On the Complexity of Matsui's Attack

Pascal Junod (pascal.junod@epfl.ch)
LASEC, Swiss Institute of Technology

- Matsui's linear cryptanalysis against 16-rounds DES (as proposed in [Matsui94])

- Widely accepted complexity of the attack:
  Given 2^{43} known plaintext-ciphertext pairs, it is possible to recover the key with a success probability of 85 % within a complexity of 2^{43} DES computations.

- The unique experimental run performed surprisingly too well.

- Several authors have suggested that linear cryptanalysis has a lower complexity.

- Motivation for an experimental complexity analysis.

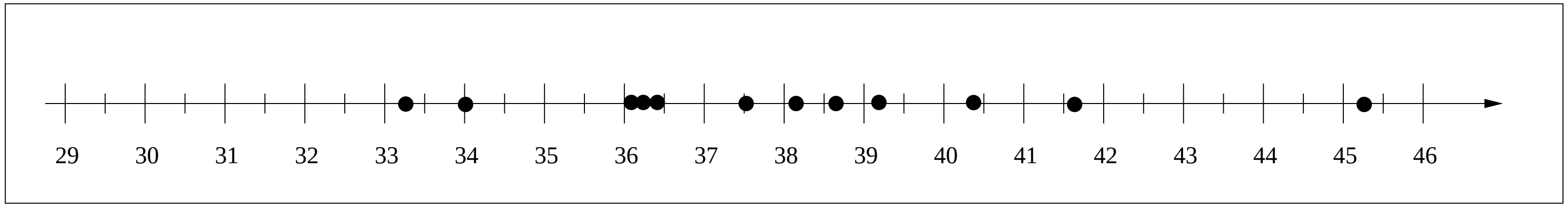
- Fast DES routine (bitsliced implementation on the Intel MMX architecture).

- 12-18 CPUs.

- 3-7 days to produce 2^{43} plaintext-ciphertext random pairs.

Experimental results (12 runs)

Average complexity seems to be far lower than Matsui's expected one.



Proposal suggested by the experimental results:

Given 2^{43} *known plaintext-ciphertext pairs, it is possible to recover the key with a success probability of 85 % within a complexity of* 2^{41} *DES computations.*

Linear cryptanalysis procedure:

- Collection of information about 26 bits of the key by analysis of 2^{43} known-plaintext ciphertexts.

- Sorting of the 26-bits subkey candidates by maximum likelihood.

- Exhaustive search for the remaining 30 bits for the subkey candidates until the right one is found.