Marcin Rogawski

George Mason University,
ECE Department, CERG,
4400 University Drive, MS 1G5
VA 22030, USA + 703-993-1561 (work)
email: mrogawsk@gmu.edu, mrogawski@poczta.onet.pl

EDUCATION

2008 – present
PhD program, Electrical and Computer Engineer,
George Mason University, Fairfax, USA

1998 – 2003
MS, Computer Engineering, 2003
Military University of Technology, Warsaw, Poland
Faculty of Cybernetics, Specialization: Cryptology
Thesis title: Analysis of hardware implementation of Hierocrypt-cipher using reconfigurable devices.

Aug. 2002
Kerberos, Warsaw, Poland
students training - LAN implementations (Firewall CheckPoint-1 and CheckPoint- NG), security hardening of Microsoft Windows family

Jul. 2001
Institute of Mathematics and Cryptology (Military University of Technology), Warsaw, Poland
students training - software implementations (C/C++) of crypto algorithms

AWARDS

First award in the Contest for the best MS Thesis in the area of Cryptography and Information Security defended at a Polish university in the period 2002-2003, 7th National Conference on Applications of Cryptography, Warsaw, Poland, 2003.

RESEARCH INTERESTS

Cryptography
- Design of block and stream ciphers
- Elliptic and Hyperelliptic Curve Cryptography

Cryptanalysis
- linear and differential cryptanalysis
- algebraic attacks

Reconfigurable Computing
- efficient implementations of crypto algorithms and security protocols in programmable logic

IPSec and other Applications of Cryptogrpahy
Micorocontroller development
Implementations of Operating Systems

Network Security

RESEARCH AND DEVELOPMENT

Aug. 2003 – Jul.2007, Prokom Software S.A., Warsaw, Poland

Designed and developed:

- FPGA-based crypto-coprocessor in Motorola Power PC environment
- FPGA-based modular arithmetic and crypto coprocessors in Renesas H8S/2300 environment
- single-task operating system for computer device extended physical security
- middleware and low-level software of RTOS based on uC/OS II
- FPGA implementations of selected eSTREAM contest candidates
- FPGA implementations of most commonly used stream ciphers (A5, BGML, E0, Helix, Leviathan, Lili-128, Mir-1, Mugi, Rabbit, RC-4, Sobber-16, VMPC, W7)
- hardware implementations of AES, 3DES, SHA-1, SHA-2, MD-5, RIPEMD-160, in Altera FPGAs for the Nefryt IP Encryptor device

Sep. 2002 – May 2003 Military University of Technology, Warsaw, Poland
Designed and developed:

- hardware implementations of Hierocrypt-3 and Camellia in Altera FPGAs

EMPLOYMENT

Aug. 2008 – present, **George Mason University**, Fairfax, USA, full time student,
Teaching Assistant (ECE 447 Single-Chip Microcomputers, ECE 511 Microprocessors)

Mar. 2007 – Aug. 2008, **MKS Sp. z o.o.**, Warsaw, Poland, full time job,
Software Engineer

Jan. 2004 – Jul. 2007, **Prokom Software S.A.**, Warsaw, Poland, full time job,
Software and Hardware Engineer
Developed multiple VHDL and AHDL implementations of cryptographic algorithms and security protocols.
Developed multiple avr-gcc, h8s-gcc implementations of RTOS and low, middle-level software.
Primary designer of Nefryt IP encryptor device.

System Administrator of TEMPEST Computer

Aug. - Dec. 2003, **Prokom Software S.A.,** Warsaw, Poland, commission contract,
AHDL, VHDL implementations (ALTERA Cyclone family)

Aug. - Nov. 2003, **Polish Ministry of Defense** – Military Unit JW2474, Bialobrzegi, Poland, full time job,
Commander of encryption platoon

Sep. 2002, **Polish Ministry of Defense** – Polish Task Force for the Informal Meeting of NATO Defense Ministers, Warsaw, Poland
Liaison Officer to the delegation of Spain

Jun. 2001 – Jul. 2002, **IT Business Centre**, Warsaw, Poland, part time job as a student,
System Administrator, Internet Applicatons Designer

Designed, implemented and administered databases and Internet applications using Linux, PostgreSQL, PHP, and OpenSSL.

PUBLICATIONS

- M. Rogawski - Hardware evaluation of eSTREAM Candidate - comparison, 11th Polish National Conference on Applications of Cryptography, ENIGMA 2007 Warsaw, Poland, May 2007
- M. Rogawski - Hardware evaluation of eSTREAM Candidates: Grain, Lex, Mickey128, Salsa20 and Trivium, State of the Art of Stream Ciphers Workshop, SASC 2007, Bochum, Germany, Feb. 2007
- M. Rogawski - "FPGA-based crypto co-processors with stream ciphers" - Cryptographic Architectures Embedded in Reconfigurable Devices – CryptArchi, Kosice, Slovakia, Jun. 2006
- M. Rogawski - "Hardware-oriented stream ciphers" - 10th Polish National Conference on Applications of Cryptography, ENIGMA 2006, Warsaw, Poland, May 2006
- M. Rogawski - "Stream ciphers in reconfigurable devices " - 9th Polish National Conference on Applications of Cryptography, ENIGMA 2005, Warsaw, Poland, May 2005
- M. Rogawski - "Architectures of crypto co-processors based on reconfigurable devices" - 2nd Workshop of Cryptography and Information Security, Lublin, Poland, May 2004
- M. Rogawski - "Analysis of Implementation of HIEROCRYPT–3 algorithm (and its comparison to CAMELLIA algorithm) using ALTERA devices" - 7th Polish National Conference on Applications of Cryptography, ENIGMA 2003, Warsaw, Poland, May 2003

CERTIFICATES AND CLEARENCES

- Certificate issued by Polish Internal Security Agency in "Information Security"
- Certificate issued by Polish Internal Security Agency in "Servicing TEMPEST Devices"
- Polish Secret Clearance – confidential level (valid until 2012)
- NATO Secret Clearance – confidential level (valid until 2012)

LANGUAGES

- English – fluent
- German – basic conversation
- Russian – basic conversation

OTHER INTERESTS

music, soccer, film, history of cryptography, history of 20th century, astronomy, astrophysics, traveling, languages, geography

REFERENCES

Available upon request