

## SCOTT W. RUSSELL

12 West St., Apt. 2

Waterville, ME 04901

Phone: (207) 872-6968

E-mail: [srussell@colby.edu](mailto:srussell@colby.edu)

Web: <http://cs-people.bu.edu/srussell>

### Objective

I am seeking a tenure-track computer science faculty position in an intimate liberal arts setting where the emphasis is on undergraduate teaching and continued scholarship. I am interested in teaching cryptography, algorithms, and other theory courses, as well as applied topics such as information security, database systems, and networking. I am also interested in teaching courses for non-majors, discrete math, linear algebra, and probability.

### Education

Ph.D. Computer Science, Boston University	expected January 2008
M.A. Computer Science, Boston University	2004
M.S. Applied Mathematics and Engineering Science, Northwestern University	1993
B.A. Mathematics, Asian Studies minor, Hamilton College	1992
Semester abroad in Japan, School for International Training	Fall 1990
Clarkson School Bridging Year Program, Clarkson University (Students complete high school by taking college courses while living at Clarkson)	1988

### Teaching Experience

Visiting Instructor, Dept. of Computer Science, Colby College Fall 2007 - present  
Taught introductory programming and problem solving in Java to majors, minors, and non-majors.  
Responsible for both lecture and small, hands on laboratory sections.

Teaching Fellow, Dept. of Computer Science, Boston University Spring 2004 - Fall 2006  
Planned and taught weekly recitation sections, substitute taught lectures, graded homework, assisted with examination grading, and coordinated external graders. Courses: CS330 - Introduction to Analysis of Algorithms, CS232 - Geometric Algorithms, and CS113 - Combinatoric Structures.

English Conversation Instructor, NOVA Intercultural Institute, Mishima, JAPAN 7/2001-6/2000  
Taught students ages 15 to 70 ranging in ability from beginner to near native fluency. Just-in-time lesson planning for eight daily four-student classes. Majority of lessons based on Nova textbooks. Also conducted new student placement interviews and moderated free conversation room.

Software Trainer, contract through Answerthink, Inc. 2/1999-6/1999  
Customized training for a multi-dimensional modeling and analysis tool for a division of GE Capital. Attained vendor instructor certification, adapted vendor written materials and training database to GE Capital specifications. Coordinated training of approximately 500 people by myself and two other trainers across multiple sites.

**Research Publications**

“Oblivious Binary Search and Private Range Queries” (with N. Dedić and L. Reyzin).

- In preparation

“Intrusion-Resilient Secure Channels” (with G. Itkis and R. McNeerney, Jr.).

- In *Proceedings of Third International Conference, Applied Cryptography and Network Security, ACNS 2005, Lecture Notes in Computer Science*, v. 3531, pg. 238-253, 2005.
- Preparing for submission to *Journal of Cryptology*

“Upper and Lower Bounds on Black-Box Steganography” (with N. Dedić, G. Itkis, and L. Reyzin).

- Submitted to *Journal of Cryptology*, Jul., 2006.
- In *Proceedings of Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Computer Science*, v. 3378 pg. 227-244, 2005.
- M.A. thesis titled “Simple, Stateless Steganography for Memoryless Channels” (advised by Prof. L. Reyzin), 2004.
- Preliminary version titled “Simple Stateless Steganography” (with L. Reyzin), appears in *Cryptology ePrint Archive, Report 2003/093*, 2003.

**Conference Presentations**

“Intrusion-Resilient Secure Channels,” *Applied Cryptography and Network Security, Third International Conference, ACNS 2005*, New York, NY, Jun 7-10, 2005.

“Upper and Lower Bounds on Black-Box Steganography,” *Second Theory of Cryptography Conference, TCC 2005*, Cambridge, MA, Feb. 10-12, 2005.

**Boston University Presentations**

“Private Range Queries” (poster with N. Dedić)

- Presented talk at *Second BU Student Conference on Information Assurance and Cyber Security*, Dec. 15, 2006
- *Center for Reliable Information Systems and Cyber Security (RISCS) Inaugural Symposium on Information Security and Privacy*, Apr. 10, 2006
- *CS Dept. IAP Research Day*, Mar. 17, 2006
- *CS Dept. IAP Research Day*, Mar. 22, 2005

“Intrusion-Resilient Secure Channels” (poster with R. McNeerney, Jr.)

- Presented talk at *Second BU Student Conference on Information Assurance and Cyber Security*, Dec. 15, 2006
- Presented talk at *CS Dept. Theory Seminar*, Oct. 7, 2005
- *CS Dept. IAP Research Day*, Mar. 22, 2005
- *Boston University Science and Technology Day*, Mar. 23, 2004
- *CS Dept. IAP Research Day*, Mar. 17, 2004

“Simple, Stateless Steganography,” (poster)

- *Boston University Science and Technology Day*, Mar. 23, 2004
- *CS Dept. IAP Research Day*, Mar. 17, 2004
- *CS Dept. IAP Research Day*, Mar. 6, 2003

*Applied Cryptography and e-Security (ACeS) Reading Group* talks

- “Privacy Preserving Data Mining” by Y. Lindell and B. Pinkas, Fall 2004
- “Zero Knowledge Proof Systems, Arguments, and Arthur-Merlin Games”, Fall 2003
- “Universally Composable Two-Party and Multi-Party Secure Computation”, by R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai, Summer 2003
- “A Forward-Secure Public-Key Encryption Scheme” by J. Katz, Fall 2002
- “Secure Human Identification Protocols”, by N. Hopper and M. Blum, Spring 2002

### **Professional Experience**

*Senior Consultant, Legacy Technology (now a division of Answerthink, Inc.)* 11/1993-10/1998  
 Developed and supported On-Line Analytical Processing (OLAP) and Decision Support System(DSS) solutions for finance and marketing groups in Fortune-1000-sized companies. Built solutions based on a variety of analysis and reporting tools for multi-dimensional and relational databases.

*Express Center of Excellence Co-head* 6/1997-10/1998  
 An internal, part time position responsible for consultant training, cross project technical support, coordinating communication between Oracle and Legacy for product release and support issues, and maintenance of internal software, documentation, and knowledge repository.

### **Select client engagements**

*Great Brands of Europe (a Danone Group company)* 3/1998-10/1998  
 Developed a sales and marketing budgeting and analysis system. System combined field sales force data and estimates with those of headquarters financial planning group to facilitate product and customer level profit and loss planning and reporting capabilities. Implementation included data source identification, data extraction from general ledger and sales systems, and multi-dimensional database modeling and development. Also served as project leader managing development work of two other consultants and day-to-day client interaction.

*The Kellogg Company* 8/1996-2/1998  
 Assisted in the validation and refinement of proposed next-generation analysis and reporting architecture. Evaluated suitability of alpha version of Oracle relational-database-based decision support package to replace existing custom multi-dimensional database applications. Also provided personnel and account oversight for several other on-site project teams.

*The Kellogg Company* 6/1994-9/1995  
 Provided incremental development and round-the-clock support for mission-critical financial budgeting and marketing funds applications. Served as sole programming resource and project manager. Helped pave the way for additional project teams and account growth.

**Awards and Societies**

Outstanding Teaching Fellow Award, College of Arts and Sciences, Boston University	2006
Third Best Poster Award, CS Dept. IAP Research Day, Boston University	2006
Second Best Poster Award, CS Dept. IAP Research Day, Boston University	2003
National Physical Science Consortium Fellowship with National Security Agency	2002-2003
Presidents University Graduate Fellowship, Boston University	2001-2002
Royal Cabell Fellowship, Northwestern University	1992-1993
Phi Beta Kappa and Sigma Xi member	1992-present
<i>Summa Cum Laude</i> , class rank 7 of 462, mathematics department honors, Hamilton College	1992
Kirkland, Huntington Memorial, and Tompkins mathematics prizes, Hamilton College	1990-1992
Oren Root Prize Scholarship, Hamilton College	1990
Phallanx Award, Clarkson University	1988

**Other Skills**

Intermediate spoken and written Japanese.

**References**

Prof. Gene Itkis (Research Advisor)  
 Department of Computer Science  
 Boston University  
 111 Cummington St.  
 Boston, MA 02215  
 (617) 353-5285  
 itkis@cs.bu.edu

Prof. Leonid Rezyin (Research Advisor)  
 Department of Computer Science  
 Boston University  
 111 Cummington St.  
 Boston, MA 02215  
 (617) 353-3283  
 rezyin@cs.bu.edu

Dr. Dale J. Skrien  
 Department of Computer Science  
 Colby Collge  
 5850 Mayflower Hill  
 Waterville, ME 04901  
 (207) 859-5851  
 djskrien@colby.edu