The Blavatnik School of Computer Science
The Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University

בי"ס למדעי המחשב
ע"ש בלווטניק
הפקולטה למדעים מדויקים
ע"ש ריימונד ובברלי סאקלר
אוניברסיטת תל-אביב

30.12.2018

Review for Maciej Skórski PhD dissertation

Following is my review for Maciej Skórski PhD dissertation I received on 22 October 2018.

The focus of this thesis is *pseudoentropy* [Impagliazzo, Levin, Luby '89], a relaxation for the computation setting of the known notion of *entropy* [Claude Shannon '48], measuring the amount of uncertainty in a random variable. Since it was introduced, pseudoentropy, and its related notions, was found to be extremely useful abstraction to capture the way randomness is perceived from the point of view of computational bounded entities, and the works using this notion have reshaped our understanding of Cryptography and Computational Complexity. This thesis studies in depth many important aspects of pseudoentropy, and enriches our understating of this important notions, and is definitely of sufficient quality to grant a PhD degree. Yet, I found parts the writing to of inadequate quality for such a publication, and **I am asking the author to address my comments below**.

Introduction.

A work whose focus is pseudoentropy should give a more elaborated perspective on the different notion of computational entropy, such as accessible entropy, and cover the recent advances done since the publications cover in this thesis (such as the ones in the study of auxiliary information simulation).

Condensed Unpredictability.

- The first work on pseudoentropy condenser was done by HILL [Lemma 5.1.2].
- The paraph on "GL vs. Condensing" is hard to read.
- Identifying HILL pseudoentropy with the Min-entropy variant, is confusing and inconsistent with the original definition (in HILL). To the very least, explain clearly that that the original definition was given for Shannon entropy (Definition 3.4.2 in HILL).
- P 30. [Hast.] is broken reference.

Lower Bounds for Pseudoentropy Chain Rules and Transformations

- The fact that your BB lower bound only applies to **restricted types** of adversaries should be out much more clearly in the description of your result (both in the abstract and in the intro).
- Fig 1 is unreadable (at least without magnifying glass...)
- P. 53. Paragraph "The adversary" is hard to read

Simulating Auxiliary Information

- This section is hard to read. In particular Algorithm 1. Is very hard to follow

- There is a typo in (4). I guess first line should be g^0
- Fn 11 is incomplete
- P 89. Why the proof amuses?

Best Generic Attacks Against Pseudoentropy

- Introduction is too short to deliver the scope of this result
- Fig 1 is unreadable

Geometric Characterization

- Lemma 3. D_i's are undefined
- Proofs of Theorems 1-3 are missing!

Bibliography

The different bibliography parts ae using different notations, some items are missing and one section has no bibliography at all! . I think it is important to have a single bibliography for the whole thesis.

Sincerely,

Prof. Iftach Haitner
Associate Professor
Blavatnik School of Computer Science, Tel Aviv University.