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. Kenny Paterson** |
| **Reviewer's home unit, institution** | Royal Holloway, University of London, Egham, UK |

The applicant's thesis presents published work in three main directions: the design and analysis of adaptive tests of randomness; the analysis of biases in software and hardware implementations of RSA keypair generation (and the attendant security vulnerabilities that arise when this is done in an insecure manner); and topics in the domain of key distribution and secrecy amplification protocols for wireless sensor networks.

The first topic I find very interesting and novel. It connects statistical randomness testing in the traditional sense with techniques from cryptanalysis, such as finding low-degree approximations to cryptographic functions. The result is a set of methodologies for semi-automatic generation of new and high-performing tests of randomness. These are compared extensively against standard tests (such as the NIST test suite) in specific settings, such as analysis of reduced-round versions of eSTREAM stream cipher candidates. The work is published in respectable conference venues (SECRYPT 2013, SECRYPT 2017, NordSec 2009).

The second topic is represented in the thesis by extremely high-quality work, as can be seen from the top tier security conferences where it was published (USENIX Security 2016, ACSAC 2017, ACM CCS 2017 (two papers)), the award of prizes for the work (e.g. a best paper award at USENIX Security 2016), and the very significant impact that the work has had since its publication. The key observation on which the work is based is that different methods for generating primes for RSA moduli lead to different, detectable fingerprints in the eventual RSA public keys. This makes it possible to carry out surveys that allocate public keys to likely cryptographic libraries and thereby evaluate the popularity of the different libraries. This avoids having to rely on the previously state of the art "indirect" methods for assessing popularity. Very surprisingly, this approach also led directly to the discovery of a major security flaw in a specific vendor implementation of primality generation. In turn, this allowed the resulting RSA keys to be broken (using a clever mathematical cryptanalysis based on Coppersmith's algorithm). This flaw impacted several customers of the vendor including the government of Estonia who has used the vendor's smartcards in their national identity-card system. The work

was widely reported in the international press and has quickly become a celebrated example of how over-optimisation in cryptography can lead to severe security vulnerabilities. In my view, the paper was one of the research highlights of 2017 in the applied cryptography community, and it is recommended reading for my students.

The third topic is seemingly not such a key part of the applicant's on-going research, and concerns methods for distributing keys in wireless sensor networks and then how to recover from intrusions in such networks by using keys in adjacent nodes to derive fresh keying material. The work, once again, was published in respectable international venues (CANS 2016, SecureComm 2012, EuroGP 2012).

The thesis provides in its "Commentary" part a lucid and accessible introduction to the detailed research that follows in Part II. In combination, the three topics presented, and the related papers, represent a very satisfying collection of published research works of good quality. The best of the work is outstanding in every dimension and has rightly brought the applicant increasing international recognition.

I commend the thesis to the habilitation committee members.

**Reviewer's questions for the habilitation thesis defence**:

1. Is it possible to apply more modern learning algorithms to the problem of developing automated tests of randomness and finding distinguishers for cryptographic algorithms? The thesis hints in this direction with a mention of deep neural networks, and this might be a direction that it would be profitable to explore further.
2. Do the techniques for RSA key fingerprinting extend to other types of keys, for example ECC keys?
3. How would the applicant frame a researcher's responsibilities in respect of disclosure of vulnerabilities found in deployed cryptographic systems to affected parties, especially those deployed in hardware where patching may be expensive and difficult to do in a timely fashion (in contrast to hardware)?

**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 Zurich on 29th March 2019