

VISHAL SARASWAT

School of Mathematics, University of Minnesota
206 Church St SE, 127 Vincent Hall
Minneapolis, MN - 55455, USA

Phone: (001) 407-584-7425
Email: vishal@math.umn.edu

RESEARCH INTERESTS

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

EDUCATION

Ph.D. - Mathematics, GPA: 3.88/4.00, University of Minnesota (UMN), Minneapolis, 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

B.Sc. - Mathematics, Honors, St. Xavier's College, University of Calcutta, Calcutta, July 2000

Certificate in Statistical Methods and Applications, First Class, Indian Statistical Institute, Calcutta, July 2000

PUBLICATIONS

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

Counterparty Credit Risk in Over-The-Counter Derivatives, Minnesota Center for Financial and Actuarial Mathematics (MCFAM), UMN, Jan 2012 - Jan 2012

Pursuit Evasion Games with Multiple Pursuers, Institute of Mathematics and its Applications (IMA), UMN, June 2010 - Aug 2010

Secure and Efficient Long Term Data Management, Intelligent Storage Consortium, Digital Technology Center (DTC), UMN, May 2007 - May 2008

Long Term Key Management, Intelligent Storage Consortium, DTC, UMN, May 2007 - May 2008

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

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

Basic Lie Theory, School of Mathematics, Tata Institute of Fundamental Research (TIFR), Bombay, July 2003

VISHAL SARASWAT

School of Mathematics, University of Minnesota
206 Church St SE, 127 Vincent Hall
Minneapolis, MN - 55455, USA

Phone: (001) 407-584-7425
Email: vishal@math.umn.edu

EXPERIENCE

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

Lectured, held recitations, and/or graded various advanced graduate and undergraduate courses including *Modern Cryptography*, *Cryptology and Number Theory*, *Coding Theory*, *Mathematical Logic*, *Preparation for Financial Mathematics*, *Mathematical Background for Finance*, *Mathematical Theory Applied to Finance*, and, *Computation, Algorithms, and Coding in Finance*

Please visit <http://www.math.umn.edu/~vishal/teaching/> for details.

Mentor, Interdisciplinary Research Experience for Undergraduates, IMA, UMN, June 2010 - Aug 2010

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, Aug 2000 - July 2003

AWARDS

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

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

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

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

COMPUTER SKILLS

Languages : C/C++, Fortran, Lisp

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

Operating Systems : Linux, Mac, Windows

REFEREES

Professor Andrew Odlyzko <odlyzko@math.umn.edu>, School of Mathematics, UMN

Professor Scott Adams <adams@math.umn.edu>, School of Mathematics, UMN

Professor David Frank <frank@math.umn.edu>, School of Mathematics, UMN