Habilitation Thesis Reviewer's Report

Masaryk University	
Faculty	Faculty of Informatics
Procedure field	Informatics
Applicant	RNDr. Petr Švenda, Ph.D.
Applicant's home unit, institution	Faculty informatics, Masaryk University
Habilitation thesis	Examining and exploiting randomness for cryptography
Reviewer	**Prof. Krzysztof Pietrzak**
Reviewer's home unit, institution	IST Austria, Austria

The research presented in this thesis can be roughly split in three main topics
(1) the work of Petr which he started during his PhD on key establishment in compromised ad-hoc networks.
(2) his work on randomness testing of reduced round cryptographic primitives.
(3) his work on biases/weaknesses in (RSA) key-generation in the wild.

Of this part (3) is the most recent and (in my opinion) by far the strongest, so let me elaborate on that. The main results are in USENIX'16 (The million-key question - investigating the origins of RSA public keys) and CCS'17 (The return of Coppersmith's attack: Practical factorization of widely used RSA moduli).
This two papers show an interesting story on using weaknesses of RSA key-generation in the wild, with the USENIX paper focusing on identifying and classifying the sources (crypto libraries) the keys come from and the CCS paper showing how a particular weakness in sampling keys used on a widely deployed (Infineon) card can be exploited to identify and factor (and thus recover secret keys).
This line of research shows a very coherent research program starting with data acquisition (of RSA public-key ``in the wild"), an effort to classify them, reverse engineering of the sampling algorithms which then culminated in the detection of a weakness that can be efficiently detected and exploited. This is first rate research in applied security that (unfortunately) we see quite rarely coming from eastern European countries. Although both papers have several authors, most of them a very junior, so it shows that Petr can engage students into his research.

My recommendation to grant habilitation is based on these recent works.

Petrs work on topics (1) and (2) is solid but clearly not as sophisticated, interesting or impactful as (3). It also appeared in much weaker venues (than CCS or USENIX).

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

Conclusion

The habilitation thesis entitled "*Examining and exploiting randomness for cryptography*" by Petr Švenda ***fulfils*** requirements expected of a habilitation thesis in the field of Informatics.

In Klosterneuburg on

…………………………
signature