

VISHAL SARASWAT

Intelligent Storage Consortium, Digital Technology Center
University of Minnesota, Twin Cities, MN - 55455, USA

Phone: (001) 763-370-3041
Email: vishal@cs.umn.edu

RESEARCH INTERESTS

Cryptography and Data Security, Algorithm Design and Analysis, Computational Complexity

EDUCATION

Ph.D. - Mathematics, GPA: 3.88/4.00, University of Minnesota (UMN), Twin Cities, MN, USA

Advisor: Prof. Andrew Odlyzko

Minor: Computer Science

M.S. - Computer Science, GPA: 3.84/4.00, UMN, Aug 2007

M.S. - Mathematics, GPA: 3.91/4.00, UMN, Aug 2007

PUBLICATION

Anonymous Signatures Revisited

with Dr. Aaram Yun, ProvSec 2009, LNCS vol. 5848, pp. 140-153, Springer-Verlag, 2009

Public-Key Encryption with Searchable Keywords based on Jacobi Symbols

with Dr. Giovanni Di Crescenzo, IndoCrypt 2007, LNCS vol. 4859, pp. 282-296, Springer-Verlag, 2007

PROJECTS

Secure and Efficient Long Term Data Management, Intelligent Storage Consortium, Digital Technology Center (DTC), UMN, May 2007 - Present

Long Term Key Management, Intelligent Storage Consortium, DTC, UMN, May 2007 - Present

Applied Remote Cache-timing Attacks against AES, Institute of Technology, UMN, Sept 2006 - Apr 2007

Cryptographic Multilinear Maps, Institute of Technology, UMN, May 2005

EXPERIENCE

Teaching Assistant, Institute of Technology, UMN, Aug 2003 - Present

Lectured, held recitations, and graded various advanced graduate and undergraduate courses including *Modern Cryptography*, *Cryptology and Number Theory*, *Coding Theory*, *Mathematical Logic*, *Preparation for Financial Mathematics*, and, *Mathematical Background for Finance*

Research Assistant, Intelligent Storage Consortium, DTC, UMN, May 2007 - Aug 2007

Research Visitor, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Rutgers University, Piscataway, NJ, Jul 2006 - Aug 2006

Research Fellow, Minnesota Center for Industrial Mathematics, UMN, June 2006 - Aug 2006

Research Scholar, Tata Institute of Fundamental Research (TIFR), Bombay, India, Aug 2000 - July 2003

AWARDS

Full-tuition Scholarship and Assistantship, Graduate School, UMN, 2003 - Present

TIFR Alumni Association Scholarship for Career Development, TIFR, Bombay, India, 2002 - 2003

Special Grant for Graduate Studies in USA, B. D. Bangur Endowment, Calcutta, India, 2003

Scholarship for Graduate Studies in USA, Manoj Mody Foundation, Calcutta, India, 2003

COMPUTER SKILLS

Languages: C++, Fortran, Lisp

Applications/Packages: MATLAB, Mathematica, MS Office Suite, LaTeX

Operating Systems: UNIX, Linux, Solaris, Windows

MEMBERSHIP

Nominee Member, American Mathematical Society (AMS)

Member, Society for Industrial and Applied Mathematics (SIAM)