EKAWAT (ICE) HOMSIRIKAMOL

571-339-9827 • ekawat@gmail.com

EDUCATION

PhD Computer Engineering, GPA: 3.83 Graduation: Fall 2014
M.S. Computer Engineering, GPA: 3.81 Graduated: Spring 2010
B.S. Electrical Engineering, Magna Cum Laude Graduated: May 2008
George Mason University, Fairfax, VA

WORK EXPERIENCE:,

George Mason University, *Research Assistant* Fairfax, VA
Cryptographic Engineering Group (CERG) Jan 2010 – Present

- Hardware Evaluation of 14 SHA-3 candidates with over 50 hardware designs of 256 and 512-bit variants targeting different speed and area trade-offs, including:
  - Datapath unrolling implementations
  - Datapath folding implementations
  - Low-area implementations
  - Piped implementations
- Hardware bechmarking of the evaluated designs using Xilinx and Altera FPGAs
- PCI Express implementations of selected hardware designs using PLDA IP cores
- Developed generic testbench and padding script for design verification of SHA-3 hardware implementations
- Developed an Automated Tool for Hardware Evaluation (ATHENa) used for simplifying the process of FPGA optimization, data gathering, and verification

George Mason University, *Teaching Assistant* Fairfax, VA
Electrical and Computer Engineering Department Jan 2009 – Dec 2009

- Lab instructor for FPGA and ASIC Design with VHDL (ECE 448) class
- Grader and class project developer for two sessions of Computer Organization (ECE 445) class
- Assisted students in class project for Digital System Design with VHDL (ECE 545)

George Mason University, *Research Assistant* Fairfax, VA
Polar Satellite Precipitation Data Center May 2007 – Dec 2007

- Update legacy FORTRAN code that routinely processes satellite data of NASA's monthly oceanic rainfall derived from special sensor microwave/imager (SSM/I) to generate microwave emission brightness temperature histogram (METH)

SKILLS

Programming Languages: C, FORTRAN, Java, MATLAB, Perl, Python, TCL, VHDL
Environments: Linux, Mac OS X, Unix, Windows

ACTIVITIES

- **Member**, Institute of Electrical and Electronics Engineers (IEEE)
- **Treasurer**, Mason United FC, Jan. 2012 - Present
- **Webmaster**, Institute of Electrical and Electronics Engineers (IEEE), Fall 2007 – Spring 2008

AWARDS

- Best student paper award. ISIM 2012.Best paper
- FPL Community award. FPL 2010.
- Excellent graduate research award. Spring 2010.

CONFERENCE PUBLICATIONS

1. B. Brewster, E. Homsirikamol, R. Velegalati, K. Gaj, "Option Space Exploration Using Distributed Computing for Efficient Benchmarking of FPGA Cryptographic Modules," in *2012 International Conference on Field Programmable Technology - FPT 2012*, Seoul, Korea, Dec. 2012
2. S. Paul, E. Homsirikamol, and K. Gaj, "A Novel Permutation-based Hash Mode of Operation FP and The Hash Function SAMOSA," in *13th International Conference on Cryptology in India - Indocrypt 2012*, Chenai, India, Dec. 2012.

3. P. Morawiecki, M. Srebrny, E. Homsirikamol and M. Rogawski, “Security margin evaluation of SHA-3 contest finalists through SAT-based attacks” *11th International Conference on Information Systems and Industrial Management – ISIM 2012*, Venice, Italy, 25-28 September 2012 (**best student paper award**)
4. K. Gaj, E. Homsirikamol, M. Rogawski, R. Shahid, and M.U. Sharif, “Comprehensive Evaluation of High-Speed and Medium-Speed Implementations of Five SHA-3 Finalists Using Xilinx and Altera FPGAs,” *The Third SHA-3 Candidate Conference*, Washington D.C., March 22-23, 2012
5. F.K. Gürkaynak, K. Gaj, B. Muheim, E. Homsirikamol, C. Keller, M. Rogawski, H. Kaeslin, and J.-P. Kaps, “Lessons Learned from Designing a 65nm ASIC for Evaluating Third Round SHA-3 Candidates,” *The Third SHA-3 Candidate Conference*, Washington D.C., March 22-23, 2012
6. E. Homsirikamol, M. Rogawski, and K. Gaj, "Throughput vs. Area Trade-offs in High-Speed Architectures of Five Round 3 SHA-3 Candidates Implemented Using Xilinx and Altera FPGAs," in LNCS 6917, *Cryptographic Hardware and Embedded Systems* - CHES 2011, Nara, Japan, Sep. 28-Oct. 1, pp. 491-506.
7. K. Gaj, J.-P. Kaps, V. Amirineni, M. Rogawski, E. Homsirikamol, B.Y. Brewster, “ATHENa – Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware using FPGAs,” *20th International Conference on Field Programmable Logic and Applications*, Milano, Italy, Aug. 31st - Sep. 2nd, 2010 (**best paper FPL Community award**)
8. K. Gaj, E. Homsirikamol, and M. Rogawski, “Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs,” in LNCS 6225, *Cryptographic Hardware and Embedded Systems - CHES 2010*, Santa Barbara, CA, USA, Aug. 2010, pp. 264-278
9. K. Gaj, E. Homsirikamol, and M. Rogawski, “Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs,” *The Second SHA-3 Candidate Conference*, Santa Barbara, CA, Aug. 23-24, 2010.
10. K. Gaj, J.-P. Kaps, V. Amirineni, M. Rogawski, E. Homsirikamol "ATHENa – Automated Tool for Hardware EvaluatioN – Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs," *The Second SHA-3 Candidate Conference*, Santa Barbara, CA, Aug. 23-24, 2010.

CONFERENCE PRESENTATIONS

1. K. Gaj, E. Homisirikamol and M. Rogawski, “SHA-3 Competition in Hardware”, *CryptArchi 2010*, Paris, France, Jun. 2010
2. K. Gaj, J.-P. Kaps, V. Amirineni, M. Rogawski, E. Homsirikamol, B. Y. Brewster, J. Pham, and M. Varchola, “ATHENa - Automated Tool for Hardware EvaluatioN: Toward Fair and Comprehensive Benchmarking of Cryptographic Hardware using FPGAs”, *CryptArchi 2010*, Paris, France, Jun. 2010

TECHNICAL REPORTS

1. E. Homsirikamol, P. Morawiecki, M. Rogawski, and M. Srebrny, “Security margin evaluation of SHA-3 contest finalists through SAT-based attacks,” *Cryptology ePrint Archive*: Report 2012/421, July 2012
2. K. Gaj, E. Homsirikamol, M. Rogawski, R. Shahid, and M.U. Sharif, "Comprehensive Evaluation of High-Speed and Medium-Speed Implementations of Five SHA-3 Finalists Using Xilinx and Altera FPGAs," *Cryptology ePrint Archive*: Report 2012/368, first version - June 2012
3. E. Homsirikamol, M. Rogawski, and K. Gaj, "Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs," *Cryptology ePrint Archive*: Report 2010/445, first version - Aug. 2010