Report on "Cryptographically Secure Random Number Generators"

The thesis is a survey on Pseudorandom Number Generators (PRNG) and their use in cryptography. The thesis provides a computer scientific basis, then surveys practical cryptographic uses of PRNGs (in operating systems, programming languages, etc.) and finally explains some mathematical constructions and cryptanalytical attacks on them. However, the main emphasis is on the practical aspects.

In Chapter 2, the student introduces the theoretical notions using [2] (but also consulting the source [16]). Chapters 3, 4, and 5 are concentrated on practical PRNGs. Chapter 3 is a survey on their use. Chapters 4 and 5 are on the attacks. These attacks are almost always not "mathematical" but mostly "engineering" which is of course natural. Chapter 4 contains an implementation of the attack described in [33] where the student modifies the code in [33] to attack Python's random number generator.

Chapter 6 is on mathematical attacks on congruential generators. Using various sources [4, 41, 42, 6, 7] it provides explanation on two attacks on congruential generators.

Topic of the thesis: Topic of the thesis PRNGs is suitable for a Master's thesis.

Mathematical content: Mathematical content (Theoretical Cryptography, Congruential Generators, LLL) is confined to two chapters (Chapters 2 and 6), but is at a satisfactory level.

Citations/References: Many sources are used but there are few citation problems (see below).

Student's contribution: Student provides a survey covering areas in mathematics, computer science and engineering. A computer implementation of an attack is given.

The strong part of the thesis is that the student brings together many PRNGs used in practice in a very nice way. This covers a lot of references. The student walks us through all of the descriptions of those PRNGs and attacks against them. Lack of mathematical depth in these chapters is natural. However, the student includes in Chapters 2 and 6 theoretical aspects of PRNGs as well.

Important issues:

- The explanation of the attack against congruential generators (Section 6.1) could be more clear. The task is desribed as "given the outputs $a_1, \ldots, a_n$ find the output a_{n+1}" (p. 49). The attack is slightly more complicated than given here. Even if the attacker makes a wrong guess of a_{n+1}, we assume that the attacker receives the correct value again and using ideas (marked as 2. and 3.) briefly explained in p. 51, gives a polynomial time algorithm to finalize the attack. The finalization could have explained in a better way.

- Overall, many proofs are omitted. This can be understood in the introductory sections. However, for instance in Chapter 6, even if the full proofs are too long, at least the main ideas of the proofs could be explained. This is most important on p. 51 (see the previous comment).
- Some statements and claims require better referencing. Most important is in the conclusion. Author claims:

  > We have determined that PRNG can only exist if $P \neq NP$, it can be constructed from one-way functions, and the output of the random number generator can be greatly expanded.

  This is certainly not proved in the thesis. In my opinion, the statement is not necessary in the conclusion. But if included, at least it should be cited properly to avoid misunderstanding. I am sure that this is an English mishap, (the student intended to state that he had explained those issues in the thesis) but it should be clarified.

  Another case (as observed by the opponent as well) on (pp. 36–37), exact contribution of the author and that of [33] should have been clarified. It is again clear to me that it is not the author's aim to misrepresent his contribution since he clearly explains it in another paragraph.

Formal matters:

- The citations should be done within the sentence, so "end of sentence. [XX]." is not good style.
- lemma X, def Y, appendix Z $\Longrightarrow$ Lemma X, Definition Y, Appendix Z.
- Overall: Many citations are omitted. The student usually cites a reference once per section then omits it in the rest.
- Overall: English could be improved.
- A final proofreading (e.g., by the supervisor) would have improved the writing (and the previously mentioned issues) a lot.

Conclusion: Despite the shortcomings listed above, I think the thesis deserves to be recognized as successful as the student brings together a good survey on an important topic. The student should provide clarifications of the issues raised by the opponent and the supervisor (pp. 49–51 and citation issues).