FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

August 30, 2024

Statement of opponent on

"Cryptographically Secure Random Number Generators" by Mykhailo Naumenko

Summary:

The thesis presents theoretical foundations of cryptographic pseudorandom generators (PRGs), some practical constructions, and various attacks on some of the historical and more recent candidates. It is a compilation of various known results, and the author does not present any new results.

In Chapter 2, the author gives an overview of classical results on complexity theoretic foundations of PRGs such as equivalence of next bit unpredictability with pseudorandomness and constructions of PRGs from one-way permutations, respectively one-way functions. In Chapter 3, the author gives a high-level description of seven candidate PRGs used in practice. In Chapter 4, the author gives a high-level overview of four practical attacks on candidate PRGs, and an adaptation of a code of attack on the Mersenne Twister random number generator. In Chapter 5, the author presents some more advanced attacks from cryptographic literature. The last Chapter 6 is the most formal and presents attacks on congruential generators using the theory of lattices and advanced algorithms for lattice basis reduction, such as the LLL algorithm.

Computer Science Institute of Charles University
Malostranské nám. 2/25, 118 00 Praha 1, Czech Republic
sekretariat@iuuk.mff.cuni.cz
+420 951554230

Evaluation:

- *Strong points:*
  - The thesis attempts to cover a wide range of results on the foundations and practice of cryptographic PRGs.
  - The student extended and tested the code of a published attack to a different implementation of the same random number generator.

- *Weak points:*
  - The breadth of the covered material is at the cost of technical depth of the text. I would prefer a narrower selection of results covered in more detail. For example, the results covered in Chapter 2 are, by now, parts of standard textbooks such as "Foundations of Cryptography" by Goldreich or "Computational Complexity" by Arora and Barak. Thus, instead of giving incomplete proofs and pointing to original papers, it would have been better to focus on some interesting aspects of some of these proofs and cover them in more detail than in the available sources.
  - Significant parts of the thesis are written in style that would be more appropriate for a popularization article or a blog post, which often makes the details of the constructions or attacks vague.
  - The extension of the attack on Mersenne Twister by Kopp is quite minimal. The only difference seems to be in leaving out the custom implementation from the original attack and using the standard implementation from the python library. The student reused most of the code from Kopp, which should have been stated and attributed. There is only minimal discussion of the performance of the attack.
  - The author is not thorough when citing known results.

Low level comments:

- There are typographical errors throughout the text. For example, the author is consistently misusing "its" and "it's" (I would avoid the informal shortenings such as "it is" as "it's" altogether).
- The parameter ε is not used Definition 1.
- Definitions 2 and 9 are identical.
- Definition 10 of a lattice would result in the whole $\mathbb{R}^n$.
- Table 1.1 does is unclear without explaining the various properties.
- The classification of attacks at the beginning of Chapter 5 is not helpful to the reader without any explanation of these types of attacks.

- Chapter 6 misses a summary. It would be interesting to discuss the practical effects of these attacks.

Recommendation:

I see the thesis at the border of what can be accepted as a MSc thesis in mathematics. However, the student did demonstrate that he can summarize a large body of scientific literature. Also, he showed that he can adapt code of a cryptographic attack. So, despite the above weaknesses, I recommend accepting the thesis as a diploma thesis.

I would appreciate if the student explained the details of his experimentation with Kopp's attack on Mersenne Twister during the defense.

Mgr. Pavel Hubáček, Ph.D.