MASARYKOVA
UNIVERZITA

Annex No. 11 to the MU Directive on Habilitation Procedures and Professor Appointment Procedures

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. Vincent Rijmen**
Reviewer's home unit, institution	KU Leuven, ESAT/COSIC, Belgium

This thesis contains 10 research articles preceded by an extensive introduction and summary of the research work performed by dr. Švenda. The results of this research can be grouped into three categories. The first category contains the innovative approaches to evaluate the quality of (pseudo-)random bit generators that have been developed. The second category contains an important follow-up result of the randomness tests: the detection and exploitation of deficiencies found by his team in a commercial library for the generation of RSA moduli, which allowed to break large classes of RSA keys that were in practical use at the time of discovery. The third category contains the results on secure key generation in distributed environments where not all nodes can be trusted.

Except for cryptographic hash functions and one-way functions, all cryptographic primitives use secret keys. The generation of these keys is a crucial step. However, generating long sequences of secret, or unpredictable, bits, turns out to be very difficult or costly. Regularly, (pseudo-)random number generators that are used in practice, are shown to have some weakness. Randomness tests are an important means to detect these weaknesses. Hence, we can characterise dr. Švenda's work as being a cornerstone for cryptographic applications.

The impact of dr. Švenda's work on the factoring of RSA moduli is very significant. All over Europe authorities, providers and users learnt that their cryptographic applications were less secure than they thought, or even dangerously weak. Software has been urgently updated, keys have been replaced. The name of dr. Švenda and his research team were on the front pages of all cryptographic news bulletins.

The work on secure key generation in distribution environments did not receive as much attention yet as the work on RSA, but it is also very important. It will receive more attention with the spreading of IoT nodes and when future cyberattacks will force developers to improve the key generation and key distribution on their IoT appliances.

From the 10 research articles included in this thesis, one has been published at Usenix, which accepts only excellent scientific work with a significant impact on practical applications of

computer security and cryptography. Two further articles have been published at CCS, which is also one of the top 5 international conferences in the field of computer security. Four more articles have been published at conferences with proceedings published by Springer in its prestigious LNCS series. The remaining three articles have also been published at internationally competitive conferences.

This thesis shows that dr. Švenda delivers scientific work of an outstanding quality, and that he can compete at the international level. Dr. Švenda masters his research topic. From the lists of coauthors on the papers it becomes clear that Dr. Švenda can effectively and efficiently lead a team of junior researchers and collaborate with researchers from other research institutions.

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

In your opinion, what is the likelihood to detect biases in ECDSA key-generation libraries? Would a bias there lead to a failure in security similar to ROCA? Can one derive recommendations for the use of RSA or ECDSA in practice?

Conclusion

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

In Leuven-Heverlee on 23 March 2019