CURRICULUM VITAE

Personal Details:

Name:	Ing. Michal Varchola, PhD.
Address:	Humenská 16, Košice, 040 11
Cell phone:	+421 903 582477
e-mail:	michal@varchola.com
Date of birth:	August 19, 1984
Marital status:	Single
Citizenship:	Slovak Republic

Current Status:

Researcher & Teacher in position of Assistant of Professor
Technical University of Košice, Faculty of Electrotechnics & Informatics
Fields of interest:

- *Applied Cryptography:*
  Implementation and side channel analysis of symmetric and asymmetric ciphers, true random number generators, and physical unclonable functions
- *Embedded Systems and electronics:*
  FPGA design, VHDL, C for microcontrolles, Matlab, PCB design, SPICE
- *Project Management:*
  Fundamentals of the project management aimed to the IT

Developer of commercial embedded systems and electronics

- Systems aimed to information security, signal processing and industry control
- Current cooperation with companies: Micronic, s.r.o. and CMMS, s.r.o.

Education:

2007 – 2010 **Technical University of Košice, Faculty of Electrotechnics & Informatics**
Field of Study: Cryptography in embedded systems
Degree: PhD. (Philosophiae Doctor)

2002 – 2007 **Technical University of Košice, Faculty of Electrotechnics & Informatics**
Field of Study: Electronics and Multimedia Communications
Degree: Ing. with honours (i. e. Master with honours)

1998 – 2002 **Secondary Electrotechnical School Košice**
Field of Study: Automatization

Stays abroad:

Oct. 2010 – Feb. 2011 **Research Stay** concerned to FPGA synthesis of lightweight Elliptic Curve Processor resistant to side channels attacks.
Invited lecture: Cryptographic True Random Number Generators for FPGAs
Ruhr Universität Bochum, Embedded Security (EmSec) group, Germany

February – July 2009 **Research Stay** concerned to Random Number Generators and Spectral Modular Arithmetic and project ATHENa (Automated Tool for Hardware EvaluatioN)
George Mason University, Cryptography Engineering Research Group
Fairfax, VA, USA

January – April 2008 **Research Stay** concerned to Random Number Generators
Université Jean Monnet, Laboratoire Hubert Curien
Saint Etienne, France

April – May 2002 **Study stay**, Leonardo Da Vinci Exchange Program
Poweria Pilot Factory, Kemijärvi, Finland

March 2001 **Study stay**, Leonardo Da Vinci Exchange Program
Gewerblich – technischen Bildungsstätte GmbH – Leipzig, Leipzig, Germany

Work experience:

2010 –	Technical University of Košice, Faculty of Electrotechnics & Informatics Researcher & Teacher in the area of electronics and embedded cryptographic systems
2008 –	Micronic s.r.o. Developer of embedded systems based on FPGAs
2004 – 2008	INSPECT – Košice Developer of embedded systems based on MCUs
2001 – 2004	INSPECT – Košice Trainee

Awards:

September 2009	Perfect Research Results in Ph.D studies Award Počítačové Archtektury & Diagnostika (PAD) (Computer Architectures & Diagnostic), Hejnice, Czech Republic
May 2005	1st place in Students' research competition ŠVOS Technical University of Košice, Faculty of Electrotechnics & Informatics
April 2004	2nd place in category E of 5th Exporecerca Jove Institut D'Investigacions Científiques i Ecologiques, Barcelona, Spain
July 2003	Expo Science International 2003, Moscow, Russian Federation (participant)
May 2002	1st place in Slovak National Students' research competition SOČ in Electronics
February 2002	2nd place in Slovak National Students' competition ZENIT in Electronics
February 2001	2nd place in Slovak National Students' competition ZENIT in Electronics

Important Publications:

1. Varchola, M., Drutarovský, M.: Cryptographic True Random Number Generator with Malfunction Detector: Mathematical Model of the Noise Source, Synthesis and Testing in FPGAs, and Built-In Malfunction Detector Architecture, LAP LAMBERT Academic Publishing, Germany, March 2011, paperback, 168 pages, ISBN: 978-3844319415
   http://www.amazon.com/Cryptographic-Random-Generator-Malfunction-Detector/dp/3844319417/ref=sr_1_1?ie=UTF8&s=books&qid=1302597228&sr=8-1

2. Varchola, M., Drutarovský, M.: New High Entropy Element for FPGA based True Random Number Generators, In Proceedings of 12th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, August 17-20, 2010, Springer, 2010, pp. 351–365

3. Varchola, M., Drutarovský, M.: Embedded Platform for Automatic Testing and Optimizing of FPGA Based Cryptographic True Random Number Generators. Radioengineering – Special Issue on Electronics and Software for Security and Defense, No.4. Vol.18, December 2009, pp. 631-638.

4. Fischer, V., Bernard, F., Bochard, N., Varchola, M.: Enhancing security of ring oscillator-based TRNG implemented in FPGA. IEEE International Conference on Field Programmable Logic and Applications (FPL), 2008, Heidelberg, Germany.

5. Drutarovský, M., Varchola, M.: Cryptographic System on a Chip based on Actel ARM7 Soft-Core with Embedded True Random Number Generator, IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS), pp. 164-169, 2008, Bratislava, Slovakia

Important Research Projects:

1. MonAMI - Mainstreaming on Ambient Intelligence 035147, EU 6th Framework Programme, January 2007 – April 2008
2. SMILING – Self Mobility Improvement in the eLderly by counteractING falls 215493, 7th RTD Framework Programme - Specific Programme Cooperation. June 2008 – September 2008
3. Reconfigurable Platforms for Wideband Wireless Communication Networks, Slovak scientific project VEGA 1/4088/07 of Slovak Ministry of Education, September 2007 – now
4. A Remote Control Laboratory for Experimental Verification of Complex Reconfigurable systems Implemented in FPGAs, Slovak scientific project KEGA 3/5238/07 of Slovak Ministry of Education, September 2007 – now
5. High Speed Syntactic Landmine Detection and Classification, Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA, USA, June-July 2009 (https://zonkil.gmu.edu/spr/spr_people.html)
6. Centre of Information and Communication Technologies for Knowledge Systems (project number: 26220120020)
7. Centre of Information and Communication Technologies for Knowledge Systems (project number: 26220120030)

Skills:

General PC skills: Microsoft Office, Microsoft Windows, Internet, Design of Web Pages, Adobe Photoshop, Corel DRAW

Specialized PC & electronics skills: ANSI C, AVR assembler, x51 assembler, VHDL, OrCAD SPICE, OrCAD Capture, OrCAD Layout Plus, KEIL uVision for ARM & x51 MCUs, Freescale CodeWarrior for HCS08 & Coldfire MCUs, ATMEL AVR Studio for AVR MCUs, Quartus for ALTERA FPGAs, Libero for ACTEL FPGAs, ISE and EDK for XILINX FPGAs, Mentor Graphic ModelSim, PCI Express, Matlab, ZigBee wireless networking, Analog & Digital electronics, Labview, Cortex M0,1,3 MCUs, Altium Designer

Languages skills: **Slovak** – native
English – FCE exam

	Understanding	**Speaking**	**Writing**
English	C1	C1	C1
German	A2	A2	A2
Russian	A2	A2	A1

(Foreign language skills according to CEF level)

Driving license: A, B

Others activities:

November 2006 European Youth Forum, Strasbourg, France

June 2006 Contact Making Seminar – "Let's project" Cracow, Poland

2005 – 2007 Member of Chairmanship in Non Government Organization ÚLET

2005 – 2008 Fashion photographer for M.S. Production Model Agency

Interests:

LF & HF, Digital & Analog Electronics
Designing of Vacuum Tube High – End Audio Systems
Digital photography
Mountain biking, Mountain – climbing, Downhill skiing
Traveling
Art