Cryptanlysis of CLEFIA

Ivica Nikolić
(joint work with Sareh Emami, San Ling, Josef Pieprzyk, Huaxiong Wang)

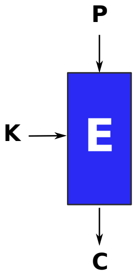
Nanyang Technological University, Singapore
Queensland University of Technology, Australia

8 December 2014

Block ciphers and analysis

Block cipher $E_K(P)$

- Input: Plaintext P and key K
- Output: Ciphertext C



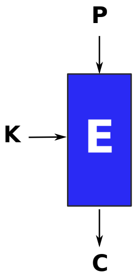
Block ciphers and analysis

Attacker does not know the key.
Attacker can fix:

- P and obtain C
- C and obtain P

and try to find:

- Distinguisher (tell apart from random)
- Key recovery (find bits of the key)

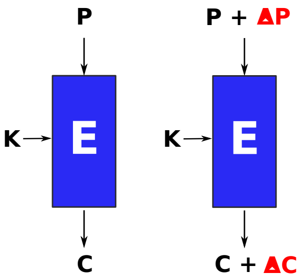


Differential Attacks

Differential analysis – the most popular form of attack. Find *specific* differences Δ_P, Δ_C s.t.:

$$\text{plaintexts } (P, P \oplus \Delta_P)$$
$$\downarrow$$
$$\text{ciphertexts } (C, C \oplus \Delta_C)$$

happens with a high probability



NANYANG TECHNOLOGICAL UNIVERSITY

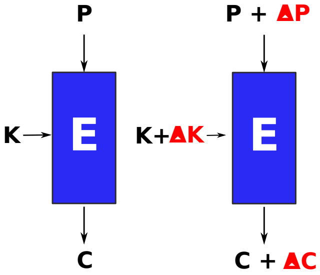
Related-key Differential Attacks

Find:

- Plaintext difference Δ_P
- Ciphertext difference Δ_C
- **Key difference** Δ_K

$$E_K(P) \oplus E_{K+\Delta K}(P \oplus \Delta P)$$
$$\downarrow$$
$$\Delta C$$

happens with a high probability



Related-key resistance

Cipher designers provide related-key resistance mainly in 4 ways:

1. we don't care
2. we don't know
3. we use automatic search tools
4. we use heavy non-linear operations in the key schedule

Weak Keys

Sometimes analysis works only for a subset of keys called **weak-key class**.
The analysis that works when the key is secret and chosen uniformly at random for the weak-key class is called **membership test**.

For attacks that use more than one key (such as related-key diff.) the weak-key class is specified as set of tuples.

CLEFIA-128

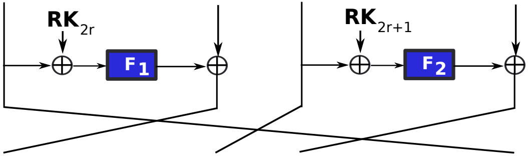
The block cipher CLEFIA-128:

- Designed by Sony in 2008
- Submitted to IETF
- In CRYPTREC candidate recommended cipher list
- ISO/IEC lightweight standard

Specifications

CLEFIA-128:

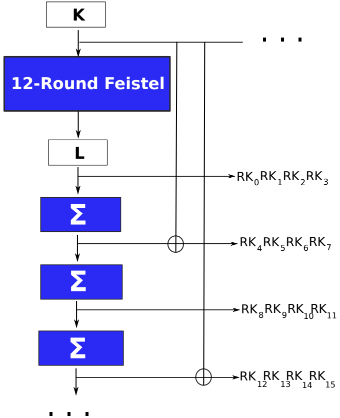
- four-branch generalized Feistel cipher
- 128-bit state and key
- 18 rounds as below



Analysis

Published analysis:

- **Single-key**: plenty of attacks on round-reduced
- **Related-key**: None! Designers proved no good differentials exist in the key schedule

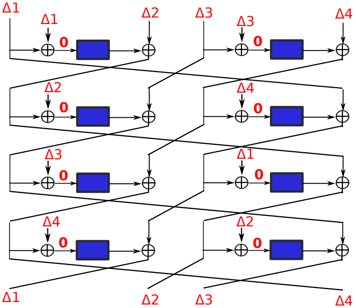


Related-key differentials in Feistel ciphers

Biryukov-Nikolić [Complementing Feistel Ciphers, FSE'13]:

Lemma

RK differentials with Pr $= 1$ *can exist for Feistel ciphers if the the round-key differences are iterative*



Iterative round key differences

Focus on the key schedule and see how to achieve iterative round key differences. It turns out it is simple:

1. $\Delta L = \Sigma^2(\Delta L)$
2. $\Delta K = \pi(\Delta L) \oplus \Sigma(\Delta L)$

Result: there are 2^{14} pairs of $(\Delta K_i, \Delta L_i)$
For each i it means that **if ΔK_i after the 12-round Feistel produces ΔL_i then state differential holds with** $\Pr = 1$**.**

ΔK_i compose the weak-key class of CLEFIA-128.

Properties of the RK differentials

The differentials $\Delta K_i \to L_i$ hold with probability 2^{-128} (random permutation). That is, **we do not break the claims of the designers**.

However, the set $(\Delta K_i, \Delta L_i)$ has a special structure:

$$(\Delta K_i, \Delta L_i) = \Lambda_1(x) \oplus \Lambda_2(y),$$
$$i \in [0, 2^{14}], x \in [0, 2^7 - 1], y \in [0, 2^7 - 1]$$

Our analysis is based on this fact.

Membership test

Assume the key pair belongs to the weak-key class, i.e. $(K, K \oplus K_i)$ for some i (generic attack requires: 2^{14})
Then:

- Take random P.
- Create a structure of plaintext $P_i = P \oplus \overline{\Lambda_1}(i)$, obtain the ciphertexts C_i under the first key, and save into list L_1 the values $P_i \oplus C_i$.
- Create a structure of plaintext $P_j = P \oplus \overline{\Lambda_2}(j)$, obtain the ciphertexts C_j under the second key, and save into list L_2 the values $P_j \oplus C_j$.
- Check on collisions between the two lists L_1 and L_2.
- If exists collision, output that the cipher is CLEFIA-128.

Membership test

Why it works?

- The XOR of the plaintexts from the two structure results in all possible ΔP_i, hence one must match the required weak-key ΔP_i (that corresponds to the weak-key pair with ΔK_i difference).
- The collisions reveal if such thing happened.

Data,time,memory $\approx 2^8$

Distinguishers for the hashing modes of CLEFIA-128

Usually, hashing mode analysis coincides with open-key analysis.
Distinguishers for the hashing mode means we can distingush the hash function based on the cipher from a random function.
CLEFIA-128 has 128-bit state and key, thus we analyze the single-block-length modes (e.g. Davies-Meyer).

Distinguishers for the hashing modes of CLEFIA-128

How it works:

- Find a key pair that belongs to the weak-key class by using the same trick as in the membership test.
- The pair defines the round key differences, thus any two plaintexts with difference defined by the subkeys will result in predictable (with $\Pr = 1$ difference in the ciphertext.
- Create differential multicollisions (i.e. examples of many pairs of plaintexts,ciphertexts that have the same difference)

Time complexity to find the weak-key pair: 2^{114}

Conclusion

- Our analysis is invariant of round functions and number of rounds
- Has been checked experimentally on small scale variants
- Does not threaten the practical use of CLEFIA-128 in any way – it simply shows that the cipher is not "ideal"
- If you design Feistel cipher, be aware that the probability of producing iterative round key differences should be much lower than $2^{-state\ size}$ (the exact formula is given in the paper)