

MASARYK UNIVERSITY  
FACULTY OF INFORMATICS



# **Statistical testing of lightweight cryptography based pseudo-random number generators**

MASTER'S THESIS

**Michal Hajas**

Brno, Spring 2018

*This is where a copy of the official signed thesis assignment and a copy of the Statement of an Author is located in the printed version of the document.*

## **Declaration**

Hereby I declare that this paper is my original authorial work, which I have worked out on 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.

Michal Hajas

**Advisor:** RNDr. Petr Švenda, Ph.D.

## Acknowledgements

Thank all.

Computational resources were supplied by the Ministry of Education, Youth and Sports of the Czech Republic under the Projects CESNET (Project No. LM2015042) and CERIT-Scientific Cloud (Project No. LM2015085) provided within the program Projects of Large Research, Development and Innovations Infrastructures.

We also acknowledge the support of Czech Science Foundation, the project GA16-08565S.

## **Abstract**

Abstract to be done

## **Keywords**

randomness testing, cryptanalysis, block functions, lightweight cryptography, pseudo-random number generators

**Contents**

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Theory</b>	<b>2</b>
<b>3</b>	<b>Implementation details</b>	<b>3</b>
<b>4</b>		<b>4</b>

# 1 Introduction



## 2 Theory

### **3 Implementation details**

