Masarykova univerzita
Fakulta informatiky

Usage of evolvable circuit for statistical testing of randomness

Bachelor thesis

Martin Ukrop

Brno, spring 2013

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Martin Ukrop

Advisor: RNDr. Petr Švenda, Ph.D.

Acknowledgement

Thanks will be here.

Abstract

Abstract will be here.

Keywords

Keywords will be here.

Contents

1 Introduction

Text ...

2 Statistical randomness testing

- intro to statistical testing of randomness
- STS-NIST
- Diehard
- Dieharder

3 Limits and disadvantages of statistical testing

- idea -> test
- check only one specific property
- can only rarely be adapted to specific situation
- results interpretation (what is wrong?)

4 Evolution based randomness testing

- general description of GA
- idea behind EACirc
- previous evolution of EACirc (SensorSim -> bc, mgr -> today)
- capabilities of EACirc
  - general object model (+picture)
  - separate modules for projects
  - separate modules for evaluators
  - guaranteed bit-reproducibility
  - computation recommencing (state, ...)
  - static checker for pregenerated test vectors

5 Experiment settings and results

- general evolution settings
- main goal: finding strong distinguisher (over 99% for 50 consecutive generations)
- if strong distinguisher -> average generation
- if not -> AAM after test set change
- statistical batteries STS-NIST and Dieharder for reference
- STS-NIST settings (lenghts, 2 test omitted)
- STS-NIST results interpretation (scores 0, 0.5, 1)
- Dieharder settings (lengths, tests roughly corresponding to Diehard)
- Dieharder results interpretation (scores 0, 0.5, 1)

6 Control distinguishers

- introduction (what are reference points? what result are "normal" and "random"?)
- control distinguisher random-random
- dependence on number of test set and test set change frequency
- distinguishing Croatia from Germany (?)

7 Distinguishing cipher outputs from random stream

- cipher modes (iv+key initialization frequency)
- tables with results
- case of LEX (not weakening the cipher, only making shorter output)
- case of TSC (producing binary stream of 0 for 1-8 rounds) => problems in 3 Dieharder tests
- conclusions
  - more or less as statistical batteries
  - dieharder better in some case than STS-NIST (is newer and some tests are redesigned)
  - statistical tests has much more input data compared to EACirc
  - using evolved distinguisher is quick

8 Analysis of Salsa20 output stream

- learns current vectors quicker than other ciphers
- the case of six

9 Distinguishing hash outputs from random stream

- hash function settings (hash length)
- test vector generation method (4 byte counters starting from random point)
- looking for best test set change frequency
- tables with results
- conclusions (???)

10 Conclusions and future work

Text ...