

XU “ERIC” GUO

302 Whittemore (0111), Virginia Tech
Blacksburg, VA 24061

xuguo@vt.edu

<http://filebox.vt.edu/users/xuguo/homepage/>

EDUCATION

Ph.D. in Computer Engineering, 2012, Virginia Tech, VA

Thesis work focused on ASIC design and FPGA prototyping of Cryptographic Algorithms, SoC Integration of Cryptographic Coprocessors, and Security Evaluation of Cryptographic Systems.

M.E. in Electrical Engineering, 2007, Huazhong Univ. of Sci. & Tech., China

Thesis work focused on Low Power Digital IC Design for LCD Display System.

B.E. in Electrical Engineering, 2004, Huazhong Univ. of Sci. & Tech., China

RESEARCH

Dr. Xu Guo has been working in the areas of *Embedded Security*, *Secure Hardware/Software Codesign*, *Digital VLSI Design*, and *System-on-Chip Integration* since 2004. His work has included research, development, teaching and industrial work at a variety of levels including algorithms, architectures, circuits and methodologies. Dr. Guo's research has been sponsored by NSF, NIST, and Pratt funds. His current research interests include:

- HW/SW Co-design for Secure Embedded Systems
- Secure Hardware Design for FPGAs and ASICs
- System-on-Chip Integration of Cryptographic Coprocessors
- Side-Channel Attacks and Fault Attacks on Cryptographic Hardware
- Performance Evaluation of Cryptographic Hardware and Software
- Trusted Computing

Graduate Research Assistant

Secure Embedded Systems Lab, CESCA, ECE, Virginia Tech

08/2007 – 05/2012

Project: Environment for Fair and Comprehensive Performance Evaluation of Cryptographic Hardware and Software (NIST Measurement Science and Engineering Research Grants)

- Built the SHA-3 ASIC SW-to-HW testing and FPGA prototyping environments based on SASEBO-R and SASEBO-GII boards.
- Led a team to tape-out the first SHA-3 ASIC (die size of 5 mm², including all the five NIST SHA-3 Finalists) using MOSIS 0.13 μ m CMOS technology.
- Developed a methodology and hardware cost model for ultra-lightweight hash design.
- Evaluated the SHA-3 candidates for high performance cryptographic computing based on system-level design and analysis of Nallatech Intel Xeon FSB FPGA Socket Fillers.
- Opensourced HDL designs and scripted flows to compare the FPGA and ASIC evaluation results for 14 SHA-3 2nd round candidates.
- Prototyped 14 SHA-3 2nd round candidates on an FPGA board and conducted real measurements.
- Proposed a methodology for hardware benchmarking of NIST SHA-3 Competition Candidates.
- Performed preliminary side-channel attack analysis of 2nd round SHA-3 candidates.
- Explored the feasibility of using High Level Synthesis (HLS) for SHA-3 hardware prototyping (C-to-HDL flow: Impulse C & CoDeveloper).

Project: Hardware/Software Codesign for Secure Embedded Systems (NSF and Pratt Funds)

- Proposed a Side-Channel Attack Resistant and Fault Tolerant (SCAR/FT) ECC Crypto-system design based on a novel FPGA heterogeneous multicore architecture.
- Developed a tutorial for physical attack resistant ECC design flow based on a comprehensive study of the state-of-the-art side-channel attacks and fault attacks.
- Proposed a novel HW/SW Codesign of Elliptic Curve Cryptography on FPGA-based SoC architecture using hierarchical controls and distributed storages.
- Evaluated the impact of System-on-Chip integration on the hardware profile of cryptographic coprocessors.

Visiting Research Assistant

Information Science Institute, University of Southern California 05/2009 - 08/2009

- Developed a tutorial for fast System-on-Chip integration of coprocessors with stream interface based on High Level Synthesis (HLS).
- Implemented, verified, and evaluated hardware kernels (e.g. various filters and cryptographic coprocessors) to run as part of the run-time application based on different FPGA platforms and design flows.
- Implemented and tested the high speed IO-SerDes modules for off-chip communications on both Altera and Xilinx FPGA development boards.

Graduate Research Assistant

Electronics Science & Technology Department, HUST 08/2004 - 02/2007

- Conducted a comprehensive evaluation of the power analysis attack resistant properties of AES S-Boxes.
- Optimized low power AES S-Boxes hardware implementations for optimal power-area tradeoffs.
- Optimized the hardware implementations of digital image processing algorithms applied to LCD display systems.

Digital IC Design Intern

Wuhan Asian Microelectronics CO., LTD., China 08/2004 - 02/2007

- Led a commercial Middle-to-small size LCD Timing Controller (TCON) ASIC project and took in charge of making design specification, logic design, FPGA prototyping, and final chip testing.
- Designed image color enhancement modules (e.g. contrast adjustment, Gamma correction, sharpness, and dithering) for an LCD Scalar ASIC project and participated in the FPGA prototyping of the image scaling engine for middle- to-large LCD display system.

WORKING DEMOS/PROTOTYPES

ASICs

- 08/2011: NIST SHA-3 5 Finalists 0.13 μ m ASIC Prototype on SASEBO-R Platform
- 03/2007: Middle-to-Small Size TFT-LCD Timing Controller 0.5 μ m Commercial ASIC

FPGAs

- 05/2010: NIST SHA-3 14 Second Round Candidates FPGA Prototype on SASEBO-GII Platform
- 09/2010: NIST SHA-3 Round 2 Candidates Prototype on Intel Xeon FSB FPGA Accelerated Server
- 08/2009: High Speed IO-SerDes FPGA Prototype on Xilinx ML410 and Altera Stratix-III Platforms
- 05/2009: SoC Integration of Programmable and Parallel ECC Coprocessor on Xilinx ML501 Board
- 12/2008: Instruction Set Extension of PowerPC440 for ECC on AVNET Virtex-5 FXT Board
- 11/2008: Hardware Trojan Designs on BASYS FPGA Board
- 08/2008: SoC Integration of Encryption Coprocessors on Xilinx Spartan-3E Kit
- 03/2007: Middle-to-Small Size TFT-LCD Timing Controller FPGA Prototype in an LCD display
- 06/2005: LCD Scalar FPGA prototype in a customized LCD display

PUBLICATIONS

JOURNALS:

- [J4] Meeta Srivistav, X. Guo, S. Huang, Dinesh Ganta, Michael B. Henry, L. Nazhandali, and P. Schaumont, "**Design and Benchmarking of an ASIC with Five SHA-3 Finalist Candidates**," *Microprocessors and Microsystems: Embedded Hardware Design (MICPRO)*. (Invited Paper in a Special Issue on "Digital System Security and Safety") (to appear)
- [J3] X. Guo and P. Schaumont, "**Optimized System-on-Chip Integration of a Programmable ECC Coprocessor**," *ACM Transactions on Reconfigurable Technology and Systems (TRETs)*, vol.4, no.1, pp.6:1-6:21, Dec. 2010. (Invited Paper in a Special Issue of ARC'09)
- [J2] J. Xing, X. Zou, and X. Guo, "**Ultra-Low Power S-Boxes Architecture for AES**," *The Journal of China University of Posts and Telecommunications*, Vol.15, no.1, Mar. 2008.
- [J1] J. Xiao, X. Zou, Z. Liu, and X. Guo, "**A Novel Adaptive Interpolation Algorithm for Image Resizing**," *International Journal of Innovative Computing, Information and Control*, vol.3, no.6(A), pp. 1335-1345, 2007.
- [J6C] Z. Liu, J. Xiao, X. Zou, and X. Guo, "**Edge-based Algorithm of Real-time Image Resizing**," *Journal of Image and Graphics*, vol.13, no.2, 2008. (in Chinese)
- [J5C] Z. Liu, W. Fan, and X. Guo, "**HVS-based Halftoning Schemes for LCD**," *Journal of Huazhong University of Science & Technology (Nature Science)*, vol.35, no.4, 2007. (in Chinese)
- [J4C] J. Zhang, Z. Liu, X. Zou, and X. Guo, "**Design of Timing Controller for LCD System**," *Computer and Digital Engineering*, vol.35, no.3, 2007. (in Chinese)
- [J3C] J. Xiao, X. Zou, Z. Liu and X. Guo, "**The Research of an Adaptive Algorithm for Real-time Image Enhancement**," *Microelectronics & Computer*, vol.23, no.5, 2006. (in Chinese)
- [J2C] Z. Liu, X. Guo, X. Zou, and J. Xiao, "**Image Color Enhancement Technique based on Improved Bayer Dithering Algorithm**," *Journal of Huazhong Univ. of Science & Technology (Nature Science)*, vol.34, no.5, 2006. (in Chinese)
- [J1C] X. Guo, Z. Liu, X. Zou, J. Xiao and H. Zhao, "**Picture Sharpness Module Design for Scalar**," *Computer and Digital Engineering*, vol.33, no.5, 2005. (in Chinese)

REFEREED CONFERENCES:

- [C17] X. Guo, Meeta Srivistav, S. Huang, Dinesh Ganta, Michael B. Henry, L. Nazhandali, and P. Schaumont, "**ASIC Implementations of Five SHA-3 Finalists**," *Design, Automation and Test in Europe (DATE2012)*, March 2012.
- [C16] X. Guo and P. Schaumont, "**The Technology Dependence of Lightweight Hash Implementation Cost**," *ECRYPT Workshop on Lightweight Cryptography (LC2011)*, November 2011.
- [C15] X. Guo, Meeta Srivistav, S. Huang, Dinesh Ganta, Michael B. Henry, L. Nazhandali, and P. Schaumont, "**Pre-silicon Characterization of NIST SHA-3 Final Round Candidates**," *14th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD2011)*, August 2011.

- [C14] X. Guo, Meeta Srivistav, S. Huang, Dinesh Ganta, Michael Henry, L. Nazhandali, and P. Schaumont, "**Silicon Implementation of SHA-3 Finalists: BLAKE, Grostl, JH, Keccak and Skein**," *ECRYPT II Hash Workshop 2011*, May 2011.
- [C13] Z. Chen, X. Guo, A. Sinha, and P. Schaumont, "**Data-Oriented Performance Analysis of SHA-3 Candidates on FPGA Accelerated Computers**," *Design, Automation and Test in Europe (DATE2011)*, March 2011.
- [C12] X. Guo, S. Huang, L. Nazhandali, and P. Schaumont, "**On the Impact of Target Technology in SHA-3 Hardware Benchmark Rankings**," *Cryptology ePrint Archive*, Report 2010/536, 2010.
- [C11] X. Guo, S. Huang, L. Nazhandali, and P. Schaumont, "**Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations**," NIST 2nd SHA-3 Candidate Conference, August 2010.
- [C10] J. Fan, X. Guo, E. DeMulder, P. Schaumont, Bart Preneel and I. Verbauwhede, "**State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures**," *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST2010) (Embedded Tutorial)*, June 2010.
- [C9] K. Kobayashi, J. Ikegami, M. Knezevid, X. Guo, S. Matsuo, S. Huang, L. Nazhandali, U. Kocabas, J. Fan, A. Satoh, I. Verbauwhede, K. Sakiyama, and K. Ota, "**Prototyping Platform for Performance Evaluation of SHA-3 Candidates**," *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST2010)*, June 2010.
- [C8] X. Guo, J. Fan, P. Schaumont, and I. Verbauwhede, "**Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security**," *Workshop on Cryptographic Hardware and Embedded Systems (CHES2009)*, LNCS5747, pp. 289-303, September 2009.
- [C7] X. Guo and P. Schaumont, "**Optimizing the Control Hierarchy of an ECC Coprocessor Design on an FPGA based SoC Platform**," *5th International Workshop on Applied Reconfigurable Computing (ARC2009)*, LNCS5453, pp. 169-180, Springer Verlag, February 2009.
- [C6] X. Guo and P. Schaumont, "**Optimizing the HW/SW Boundary of an ECC SoC Design Using Control Hierarchy and Distributed Storage**," *Design, Automation and Test in Europe (DATE2009)*, April 2009.
- [C5] Z. Chen, X. Guo, R. Nagesh, A. Reddy, M. Gora, and A. Maiti, "**Hardware Trojan Designs on BASYS FPGA Board**," *Embedded System Challenge Contest in Cyber Security Awareness Week (CSAW08)*, 2008.
- [C4] X. Guo, Z. Chen, and P. Schaumont, "**Energy and Performance Evaluation of an FPGA-based SoC Platform with AES and PRESENT Coprocessors**," *International Workshop on Systems, Architectures, Modeling, and Simulation (SAMOS2008)*, LNCS5114, pp. 16-115, Springer Verlag, July 2008.
- [C3] X. Guo, Z. Liu, J. Xing, W. Fan and X. Zou, "**Optimized AES Crypto Design for Wireless Sensor Networks with a Balanced S-box Architecture**," *International Conference on Informatics and Control Technologies (ICT2006)*, pp. 203-208, IET, December 2006.
- [C2] Z. Liu, X. Guo, Y. Chen, Y. Han and X. Zou, "**On the Ability of AES SBoxes to Secure Against Correlation Power Analysis**," *3rd Information Security Practice and Experience Conference (ISPEC2007)*, LNCS 4464, pp. 43-50, Springer Verlag, May 2007.

[C1] J. Xiao, X. Zou, Z. Liu, and X. Guo, "**Adaptive Interpolation Algorithm for Real-time Image Resizing**," *International Conference on Innovative Computing, Information and Control (ICICIC'06)*, vol. 2, pp. 221-224, IEEE, August 2006.

POSTERS:

[P7] X. Guo, Meeta Srivistav, S. Huang, Dinesh Ganta, Michael Henry, L. Nazhandali, and P. Schaumont, "**Benchmarking ASIC with Five NIST SHA-3 Finalists**," *Workshop on Cryptographic Hardware and Embedded Systems (CHES2011) Exhibition Poster*, September 2011.

[P6] X. Guo, Meeta Srivistav, S. Huang, L. Nazhandali, and P. Schaumont, "**VLSI Characterization of NIST SHA-3 Finalists**," *48th Design Automation Conference (DAC2011) Work-In-Progress (WIP)*, June 2011.

[P5] S. Huang, X. Guo, Meeta Srivistav, Dinesh Ganta, L. Nazhandali, and P. Schaumont, "**Hardware Evaluation of SHA-3 Candidates**," *Annual Workshop of Virginia Tech's Center for Embedded Systems for Critical Applications (CESCA)*, May 2011.

[P4] X. Guo, S. Huang, Meeta Srivistav, L. Nazhandali, and P. Schaumont, "**The Role of Storage Structures in Lightweight Cryptography**," *Annual Workshop of Virginia Tech's Center for Embedded Systems for Critical Applications (CESCA)*, May 2011.

[P3] K. Kobayashi, J. Ikegami, M. Knezevid, X. Guo, S. Matsuo, S. Huang, L. Nazhandali, U. Kocabas, J. Fan, A. Satoh, I. Verbauwhede, K. Sakiyama, and K. Ota, "**A Prototyping Platform for Performance Evaluation of SHA-3 Candidates**," *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST2010)*, Jun. 2010.

[P2] X. Guo, S. Huang, L. Nazhandali, and P. Schaumont, "**Crypto Hardware Benchmark: from SHA-FPGA to SHA-ASIC**," *Annual Workshop of Virginia Tech's Center for Embedded Systems for Critical Applications (CESCA)* May 2010.

[P1] Z. Chen, X. Guo, R. Nagesh, A. Reddy, M. Gora, and A. Maiti, "**Hardware Trojan Designs on BASYS FPGA Board**," *Embedded System Challenge Contest in Cyber Security Awareness Week (CSAW08)*, 2008.

TECHNICAL REPORTS & TUTORIALS:

[T10] X. Guo, "**NIST SHA-3 ASIC User Guide**," VT CESCA Technical Report, August 2011.

[T9] X. Guo, "**NIST SHA-3 ASIC Datasheet**," VT CESCA Technical Report, August 2011.

[T8] X. Guo, "**Virginia Tech SHA-3 ASIC Testing Report**," VT Secure Embedded Systems Lab Technical Report, June. 2011.

[T7] X. Guo, "**Preliminary Side-Channel Attack Analysis of 14 2nd round SHA-3 Candidates**," VT Secure Embedded Systems Lab Technical Report, Jul. 2010.

[T6] X. Guo, "**Tutorial of SHA-3 on SASEBO-GII**," ECE 5520 Secure Hardware Design Class Tutorial for Student Final Projects, Mar. 2010.

[T5] X. Guo, "**Benchmarking of Hardware Implementations of SHA-3 Candidates Using High Level Synthesis**," VT Secure Embedded Systems Lab Technical Report, Mar. 2010.

[T4] X. Guo, "**Tutorial of IO-SerDes Implementations on Xilinx ML410 & Altera Stratix-III Development Boards**," University of Southern California - Information Sciences Institute Technical Report, Jul. 2009.

[T3] X. Guo, "**Filter Kernel and Data Generator with IO-SerDes**," University of Southern California - Information Sciences Institute Technical Report, Jul. 2009.

[T2] X. Guo, "**Redsharc Hardware Kernel Generation Using Impulse C**," University of Southern California - Information Sciences Institute Technical Report, Aug. 2009.

[T1] X. Guo, M. Gora, "**An Instruction Set Extension of the Virtex-5 PowerPC 440 for Elliptic Curve Cryptography**," EE5530 Configuration Computing Class Final Project Report, Dec. 2008.

INVITED TALKS:

[P3] X. Guo, "**Fair and Comprehensive Performance Evaluation of SHA-3 Hardware Implementations**," CESCA Seminar, ECE Department, Virginia Tech, September 2010.

[P2] X. Guo, "**Optimizing the HW/SW Boundary of a Runtime Programmable and Parallel ECC Coprocessor Design Using Control Hierarchy and Distributed Storage**," ESAT-COSIC, K.U. Leuven, Belgium, April 2009.

[P1] X. Guo, "**Area, Delay, and Power Characteristics of Hardware Implementations of the AES S-Box**," Research Center for Integrated Circuit Design, Wuhan, China, September 2006.

AWARDS

- 2012 awarded by the Travel Fund Program of GSA, Virginia Tech.
- 2010 Awarded a stipend funded under NSF grant CCF-1057551 to attend ECC2010 workshop at Redmond, WA.
- 2009 funded by the Pratt funds to visit ESAT/COSIC, K.U. Leuven, Belgium.
- 2008 awarded by the Travel Fund Program of GSA, Virginia Tech.
- 2008 4th Place with Honorable Mention, Embedded System Challenge in Cyber Security Awareness Week (CSAW08) - National Hardware Trojan Design Contest, USA.
- 2006 Outstanding Graduate Pace-setter, awarded by Graduate School, HUST. (10/19,000)
- 2006 Merit Paper Award, Int. Conf. on Informatics & Control Technologies (ICT06).
- 2006 Full Fellowship, Graduate School, HUST.
- 2006 Excellent Research Paper scholarship, Graduate School, HUST. (2/137)
- 2005 Outstanding Teamwork Award, 'Altera Cup' China 5th Graduate EDA Contest.
- 2005 Excellent Student Leader Scholarship, Graduate School, HUST. (6/137)
- 2004 Excellent Researcher Scholarship, Graduate School, HUST. (6/137)
- 2004 Best Presentation Award, Annual Academic Conference of EST Department, HUST.

MEMBERSHIP

IEEE Student Member since 2007

ACM Student Member since 2010

ACADEMIC SERVICE

REVIEWER FOR JOURNALS:

IEEE Transactions on Computers (IEEE-TC)
IEEE Transactions on VLSI (IEEE-TVLSI)
IEEE Embedded Systems Letters (IEEE-ESL)
IEEE Transactions on Circuits and Systems I (IEEE-TCAS-I)
ACM Transactions on Embedded Computing Systems (ACM-TECS)
ACM Transactions on Reconfigurable Technology and Systems (ACM-TRETS)
Elsevier Integration the VLSI Journal
Springer Transactions on Computational Science (Springer-TCS)
ACTA International Journal of Computers and Applications
Springer Journal of Cryptographic Engineering

REVIEWER FOR CONFERENCES:

APACE'12;
CAMAM'13;
CHES'08,'09,'10,'11;
CT-RSA'12;
DAC'09,'10,'11;
DATE'09,'10,'11;
FPT'11;
HOST'09;
ICCAIE'11;
ICIMTR'12;
ICEDSA'12;
ISIEA'12;
ISCI'12;
ISWTA'12;
ReConfig'09,'10,'11;
SHUSER'12;
WESS'10;

□