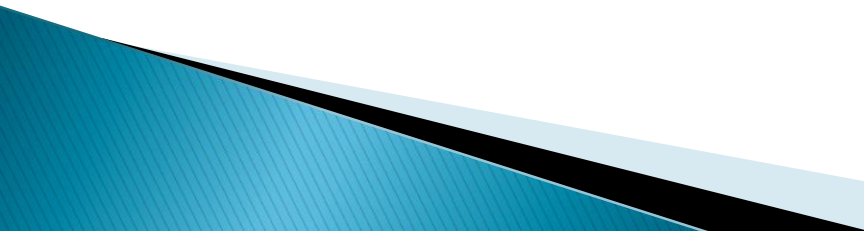


Solving the FEAL 25 Years Prize Problems

Eli Biham and Yaniv Carmeli
Presented by Adi Shamir

FEAL

- ▶ Designed by Miyaguchi and Shimizu (NTT).
 - ▶ 64-bit block cipher family with the Feistel structure.
 - ▶ Original key size was 64 bits, later extended to 128 bits as FEAL-X.
 - ▶ Had major contributions to the history of block ciphers.
 - ▶ Inspired many new ideas, including differential and linear cryptanalysis
- 

The FEAL 25 years prize competition

- ▶ Announced by Mitsuru Matsui at the rump session of CRYPTO'12
- ▶ Deadline is CRYPTO'13
- ▶ The target cipher: FEAL-8X
- ▶ 2^b plaintext-ciphertext pairs are given ($b \leq 20$).
- ▶ Winner: (min b , first)

The initial idea

- ▶ Use the iterative approximation [Biham94] reduced to 6 rounds (bias: 2^{-9}).
 - Analyze one extra round from each end (total 8 rounds).
 - Bad news: The correct key is often not among the most frequent.

- ▶ After implementing the attack we learned about a better 7-round approximation [Ohta Aoki Matsui Moriai 95]
 - bias $\sim 2^{-9}$
 - Found the key in 5 hours on 12 cores.
 - The rest of the subkeys were found in less than one computation hour.
 - Computing the FEAL-X key from the subkeys took less than a second.
 - K(b=20): 7196d25c0ff401c1d6c24f09b94381e3

- ▶ Sent the key on July 24th, 2013 to feal25years@gmail.com and received confirmation for being the first to submit a correct key.
- ▶ Only lasted 4 days:
 - >> Yesterday I received an email from another group; they gave me the solutions of $b=20,19,18,17,16,15$.
I confirmed that they were correct.
(email from Mitsuru Matsui, July 28th)
- ▶ We had no choice but to search for the key of $b=14$.

Back to the initial idea

- ▶ But with the new approximation.
 - Reduced to 6 rounds (bias: $\sim 2^{-5.6}$).
 - Required several improvements to the attack.
 - Unfortunately succeeds for 2^{15} , but for 2^{14} the correct key is rarely the most frequent.
 - We developed an improvement for the linear approximation based on the additive properties of the SBox. It allows us to filter plaintexts, thus improving the quality of the data.
 - The next day we got the key:
 - Key(b=14): 5681891eec34ce1241ed0f52c9c23f65

- ▶ We expect to be able to find the key with fewer than 1000 known plaintexts with further improvements and higher computation time ($<2^{64}$ computation time).

Acknowledgements

- ▶ We would like to thank Mitsuru Matsui for offering the FEAL 25–Years Prize Problems.
 - ▶ And to the competing group that found the key for $b=15$.
 - ▶ Without whom we would not have gained the same insights and cryptanalytic ideas that we eventually came up with.
- 