GEORGE MASON UNIVERSITY

Department of Electrical and Computer Engineering

4400 University Drive, MS 1G5, Fairfax, Virginia 22030
Phone: 703-993-1569; Fax: 703-993-1601; Web: http://ece.gmu.edu/

Nadacia Intenda
Prazska 11
811 04 Bratislava
Slovakia

10/28/09

Subject: Recommendation for Michal Varchola

To Whom It May Concern:

It is a great pleasure and honor for me to recommend Michal Varchola as a candidate for scholarship within "Supporting individuals" project of the "Intenda" organization. I worked with Michal in my capacity of Co-Director of the Cryptographic Engineering Research Group (CERG) at George Mason University when he joined us as a research scholar for 5 months from February to July 2009 as short term research scholar. During his time here, he was extremely hard-working, responsible, and very committed to his research.

Michal Varchola was continuing research related to his PhD thesis topic on "True Random Numbers Generators (TRNG) for FPGAs". He has invented an novel randomness source for TRNGs during his stay in our laboratory. I had a Master's student during this time working on the same topic, but using a classical approach, which is very different from Michal's. Michal's initial results suggest that his new approach has many advantages over existing designs, however further research is necessary. He has published the preliminary results in:

Varchola, M., Drutarovský, M.: *New FPGA based TRNG Principle Using Transition Effect with Built-In Malfunction Detection*, Proceedings of the 7th International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices – CrytArchi 2009, Prague, Czech Republic, June 24-27, 2009, pp. 150-155.

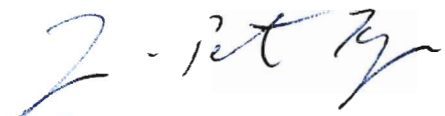
In addition to his research, Michal has actively participated in several research activities of CERG. Most importantly, he helped with the initial stages of the ATHENa – Automated Tool for Hardware EvaluatioN project, which enables fair comparison of hardware implementations (*Fair Comparison of Hardware Implementations of Cryptography without Revealing the Source Codes*, 7th International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices - CrytArchi 2009).

Furthermore, Michal integrated very well in our research group and actively participated in our day-to-day activities e. g.: reviewing of scientific papers submitted to Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2009 and working on a case study regarding hardware and tool selection for PCI Express – FPGA interconnection. We were very happy that he joined our team even if it was for only 5 months.

Michal Varchola is in his last year of study towards the PhD degree. He is continuing his work on his new TRNG design. In order to provide exceptional results, it will be more than helpful to present his results on well known conferences and to take measurements in high-end laboratories abroad. That is why Michal Varchola's work would be an ideal match for the scholarship of your organization.

If you need any further information, please do not hesitate to contact me

Sincerely



Dr. Jens-Peter Kaps
Assistant Professor
Phone: +1-703-993-1611
E-Mail: jkaps@ece.gmu.edu
Web: http://ece.gmu.edu/~jkaps