TEA analysis using genetic programming

Karel Kubíček, karel-kubicek@mail.muni.cz
Faculty of Informatics, Masaryk University

December 3, 2015

Motivation

- Cipher output should look like random data
  - but it is completely deterministic
- If we can distinguish between cipher output and truly random data, cipher is not considered to be secure
  - used as one of the test for AES candidate
- Randomness testing can be automatized
  - to save expensive time of skilled cryptanalyst

Common way of randomness testing – statistical batteries

- Common criteria:
  - for example monobit test
- From pros to cons:
  - quick
  - interpret
  - but may be hard to design
- Closed set of tests
  - there exist nonrandom data, s.t. pass tests

Tiny Encryption Algorithm

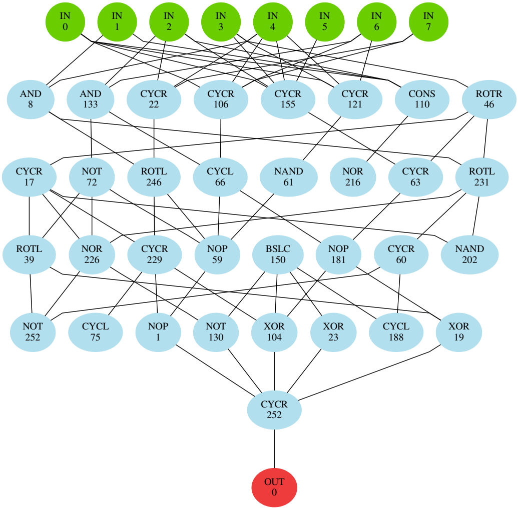
- Simple structure
- Blocks of 64 bits, 128 bits key
- Feistel network, 32 rounds
- Currently weak (related-key attack)

Tiny Encryption Algorithm

- Simple structure
- Blocks of 64 bits, 128 bits key
- Feistel network, 32 rounds
- Currently weak (related-key attack)
- Why to test TEA?
  - used by other teams ([HSIR02], [HI04], [Hu+10]) with same idea as benchmark
    - they evolved a mask to restrict the input

EACirc – software-emulated electronic circuit

- We want to create tests automatically



EACirc – process

- Generate 2 sets of test vectors
  1. output of the cipher
  2. truly random data – QRNG (from physical source)
- let the distinguisher choose, which vector is random and which is nonrandom
- fitness is $\frac{\#\text{correct quesses}}{\#\text{test vectors count}}$

Results – Plaintext mode: counter

- Plaintext: counter incremented by one for each test vector
- EACirc_{1a} nodes without shifts and rotations
- EACirc_{1b} shifts and rotations enabled

Rounds	NIST STS	Dieharder	EACirc_{1a}	EACirc_{1b}
1	1/162	0/20	100	100
2	1/162	0/20	100	100
3	27/188	1.5/20	100	100
4	183/188	6.0/20	(5.0)	100
5	188/188	16.5/20	(3.0)	(5.3)
Expected	188/188	20/20	(5.0)	(5.0)

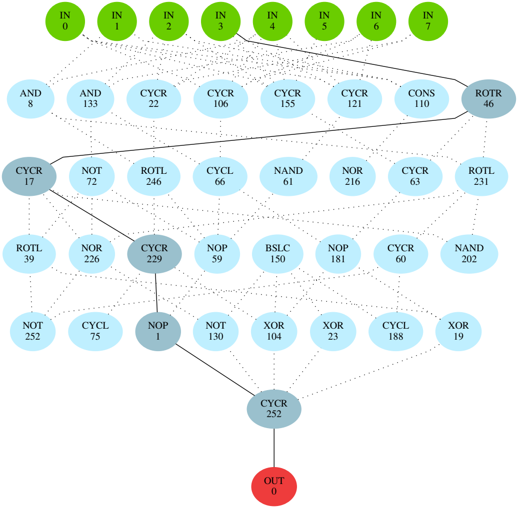
Results – Plaintext mode: strict avalanche criterion

- Plaintext: vector with two almost identical parts (first is random) differing only in a single bit

Rounds	NIST STS	Dieharder	EACirc$_2$
1	29/188	2.5/20	100
2	67/188	2.5/20	100
3	(186)/188	7.0/20	100
4	(187)/188	8.5/20	100
5	(188)/188	16.0/20	(4.5)

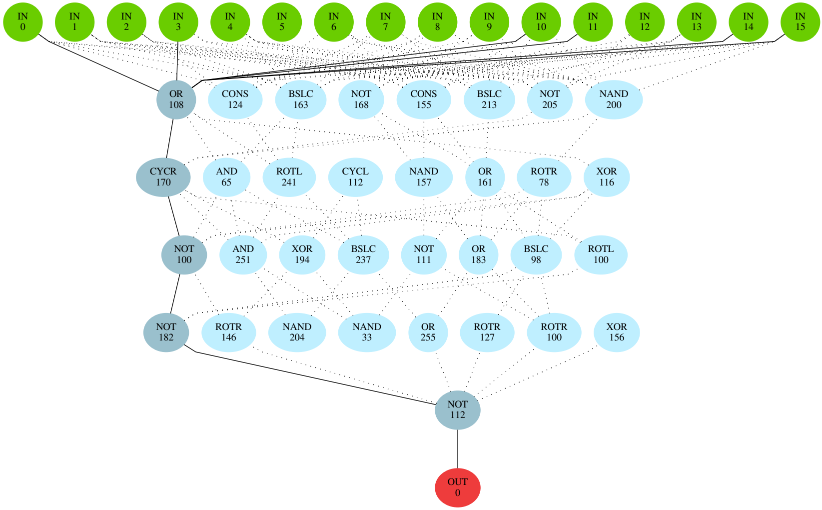
Results – interpretation

- 4 rounds TEA distinguisher (fitness 99%) for counter plaintext



Results – interpretation

- 4 rounds TEA distinguisher (fitness 99%) for SAC plaintext



Future plans

- Better analysis of defects in data.
- "Give us your data" website

Questions

Questions?

Full version of MKB paper on http://crcs.cz/papers/mkb2015

Bibliography

J. C. Hernández and P. Isasi, “Finding Efficient Distinguishers for Cryptographic Mappings, with an Application to the Block Cipher TEA”, *Computational Intelligence*, vol. 20, no. 3, pp. 517–525, 2004.

J. C. Hernández, J. M. Sierra, P. Isasi, and A. Ribagorda, “Genetic Cryptoanalysis of Two Rounds TEA”, in *Computational Science—ICCS 2002*, Springer, 2002, pp. 1024–1031.

W. Hu *et al.*, “Cryptanalysis of TEA Using Quantum-Inspired Genetic Algorithms”, *Journal of Software Engineering and Applications*, vol. 3, no. 01, p. 50, 2010.