GEORGE MASON UNIVERSITY

The Volgenau School of Information Technology and Engineering
Department of Electrical and Computer Engineering
4400 University Drive, MS 1G5, Fairfax, Virginia 22030
Phone: 703-993-1569; Fax: 703-993-1601

Kris Gaj
ECE Department
George Mason University
e-mail: kgaj@gmu.edu
phone: +1 571 218 0270
url: http://ite.gmu.edu/~kgaj/

October 29, 2009

Nadacia Intenda
Prazska 11
811 04 Bratislava
Slovakia

To Whom It May Concern:

It is my great pleasure to recommend Michal Varchola for a scholarship within "Supporting individuals" project of "Intenda" organization. I have met Michal for the first time in June 2008, at the 6th International Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices - CryptArchi 2008, in Tregastel, France. During this workshop, Michal and his supervisor, Dr. Milos Drutarovsky have presented a very interesting article on their research in the area of True Random Number Generators, and their implementation using Actel FPGAs. I was very impressed by this work, and in November of 2008, I invited Michal to spend five months in my laboratory at George Mason University (GMU). During his stay at GMU, from February to July of 2009, Michal, worked very closely with me on several research projects. Additionally, Michal was also attending my graduate class called Computer Arithmetic. As a result, I had an opportunity to interact closely with Michal on a daily basis, and to get to know him at the both professional and personal levels.

Michal Varchola is an exceptional graduate student and researcher. He is among the top 3% of the very best graduate students I happened to work with over my ten-year period as a professor at George Mason University. Michal is unique in that he combines all qualities necessary to succeed in science. He is brilliant and innovative. He is a team player contributing his ideas to the entire research group and helping others to succeed. He is also mature, independent, and goal-oriented, and used to overcoming obstacles on the way.

Several qualities of Michal have particularly impressed me during his stay at GMU. He was very focused and academically mature. After a relatively short period of initial discussions, we was able to very effectively pinpoint the best areas for the joined research and collaboration. As a result, he contributed immensely to two projects started by our team in Spring 2009: ATHENa – An Automated Tool for Hardware Evaluation, and implementation of Spectral Modular Arithmetic in Reconfigurable Hardware. In the first area, Michal has contributed the investigation and development of scripts for benchmarking of cryptographic hardware using Actel FPGAs. This was a very significant extension of the GMU project, which previously was planned to be based only on Xilinx and Altera tools. This extension was possible because of the Michal's earlier expertise in development of cryptographic modules using Actel FPGAs, and his excellent knowledge of the Actel design flow. In the area of Spectral Modular Exponentiation, Michal has contributed a thorough investigation of the earlier work in this area by the groups of Prof. Koc and Prof. Sunar, and the development of the Matlab program for the effective choice of parameters for the most popular public key cryptosystems. This effort required getting familiar with the quite complex mathematical background based on the combination of Number Theory, Signal Processing Algorithms, and Computer Arithmetic. It is my strong intention to continue collaboration with Michal in these two areas, which is likely to lead to significant future publications.

The other quality of Michal that impressed me the most were his extremely strong experimental skills and ability to work with complex measurement equipment (logic analyzers, oscilloscopes, signal generators, etc.). In particular, during his stay at GMU, Michal has developed an experimental setup, based on the Xilinx FPGA boards and the measurement equipment available in our lab, in order to thoroughly test a novel True Random Number Generator, he invented as a part of his Ph.D. research. He has also collaborated with my colleague, Prof. Ken Hintz, on the development of an experimental setup for another project in the area of land mine detection.

During his stay at GMU, Michal has given several presentations at the meetings of the GMU Cryptographic Engineering Group. These presentations covered a wide range of topics, from the background and innovative ideas in the area of True Random Number Generation, through Actel Design Flow, Spectral Modular Exponentiation, to reports on papers submitted to CHES 2009, which Michal has helped to review. Each of these presentations was truly outstanding, extremely well organized, very clear and well thought through. Michal is one of the best speakers among all graduate students I have ever worked with.

Michal has impressed me with both the depth and breadth of his research and knowledge. He developed a truly impressive, and very innovative idea for a new family of True Random Number Generators, which offers several potential advantages over previously reported designs. At the same time, he does not want to limit his future (post Ph.D.) research to this single subject, but rather uses every possible opportunity to extend his horizons, and get knowledge and proficiency in other areas. In particular, during his stay at GMU, Michal attended two graduate courses in the area of Computer Arithmetic and Digital Signal Processing Hardware Architectures.

Collaborating with Michal is always a true pleasure, as he is always extremely friendly, humble, and willing to share his knowledge and experiences with others. During his stay at GMU, Michal has integrated very quickly into the GMU research group, and established close friendships with his labmates and several other persons he interacted with.

At this point, Michal Varchola is in his last year of study toward his PhD degree. I believe that he has a great potential to develop a truly outstanding Ph.D. thesis, which will be at the very forefront of the worldwide research in the area of True Random Number Generation. This thesis is likely to result in publications at the top cryptographic conferences, and in the renowned scientific journals. In order to take full advantage of this potential, a substantial funding is required. This funding can be used to support Michal's visits in the top research laboratories, where he can perform further investigation of his ideas using the world-class measurement equipment and high-end FPGA boards. The funding will also be necessary to properly disseminate the results of Michal's research through his attendance and presentations at the top international conferences, such as CHES, FPL, FCCM, etc. Therefore, I highly recommend and enthusiastically embrace granting your scholarship to this truly outstanding and exceptionally gifted candidate!

Sincerely

KGaj

Kris Gaj