_1', c_1'), (p_2', c_2') \in P'$
    - If $c_1' \oplus c_2' = \Delta_{\texttt{out}}$ increase the counter C_k by one.
  - Pick the key k for which C_k is maximal.

Questions

- How many rounds of TC05 mini can we attack?
- And if we increase the key size to 128-bit?
- Does the key schedule influence the attack?
- What components can we change to make the cipher better w.r.t. differential cryptanalysis?

Key Schedule

- We have to keep the key schedule in mind when recovering a key.
- Key schedules are often linear, which is nice for us :)
- Most often we can find the master key by recovering some round keys.
- In case of TC05 we can find the master key by finding 4 consecutive round keys.
- Introduces dependencies in between rounds $\implies$ which can be good for us.

Differentials

- Often several characteristics with same $\Delta_{\texttt{in}}$ and $\Delta_{\texttt{out}}$.
- Increases the probability that we see some $\Delta_{\texttt{out}}$ given a $\Delta_{\texttt{in}}$.
- Depending on the cipher it can greatly decrease time and data.
- Some tools can find differentials, but sometimes some pen and paper analysis is needed.

Finding Differentials

- Find a nice characteristic and experimentally verify the probability of a charactersitic.
- If expected and experimental probability are far apart, probably differential effect.
- We can also look at a truncated output differential, so what is the probability 0002 0000 → 0x00*0 000*, where $*$ can be any difference.
- Use STP/MILP/etc.
- By hand?

Truncated differential

- Special case of differentials.
- Only look at: difference is 0 or non-zero.
- Can only be used as a distinguisher.
- Difference propagation same as information propagation in MitM.
- More on this next class.

Project

- Two options: Competition and LWC.
- Competition - Everyone designs a cipher, then everyone tries to break the ciphers. Grade is determined both by the design as well as the attacks.
- LWC - We look at the LightWeight Competition candidates that will be published (hopefully) soon by NIST.
- Both options are fun, in the first you get to design your own cipher. The second option lets you attack real ciphers (if you succeed you might be able to write a paper about it).
- Send me an email with your preference before the 16th of April.

Homework

- We attack TC05 with differential attack, so chosen plaintext model.
- Extra field for get data on website (additional input) which takes the input difference (hexadecimal).
- Every call will give you other pairs, you can use this to get slightly more pairs if needed, but be aware that there is a rate limiter (30 requests per hour).
- Keep in mind that you will probably need 4 different sets of input differences to succesfully attack the cipher.
- Do not misuse the multiple requests ‘feature’, if you hit the rate limiter you need to wait for an hour.

Next Week

- Pesach, so next two weeks no class.
- Attack TC05, exercise will be online shortly.
- Read tutorial if you haven't already.
- Relax and enjoy your holiday.
- If you have any questions regarding the course, please email me
- After holidays we will start on project.