Supervisor's statement on Ph.D. candidate Ing. Stanislav Jeřábek

Student: Ing. Stanislav Jeřábek
Thesis title: Differential Power Analysis Countermeasures in Programmable Hardware
Supervisor: doc. Ing. Jan Schmidt Ph.D.
Co-supervisor: Dr.-Ing. Maritn Novotný Ph.D.

Ing. Stanislav Jeřábek started his Ph.D. study in the program "Informatics" at the Faculty of Information Technology (FIT) on September 1st, 2016. After a short time, he came with his innovative technique of countermeasures against side-channel analysis. He was able to communicate his idea on conferences and workshops, and within the Digital Design and Dependability research group. He also spent time at stays at University of Bochum (2018) and KU Leuven (2022). He defended his thesis proposal on November 11th, 2019.

Although the work did delay at times, as the student provided valuable services to the students' community in his multiple capacities, results comparative to the state of the art were finally achieved, leading to the present Ph.D. thesis. The results were published in WoS indexed conferences (DSD, DDECS).

Since the start of his Ph.D. study, the student has been an active member of the Digital Design and Dependability research group and has supervised several bachelor and diploma theses. He participated in research funded by grant agencies, namely:

- CELSA project "DRASTIC: Dynamically Reconfigurable Architectures for Side-channel analysis protection of Cryptographic implementations" (CELSA/17/033), and
- GA16-05179S of the Czech Grant Agency, "Fault-Tolerant and Attack-Resistant Architectures Based on programmable Devices: Research of Interplay and Common Features" (2016-2018)

Besides those grants, he was awarded support from internal CTU grants. His current h-index is 1.

The main contributions of the thesis are:

- A novel method of countermeasures against side-channel analysis, its combination with other methods and evaluation; first design of lightweight countermeasures for complex ciphers.
- Bringing attention to the control part of the circuit, as opposed to the usual focus on side channels of the datapath, optimization of the control algorithm and safe controller design.

I can state that Stanislav Jeřábek fulfilled all requirements for the successful accomplishments of his Ph. D. study. He has proven to be scientifically qualified and has proven the ability to conduct his own research and publish the result. Therefore,

I recommend accepting this thesis for defense.

Prague, Aug. 28th, 2023

doc. Ing. Jan Schmidt Ph.D.
Czech Technical University in Prague
Faculty of Information Technology
Dept. of Digital Design