

Nenad Dedić

Computer Science, Boston University Office: 617-358-1121 nenad@bu.edu
111 Cummington Street Home: 617-776-0987 <http://cs-people.bu.edu/nenad>
Boston, MA 02215 Cell: 617-230-2844

Research Interests

Cryptography; computer security; computer theory. Particular areas of interest:

- secure computation on encrypted data; secure computation with encrypted programs
- efficient two-party secure computation
- software protection
- efficient pseudorandom generators
- relations among cryptographic primitives
- provably undetectable steganography

Education

PhD candidate. Expected graduation in Summer 2007. Focusing in cryptography at the [Department of Computer Science](#), Boston University. Advised by [Professor Leonid Reyzin](#).

B.S. (Sep 1995 - Jun 2000). [Department of Mathematics](#), School of Informatics and Computer Science, Belgrade University, Serbia.

High School (Sep 1991 - Jun 1995). [Mathematical High School](#), Belgrade, Serbia.

Employment History and Experience

Visiting Research Fellow. [Securing Cyberspace](#) research program,

Institute for Pure and Applied Mathematics, University of California, Los Angeles, Fall 2006.

Designed efficient protocols for secure database queries. Investigated properties of one-way functions.

Research Intern. Microsoft Research, Redmond, Summer 2006, Summer 2005.

Worked on theoretical models for software tamper-proofing.

Research Fellow. Boston University, Spring 2007, Spring 2004, Fall 2003, Spring 2003.

Worked on secure database queries, steganography, pseudorandom generators.

Teaching Fellow. Boston University, Spring 2006, Fall 2005, Fall 2002, Spring 2002, Fall 2001.

Taught: Theory of Computation, Programming Languages, Discrete Mathematics, and some basic computer literacy courses.

Teaching Assistant. State University of New York, Stony Brook, Spring 2001, Fall 2000.

Taught: Discrete Mathematics, Basic JAVA.

Instructor. [Braća Karić University](#), Belgrade, Serbia, part-time 1997-2000.

Taught various basic computer and office courses.

Publications

Constant-Round Private Database Queries

with Payman Mohassell. In submission.

Oblivious Binary Search Tree Traversal and Private Range Queries

with Leonid Reyzin and Scott Russell. In submission.

Upper and Lower Bounds on Black-Box Steganography

with G. Itkis, L. Reyzin and S. Russell. Submitted to Journal of Cryptology. Extended abstract in Theory of Cryptography (TCC) 2005, J. Kilian, editor, LNCS 3378, pp 227-244, Springer-Verlag, 2005.

An Improved Pseudorandom Generator Based on Hardness of Factoring

with Leonid Reyzin and Salil Vadhan. Security in Communication Networks (SCN) 2002, Cimato, Galdi, Persiano, eds. LNCS 2576, pp 88-101, Springer-Verlag, 2004.

On Different Models for Generating SAT Problems

with P. Janičić and G. Terzić. In Computing and Informatics, Vol. 20, Number 5, pp 451-469, 2001.

Talks and Presentations

Oblivious Binary Search Tree Traversal and Private Range Queries:

December 13, 2006, Institute for Pure and Applied Mathematics at University of California, Los Angeles

Upper and Lower Bounds on Black-Box Steganography:

January 28, 2005, New York University Cryptography Reading Group

February 18, 2005, Boston University Complexity Theory Seminar

March 4, 2005, MIT Cryptography and Information Security Group Seminar

An Improved Pseudorandom Generator Based on Hardness of Factoring:

December 5, 2002, Boston University Complexity Theory Seminar

October 11, 2002, MIT Cryptography and Information Security Group Seminar

September 12, 2002, Third Conference on Security in Communication Networks, Amalfi, Italy

Awards and Honours

Fellowship of Institute for Pure and Applied Mathematics. University of California at Los Angeles, 2006. Awarded for Fall 2006 “Securing Cyberspace” research program.

Best Teaching Fellow Prize. Department of Computer Science, Boston University, 2006.

Annual Student Accomplishment Award. Department of Mathematics, University of Belgrade, 2000.

Best Student Paper Award. Republic of Serbia Department of Education, 1999.

Fellowship for Exceptionally Talented Students. Republic of Serbia Dept. of Education, 1997 - 2000.

Service

Journal Reviewer. IEEE Transactions on Computers.

External reviewer for conferences. Public Key Cryptography (PKC 2006), Crypto 2005, Theory of Cryptography (TCC 2005), Information Security (ISC 2005), Principles of Distributed Computing (PODC 2003).

Software and Other Projects

2002 – Data presentation tool for Centre for Free Election and Democracy: Implemented a tool for reviewing results of all elections during 1992-2002 in Serbia. Worked in a two-man team. The final product was a stand-alone CD for convenient review of a large volume of data on a low-end Windows PC. I implemented a small and fast engine for querying data. Using a database was unacceptable because of the low minimum system specifications. <http://www.cesid.org/cd2/c3.cgi?tip=ser&lang=en>.

1998-2000 – Geometry Construction Language: Developed a specialized language, GCL, for describing geometric constructions at University of Belgrade, under supervision of Predrag Janičić. I designed the language itself (semantics, syntax), and developed the compiler / interpreter for it. The project was terminated abruptly because of sudden deterioration of the state in the country. Recently, it has been revived again: <http://www.matf.bg.ac.yu/~janicic/gclc>.

2001 – NFS range mapping: Extended functionality of NFS (both Linux kernel and user-space) to allow cross-administrative domain access. The work was eventually incorporated into publication: <http://homepages.inf.ed.ac.uk/s0239160/papers/rmap/rmap.pdf>.

2001 – Image inpainting: Implemented an algorithm for image inpainting (based on Bertalamio and Sapiro’s paper), a method for restoration of damaged images.

1998-2000 – Linux system administrator: Volunteered as a system administrator at the University Braća Karić in Belgrade.