Christopher A. Wood

1114 Corella
Newport Beach, CA 92660

www.christopher-wood.com
woodc1@uci.edu
315-806-5939

Academic Information

- **University of California Irvine** Irvine, CA
  Ph.D. Computer Science *2013 – 2018 (expected)*
  - Advisors: Dr. Gene Tsudik and Dr. Stanisław Jarecki
  - Research Areas: applied cryptography, security, and privacy
  - GPA: 4.0/4.0

  Rochester Institute of Technology Rochester, NY
  M.S. Computer Science *2012 – 2013*
  - Advisor: Dr. Stanisław Radziszowski
  - Thesis: Large Substitution Boxes with Efficient Combinational Implementations
  - GPA: 4.0/4.0

- **Rochester Institute of Technology** Rochester, NY
  B.S. Computer Science and Software Engineering *2008 – 2012*
  - Concentrations: Computational Mathematics and Computer Engineering
  - Minor: Mathematics
  - GPA: 3.98/4.0 (Primary Field of Study GPA: 4.0/4.0)

Publications

Forthcoming

[F-1.]P. Bajorski, A. Kaminsky, M. Kurdziel, M. Lukowiak, S. Radziszowski, and C. A. Wood, “Modeling Multi-Epoch Message Distribution Times in Unbounded Spanning Trees,” *in preparation.*

Journal Articles

[J-1.]C. A. Wood and J. Jacob, “Characterization of Small Trees Based on their L(2,1)-Span,” *submitted.* C. A. Wood and J. Jacob, “Forbidden Subtree Construction Techniques for Trees Under the L(2,1)-Labeling Problem,” *submitted.* P. Bajorski, A. Kaminsky, M. Kurdziel, M. Lukowiak, S. Radziszowski, and C. Wood, “Statistical Analysis and Modeling of a Tree-Based Group Key Distribution Method in Tactical Wireless Networks,” *submitted.* M. Lukowiak, S. Radziszowski, J. Vallino, C. Wood, “Cybersecurity Education: Bridging the Gap between Hardware and Software Domains,” to appear in *ACM Transactions on Computing Education.*

Conference Proceedings

[C-1.]C. A. Wood, S. P. Radziszowski, and M. Lukowiak, “Affine-Power S-Boxes over Galois Fields with Area-Optimized Logic Implementations,” *submitted.* C. A. Wood and E. Uzun, “Flexible End-to-End Content Security in CCN,” in *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC 2014) Special Seesion: Information Centric Networking*, Las Vegas, Nevada. January 2014. S. Skalicky, C. A. Wood, M. Lukowiak, and M. Ryan, “High Level Synthesis: Where Are We? A Case Study on Matrix Multiplication,” to appear in *Proceedings of the 2013 International Conference on Reconfigurable Computing and FPGAs - ReConFig 2013*, Cancun, Mexico. December 2013. M. Lukowiak, A. Meneely, S. Radziszowski, J. Vallino, and C. Wood, “Developing an Applied, Security-Oriented Computing Curriculum,” in *Proceedings of the ASEE 2012*, San Antonio, Texas. June 2012. C. A. Wood, “Chaos-Based Symmetric Key Cryptosystems,” in *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada. July 2011. C. A. Wood and R. K. Raj, “Keyloggers in Cybersecurity Education,” in *Proceedings of the 2010 International Conference on Security & Management*, Las Vegas, Nevada. July 2010.

Theses

[T-1.]C. A. Wood, “Large Substitution Boxes with Efficient Combinational Implementations,” M.S. Thesis, Computer Science, Rochester Institute of Technology, Rochester, NY. August 2013.

Surveys

[S-1.]C. A. Wood, “Small Folkman Numbers.” *Draft available online:* `http://christopher-wood.com/papers/FolkmanSurvey.pdf`.

Presentations and Posters

[P-1.]“On the $L(2,1)$ Labeling of Trees,” with Dr. Jobby Jacob (presenter), *Joint Mathematics Meetings*, Baltimore, MD. January 15-18, 2014. “Secure Content Dissemination in Content Centric Networking,” with Dr. Ersin Uzun, *CCNxCon 2013, Palo Alto Research Center, Palo Alto, CA*. September 5, 2013. “Characterization Results for the L(2,1)-Labeling Problem on Trees,” *AMS Sectional Meeting, RIT, Rochester, NY*. September 22, 2012. “Chaos-Based Symmetric Key Cryptosystems,” *RIT Graduate Research Symposium, RIT, Rochester, NY*. July 22, 2011. “Keyloggers in Cybersecurity Education,” *2010 International Conference on Security & Management*, Las Vegas, Nevada. July 2010. “Layered Driver Rootkit Detection on Microsoft Windows PCs,” Poster Presentation, *RIT Undergraduate Research Symposium, RIT, Rochester, NY*. August 24, 2009.

Active Research Projects

- **3-Party Oblivious RAM with SSE Applications** UC Irvine
  Applied Cryptography *October 2013 - present*
  - *Advisor:* Dr. Stanisław Jarecki
  - *Colleagues:* Dr. Sotirios Kentros (University of Connecticut) and Sky Faber (UC Irvine)
  - I am investigating various ways to improve the performance of Oblivious RAM constructions in a three-party setting using secure multiparty computation. We are beginning the design and development of a software system using our protocol to gather preliminary performance metrics and experiment with support for searchable symmetric encryption (SSE).
- **Privacy and Anonymity in Named Data Networking** UC Irvine and PARC
  Security, Privacy, Content-Centric Networking *September 2013 - present*
  - *Advisors:* Dr. Gene Tsudik and Dr. Ersin Uzun (PARC)
  - I am investigating and implementing software for establishing session-based onion routing circuits, analogous to TOR, that enable consumer and producer anonymity in content-centric networks (e.g., CCN and NDN).
- **Circuit Minimization and Cryptographic Applications** NIST
  Boolean Functions, Algorithms, Complexity Theory *May 2013 - present*
  - *Advisor:* Dr. René Peralta
  - *Colleagues:* Cagdas Calik and Meltem Turan
  - I am designing and implementing algorithms and heuristic techniques for minimizing the combinational logic required to implement small linear and nonlinear circuits of cryptographic interest, such as the AES S-box and binary $GF(2)$ polynomial multiplication circuits. My primary focus is on improving the efficiency of known solutions through algorithmic changes and implementation improvements, such as through the application of multi-core parallel and grid computing.
- **Narrowing Edge Folkman Number Bounds** RIT
  Combinatorics, Computational Graph Theory *January 2013 - present*
  - *Advisor:* Dr. Stanisław Radziszowski
  - I am investigating various computational techniques to attempt to prove the conjecture that the edge Folkman number $F_e(3,3;4) \leq 127$, including a reduction of $G \to (3,3;4)^e$ to an equivalent $3-\mathsf{SAT}$ formula to be solved using modified (guided) SAT solvers.

- **$L(2,1)$-Labeling Problem** RIT
  Computational Graph Theory *September 2011 - present*
  - *Advisor:* Dr. Jobby Jacob (Mathematics)
  - We are studying the $L(2,1)$-span of bicubic graphs, which are 3-regular bipartite graphs, and generalizing these results to larger k-regular and t-partite graphs.
  - Past results include the development of graph construction algorithms that can produce infinitely many trees with a $L(2,1)$-span of $(\Delta(T)+2)$, as well as a complete $L(2,1)$-span characterization of all trees with up to twenty vertices.

Professional Experience

- **Palo Alto Research Center, Computer Science Laboratory** Palo Alto, CA
  Security and Privacy Research Intern *July 2013 - September 2013*
  - Researched security and privacy aspects related to content-centric network (CCN).
  - Implemented the Green-Ateniese (pairing-based) and Chow-Weng-Yang-Deng (Schnorr-ElGamal-based) Proxy Re-Encryption schemes in Java for use in a CCNx application.
  - Studied and tested various techniques for securing content that is distributed throughout a CCN mesh for confidentiality purposes.
  - Experimented with techniques for improving name privacy in CCN.
- **Intel Corporation, Virtual & Parallel Computing Group** Folsom, CA
  Graphics Software Engineer Intern *June 2012 - August 2012*
  - Developed production features for tool that processes hardware specifications to generate web content and source code for VHDL and C/C++ testbeds.
  - Interacted with internal customers within the VPG to utilize debug tools and environments for architecture specification and post-silicon testing.
- **L-3 Communications** Victor, NY
  Software Engineer Intern *March 2011 - August 2011*
  - Designed and implemented a library and supporting drivers for the u-blox NEO5/6 GPS receiver driven by an Analog Devices Blackfin processor.
  - Extended an existing FAT file system driver to add support for SD devices.
  - Improved functionality of a CPLD controller for an embedded power supply.
- **Rochester Software Associates** Rochester, NY
  Software Engineer Intern *November 2010 - March 2011*
  - Led the design, development, and documentation efforts for a new printer job management application that would service any number of jobs from clients across the network.
  - Tested and debugged an existing .NET implementation of an LPD client.
- **C Speed, LLC** Liverpool, NY
  Software Engineer Intern *May 2010 - August 2010*
  - Designed and implemented an internal manufacturing part supply management system.
  - Implemented embedded firmware features and test routines in C, C++, and assembly for Coldfire V2 processors.

Teaching & Other Academic Experience

- **Cryptography II** RIT
  Guest Lecturer for Dr. Stanisław Radziszowski (CS) *April 8, 2013*
  - Lectured about recent research on the security and (hardware) implementation efficiency of cryptographic S-boxes.
- **Hardware and Software Design with Cryptographic Applications** RIT
  Teaching Assistant and Lecturer for Dr. Marcin Lukowiak (CE) *February 2011 - May 2013*
  - Developed and delivered lecture material on cryptography, embedded software optimization techniques, the Impulse C high-level synthesis tool, and AES cache timing attacks.
  - Assisted students with weekly assignments and graded lab and project deliverables.

- **Computer Science I, II, and IV** RIT
  Student Lab Assistant and Grader *January 2009 - present*
  - Proctor problem solving sessions and run lab meetings with lectures of weekly material.
  - Grade weekly lab assignments and midterm examinations.
- **Personal Software Engineering** RIT
  Teaching Assistant for Professor Tom Reichlmayr (SE) *December 2011 - March 2012*
  - Assisted students with in-class programming assignments and course projects.
  - Graded projects written in C/C++ and Ruby (with Ruby on Rails).
- **Engineering of Software Subsystems** RIT
  Teaching Assistant for Dr. James Vallino (SE) *September 2011 - December 2011*
  - Assisted students with in-class exercises and unit questions based on a subset of the design patterns taught during the course.
  - Spent time with each student team to discuss course projects, including design decisions, application of design patterns, and alternatives considered.

Honors, Awards, & Activities

l@r

Academic and Personal Projects

- Replicating the published cache timing attack on LUT-based implementations of the Advanced Encryption Standard on an FPGA-based embedded system.
- Implemented a fully-compliant FTP client with a text-based interface in Java (approximately 2,000 lines of code).
- Led the development effort for a four-person team that worked on a Kanban taskboard web application using Adobe Flex, Flash, BlazeDS, Hibernate, Jasper Reports, and Java (approximately 10,000 lines of code).
- Led team to develop a Java-based medical image viewing and reconstruction system featuring image scrolling and multi-axis reconstructions of X-ray, CT scan, and MRI images in various file formats (approximately 6,500 lines of code).

Technical Skills

Programming Languages: C/C++, C#, Java, Python, Scala, Ruby, Assembly (MIPS), JavaScript, Objective-C, Standard ML, Scheme

Modeling Languages and Tools: VHDL, Verilog, UML, SPIN (with PROMELA), Alloy

Specialized Software: MATLAB, Mathematica, WEKA, Magma, Sage, LLVM

Markup Languages: LaTeX, HTML(5), CSS3

Web Frameworks: Play (Java and Scala), Spring MVC, Ruby on Rails

Personal Information

Lake Placid Marathon finisher, June 12, 2011. Time of 4:28:08.

My Erdős number is 3 (Me → Stanisław Radziszowski → Brendan McKay → Paul Erdős)

Capable of reading and writing introductory Spanish. Learning elementary French and Polish.