Annex 7: Habilitation thesis reviewer's report

Masaryk University	
Faculty	Faculty of Informatics, MU
Habilitation field	Informatics
Applicant	RNDr. Jan Bouda, Ph.D.
Unit	Faculty of Informatics Masaryk University, Brno
Habilitation thesis	Randomness in (Quantum) Information Processing
Reviewer	Prof. Dr. Renato Renner
Unit	Institute for Theoretical Physic, ETH Zurich, Switzerland

Reviewer's report (extent of text up to the reviewer)

The topic of the habilitation thesis of Dr. Jan Bouda is concerned with the use of randomness in quantum information processing. In particular, it addresses the question of how (and under which conditions) low-quality randomness can be turned into high-quality randomness. Furthermore, he investigates the possibility of using low-quality randomness directly in cryptographic applications.

Bouda has made several solid contributions to this area of research. Among them is a careful analysis of the number of unitaries needed for a two-design, a concept that plays an important role in quantum information theory. Another is the investigation of the security of private quantum channels, where Bouda proposed and analysed an attack that may be regarded as a quantum analogue of the known plaintext attack.

One particularly important result is the finding that the use of weak randomness in a quantum key distribution protocol can lead to security loopholes. Because, in realistic implementations, one cannot usually assume that the randomness used by the legitimate parties is perfect (although perfect randomness is assumed in most known security proofs), this is of high practical relevance.

Conversely, however, Bouda has also been able to show that, while classical encryption schemes cannot usually tolerate weak randomness, this problem can be circumvented by employing a quantum ciphertext. In other words, even if the key used for encryption is sampled from a weak random source, secrecy can be guaranteed in most cases.

Another important line of results achieved by Bouda concerns the generation of randomness using physical devices (such as the camera of a mobile device). In his work, he showed that such randomness generation is possible with state-of-the-art equipment and appropriate software for post-processing the raw randomness. Here, randomness extractors play a crucial role, and Bouda has also made significant contributions to the development of such extractors.

In his very recent work, Bouda extended these considerations to a device-independent setting. This means that the quality of the generated randomness can be guaranteed even if the devices that produce them are only partially trusted. This, again, is of high practical importance, as realistic devices do not usually meet the theoretical specifications perfectly.

The contributions of Bouda, as described above, have appeared in reasonable physics and computer science journals, such as Physical Review A and the Journal on Quantum Information and Computation, as well as in conference proceedings. Taken together, they show that Bouda has a well-defined and well motivated research program. He is a respected member of the quantum information research community and he entertains various international collaborations.

Summarising, Jan Bouda has made a large number of relevant contributions in the area of quantum information theory. He has clearly demonstrated his expertise in this field and shown his ability to lead a well-motivated and productive research program. Given these achievements, I am happy to recommend acceptance of his habilitation thesis.

Reviewer's questions for the habilitation thesis defence (number of questions up to the reviewer)

1. There are obviously many ways to characterise weak randomness. How universal are the various results on weak randomness? In other words, to what extent do they depend on the precise definition of what one calls "weak"?
2. In practice, it is usually possible to extract almost perfect random bits from weak randomness. Why is it still relevant to study the workings of cryptographic schemes when used directly with weak randomness?
3. From a conceptual point of view, what is the difference in using "classical" physical devices (such as random number generators based on thermal noise) from quantum random number generators (e.g., those based on a beam splitter)? Is there a clear advantage when using the latter?
4. What are the most important open research problems concerning the use of weak randomness in quantum information processing?

Conclusion

The habilitation thesis submitted by Jan Bouda entitled *"Randomness in (Quantum) Information Processing"* **meets** the requirements applicable to habilitation theses in the field of Informatics.

In Zurich on October 30, 2015 Renato Renner (signature)