Christopher A. Wood

Permanent Address
Department of Computer Science
University of California, Irvine
Irvine, CA 92617

Contact Information
Voice: (315) 806-5939
Email: woodc1@uci.edu
www.christopher-wood.com

RESEARCH INTERESTS

Secure multiparty computation, privacy and anonymity intersections with cryptography, symmetric-key cryptographic algorithms, applications, and implementations, information-centric networking security and applications, computational and extremal graph theory

EDUCATION

Doctor of Philosophy, Computer Science
University of California Irvine, Irvine, CA 2013 - 2018 (expected)
Advisors: Dr. Gene Tsudik and Dr. Stanisław Jarecki
GPA: 4.0/4.0

Master of Science, Computer Science
Rochester Institute of Technology, Rochester, NY 2012 - 2013
Thesis: Large Substitution Boxes with Efficient Combinational Implementations
Advisor: Dr. Stanisław Radziszowski

Bachelor of Science, Computer Science and Software Engineering
Rochester Institute of Technology, Rochester, NY 2008 - 2012
Concentrations: Computational Mathematics and Computer Engineering
Minor: Mathematics
GPA: 3.98/4.0 (Professional Field of Study GPA: 4.0/4.0)

ACTIVE RESEARCH PROJECTS

3-Party Oblivious RAM with SSE Applications October 2013 - present
Applied Cryptography (UC Irvine)

- *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 September 2013 - present
Security, Privacy, Content-Centric Networking (UC Irvine and PARC)

- *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 May 2013 - present
Boolean Functions, Algorithms, Complexity Theory (NIST)

- *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 January 2013 - present
Combinatorics, Computational Graph Theory (RIT)

- *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 $G \rightarrow (3,3;4)^e$ to an equivalent $3-\mathsf{SAT}$ formula to be solved using modified (guided) SAT solvers.

$L(2,1)$-Labeling Problem September 2011 - present
Computational Graph Theory (RIT)

- *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 July 2013 - September 2013
Computer Science Laboratory, Palo Alto, CA (Security and Privacy Research Intern)

- 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 June 2012 - August 2012
Virtual & Parallel Computing Group, Folsom, CA (Graphics Software Engineer Intern)

- 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 March 2011 - August 2011
Victor, NY (Software Engineer Intern)

- 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 November 2010 - March 2011
Rochester, NY (Software Engineer Intern)

- 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 May 2010 - August 2010
Liverpool, NY (Software Engineer Intern)

- 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.

ACADEMIC EXPERIENCE

Cryptography II April 8, 2013
Guest Lecturer for Dr. Stanisław Radziszowski (CS) (RIT)

- Lectured about recent research on the security and (hardware) implementation efficiency of cryptographic S-boxes.

Hardware and Software Design with Cryptographic Applications February 2011 - May 2013
Teaching Assistant and Lecturer for Dr. Marcin Lukowiak (CE) (RIT)

- 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 January 2009 - May 2013
Student Lab Assistant and Grader (RIT)

- Proctored problem solving sessions and ran lab meetings with lectures of weekly material.
- Graded weekly lab assignments and midterm examinations.

Personal Software Engineering December 2011 - March 2012
Teaching Assistant for Professor Tom Reichlmayr (SE) (RIT)

- 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 September 2011 - December 2011
Teaching Assistant for Dr. James Vallino (SE) (RIT)

- 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.

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

PUBLICATIONS

- "Job Analysis - A True Picture," Journal of Headhunters, Vol. 5, Number 3. Fall 1990
- "The Fine Tuning of Interpersonal Skills," Journal of Recruiting/Hiring, Vol. 16, Number 7, August 1990

MEMBERSHIPS

IEEE, Student Affiliate
ACM, RPI Weight-training Club
SIAM, Utica College

HONORS AND ACTIVITIES

- RIT Honors Program, 2009 – 2013
- RIT Tau Beta Pi Engineering Honors Society, 2011 – 2013
- RIT Outstanding Undergraduate Student award, selected, Winter 2012
- RIT Computer Science MS Student Delegate, selected, Winter 2012
- Recipient of Golisano College Honors research assistantship stipend, Winter 2009/2010
- Recipient of Golisano College Honors research assistantship stipend, Spring 2011
- Recipient of RIT undergraduate research award stipend, Summer 2009
- RIT Golisano College Dean's List, 2008 – 2013
- Student mentor for the FIRST LEGO League team hosted by RIT, Fall 2009 – Winter 2010
- Rochester Foodlink volunteer, Winter 2012/2013 – March 2013
- Society of Software Engineers, member, Fall 2008 – Winter 2009/2010
- RIT Electronic Gaming Society, member, Fall 2008 – Spring 2010
- RIT Intramural Flag Football Team, member, Fall 2010

INTERESTS

Guitar, hard rock and heavy metal, marathon running and cycling, weightlifting, cooking