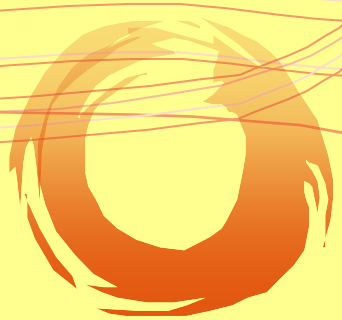
The FEAL Cipher Prize Problem

- Winner Announcement -



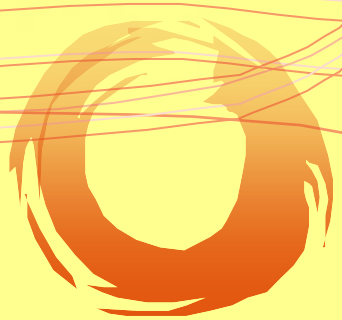
August 20 2013

Mitsuru Matsui
Mitsubishi Electric Corporation

The title of last year's rump presentation was …

Celebrating the 25th year of FEAL

- A New Prize Problem -



August 21 2012
Mitsuru Matsui
Mitsubishi Electric Corporation

The New Prize Problem

- The target cipher: FEAL-8X
  - FEAL cipher with 8 rounds and 128-bit key
  - Same as FEAL-8 except its key scheduling part
- 2^b plaintext-ciphertext pairs are given ($b \leq 20$).
- Good news: winner (min b, first) receives $1500.
- Bad news: brute force is infeasible (128-bit key)
- Deadline: CRYPTO 2013
- For more details, see

https://docs.google.com/open?id=0B3xMqN36HCf2eDVzb191R1VHY0k

Timeline

Jul 24 Received solution of b=20 from group A.

Timeline

Jul 24 Received solution of b=20 from group A.

Jul 27 Received solution of b=15 from group B.

Timeline

Jul 24 Received solution of b=20 from group A.

Jul 27 Received solution of b=15 from group B.

…

Timeline

Jul 24 Received solution of b=20 from group A.

Jul 27 Received solution of b=15 from group B.

…

Aug 15 Received solution of b=14 from group A!

Timeline

Jul 24 Received solution of b=20 from group A.

Jul 27 Received solution of b=15 from group B.

…

Aug 15 Received solution of b=14 from group A!

Aug 18 Received message from group B, saying "we are in a summer vacation".

Timeline

Jul 24 Received solution of b=20 from group A.

Jul 27 Received solution of b=15 from group B.

…

Aug 15 Received solution of b=14 from group A!

Aug 18 Received message from group B, saying "we are in a summer vacation".

Winner is group A: Eli Biham and Yaniv Carmeli

Adi Shamir will give a winner talk on behalf.