Masarykova univerzita
Fakulta informatiky

FACULTAS ARTIS INFORMATICÆ • UNIVERSITAS MASARYKIANA •

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

Text ...

3 Limits and disadvantages of statistical testing

Text ...

4 Evolution based randomness testing

Text ...

5 Distinguishing cipher outputs from random stream

Text ...

6 Analysis of Salsa20 output stream

Text ...

7 Distinguishing hash outputs from random stream

Text ...

8 Conclusions and future work

Text ...