DR. VISHAL SARASWAT, Visiting Scientist
Department of Computer Science and Engineering
Indian Institute of Technology (IIT)
Paloura, Jammu - 181121, J&K, India.

(091) 970-357-2379
(001) 407-584-7425
vishal.saraswat@gmail.com
http://www.math.umn.edu/~vishal/

RESEARCH INTERESTS

Number Theory and Cryptography, Algorithm Design and Analysis, Computational Complexity, Quantum Computation

EDUCATION

Ph.D. - Cryptography, GPA: 3.86/4.00, May 2012
University of Minnesota (UMN), Minneapolis, MN, USA
Advisor : Prof. Andrew Odlyzko

M.S. - Computer Science, GPA: 3.84/4.00, Aug 2007
Department of Computer Science and Engineering, UMN

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

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

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

EXPERIENCE

Visiting Faculty, February 2018 - *Present*
Indian Institute of Technology, Jammu, India

Adjunct Faculty, March 2017 - *Present*
S P Jain School of Global Management, Mumbai, India

Visiting Scientist, April 2017 - January 2018
R.C.Bose Centre of Cryptology & Security, Indian Statistical Institute, Kolkata,India

Assistant Professor, May 2012 - April 2017
C.R.Rao Advanced Institute of Mathematics Statistics and Computer Science (AIMSCS), Hyderabad, India

Honorary Lecturer, January 2013 - May 2015
University of Hyderabad, Hyderabad, India

Visiting Faculty, August 2013 - May 2015
Indian Institute of Technology, Hyderabad, India

Lecturer / Teaching Assistant, Aug 2003 - May 2012
University of Minnesota (UMN), Minneapolis, MN, USA
Lectured, held recitations and labs, and graded various advanced graduate and undergraduate courses including *Probability*, *Calculus*, *Analysis* (*real & complex*), *Differential Equations*, *Algebra*, *Linear Algebra*, *Finite Fields*, *Mathematical Logic*, *Cryptography* (*classical & quantum*), *Error correcting codes*, *Mathematical Theory Applied to Finance*, and *Computation, Algorithms, & Coding in Finance*
Please visit http://www.math.umn.edu/~math-sa-sara0050/teaching/ for details.

Mentor, June 2011 - Aug 2011
Interdisciplinary Research Experience for Undergraduates, Institute of Mathematics and its Applications (IMA), UMN

Research Assistant, May 2007 - Aug 2007
Intelligent Storage Consortium, Digital Technology Center (DTC), UMN

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

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

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

BOOKS / EDITED VOLUMES

Introduction to Cryptography (ISBN: 1138071536)
with Sahadeo Padhye and Rajeev Anand Sahu, CRC Press, 2017.

Proceedings of SPACE 2016
with Claude Carlet and Anwar Hasan, LNCS, Springer, 2016.

Journal of Hardware and Systems Security
Guest Editor for special issue on SPACE 2016, Springer, 2017.

Journal of Cyber Security and Mobility
Guest Editor for special issue on SPACE 2016, River Publishers, 2017.

PUBLICATIONS (INTERNATIONAL JOURNALS / BOOK CHAPTERS)

Public-key Encryption with Integrated Keyword Search
with R.A.Sahu, Journal of Hardware and Systems Security, Springer, 2018.

An Evaluation of Lightweight Block Ciphers for Resource-Constrained Applications: Area, Performance, and Security
with R.Sadhukhan, S.Patranabis, A.Ghoshal, D.Mukhopadhyay and S.Ghosh, Journal of Hardware and Systems Security 1 (3), pp.203-218, Springer, 2017.

A Secure Anonymous Proxy Signcryption Scheme
with R.A.Sahu and A.K.Awasthi, Journal of Mathematical Cryptology 11 (2), pp.63-84, DeGruyter, 2017.

Analysis-Preserving Protection of User Privacy against Information Leakage of Social-Network Likes
with F.Buccafurri, L.Fotia, and G.Lax. Information Sciences 328, pp.340-358, Elsevier, 2016.

An Anonymous Proxy Multi-signature with Accountability
with R.A.Sahu, E-Business and Telecommunications, CCIS 554, pp.234-254, Springer, 2014.

An Efficient Integrated PKE+PEKS Scheme with Joint CCA Security in the Standard Model
with F.Buccafurri, G.Lax and R.A.Sahu, *In Submission*.

A Lightweight and Secure PRNG for Low-Cost Devices
with F.Buccafurri, D.Gulati and G.Lax, *In Submission*.

PUBLICATIONS (INTERNATIONAL CONFERENCES)

Anonymous yet Traceable Strong Designated Verifier Signature
with V.Kuchta, R.A.Sahu, G.Sharma, N.Sharma and O.Markowitch. ISC 2018, LNCS, Springer, 2018

A Novel Lattice Reduction Algorithm
with D.Das. Secrypt 2018, SciTePress, 2018

Compact Lattice Signatures
with D.Das. Secrypt 2018, SciTePress, 2018

Short Integrated PKE+PEKS in Standard Model
with R.A.Sahu. SPACE 2017, LNCS 10662, Springer, 2017

Offline Outdoor Navigation System with Full Privacy
with P.Kaushik and F.Buccafurri. WINSYS 2017, SciTePress, 2017

Adaptively Secure Strong Designated Signature
with N.Sharma, R.A.Sahu and B.K.Sharma. IndoCrypt 2016, LNCS 10095, Springer, 2016

Efficient Proxy Signature Scheme from Pairings
with F.Buccafurri and R.A.Sahu. Secrypt 2016, SciTePress, 2016

Differential Fault Attack on SIMECK
with V.Nalla and R.A.Sahu. CS2, HiPEAC 2016, ACM, 2016

Efficient and Secure Many-to-One Signature Delegation
with R.A.Sahu. ICICS 2015, LNCS 9543, Springer, 2015

Strengthening NTRU Against Message Recovery Attacks
Arithmetic 2015: Elliptic curves, diophantine geometry, and arithmetic dynamics, Brown University, Providence, RI, USA, 2015

Practical and Secure Integrated PKE+PEKS with Keyword Privacy
with F.Buccafurri, G.Lax and R.A.Sahu. Secrypt 2015, SciTePress, 2015

Secure and Efficient Scheme for Delegation of Signing Rights
with R.A.Sahu. ICICS 2014, LNCS 8958, Springer, 2014

How to Leak a Secret and Reap the Rewards too
with S.K.Pandey. LatinCrypt 2014, LNCS 8895, Springer, 2014

A Secure Anonymous Proxy Multi-Signature Scheme
with R.A.Sahu. Secrypt 2014, SciTePress, 2014

Remote Cache-timing Attacks on AES
with D.Feldman, D.F.Kune, and S.Das. CS2, HiPEAC 2014, ACM, 2014

Anonymous Signatures Revisited
with A.Yun. ProvSec 2009, LNCS 5848, Springer, 2009

Public-Key Encryption with Searchable Keywords based on Jacobi Symbols
with G.D.Crescenzo. IndoCrypt 2007, LNCS 4859, Springer, 2007

FUNDED PROJECTS

Attacks on Elliptic Curve Discrete Log Problem Oct 2015 - March 2018
Co-principal Investigator. *Grant Amount:* INR 24,65,500*. Funded by:* Govt. of India

Post Quantum Cryptology Oct 2014 - March 2017
Principal Investigator. *Grant Amount:* INR 1,01,78,200*. Funded by:* Govt. of India

FUNDED PROJECTS (UNDER CONSIDERATION)

Remote Cache Timing Attacks on AES

Implementation of Attacks on Discrete Log Problem using Function Field Sieve

Post-Quantum Cryptosystems based on Isogenies

OTHER RECENT PROJECTS

Side Channel Cryptanalysis (of block/stream ciphers) May 2012 - April 2017
Lead Researcher, Funded by: Govt. of India, AIMSCS, Hyderabad

Development of an Indigenous 128-bit Block Cipher Feb 2014 - April 2017
Lead Researcher, Funded by: Govt. of India, AIMSCS, Hyderabad

Development of an Indigenous Lightweight Block Cipher May 2012 - Oct 2015
Lead Researcher, Funded by: Govt. of India, AIMSCS, Hyderabad

Design of a Lattice Based Cryptosystem May 2012 - Sep 2013
Lead Researcher, Funded by: Govt. of India, AIMSCS, Hyderabad

Software Methodologies for Lattice Based Cryptanalysis May 2012 - Sep 2013
Lead Researcher, Funded by: Govt. of India, AIMSCS, Hyderabad

PAST PROJECTS

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

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

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

Long Term Key Management May 2007 - May 2008
Intelligent Storage Consortium, Digital Technology Center, UMN

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

Cryptographic Multi-linear Maps Jan 2005 - May 2005
Institute of Technology, UMN

Basic Lie Theory Aug 2000 - July 2003
School of Mathematics, Tata Institute of Fundamental Research, Bombay

Engel Curve Analysis of Expenditure of Employees of ISI, Calcutta,
Indian Statistical Institute, Kolkata Jan 2000 - June 2000

WORKSHOPS AND SEMINARS ORGANIZED/CONDUCTED

SPACE 2018 (Ph.D. Forum Chair) 12-16 December 2018

The Eighth International Conference on Security, Privacy and Applied Cryptographic Engineering. https://space2018.cse.iitk.ac.in/

FARES 2018 (PC Member) 27-30 August 2018

The 13th International Workshop on Frontiers in Availability, Reliability and Security. https://www.ares-conference.eu/

SPACE 2017 (Tutorial Chair) 13-17 December 2017

The Seventh International Conference on Security, Privacy and Applied Cryptographic Engineering. http://www.space.dbcegoa.ac.in/

SPACE 2016 (Program Chair) 14-18 December 2016

The Sixth International Conference on Security, Privacy and Applied Cryptographic Engineering. http://www.math.umn.edu/~math-sa-sara0050/space16/

Workshop on Side Channel Cryptanalysis 19-21 December 2016

International workshop jointly organized with IIT Kharagpur

Short course on Elliptic Curve Cryptography July 2016

for post-graduate research scholars at AIMSCS

Training on Block Cipher Cryptanalysis June 2016

for scientists of the Signal Intelligence, New Delhi

Training on Code Based Cryptology May 2016

for scientists of Scientific Analysis Group (SAG, DRDO), New Delhi

Code Based Crypto Workshop 2015 September 2015

International workshop jointly organized with SAG, DRDO

Training on Elliptic Curves March 2015

for scientists of the SAG, DRDO

Training on Block Cipher Design July 2014

for scientists of the Cabinet Secretariat, New Delhi

Training on Lattice-based Cryptosystems and Cryptanalysis March 2013

for scientists of SAG, DRDO

Training on Lattice-based Cryptosystems and Cryptanalysis January 2013

for scientists of SAG, DRDO

Training on Block Ciphers November 2012

for scientists of National Technical & Research Organization (NTRO), New Delhi

Short course on Anonymous Identity-based Cryptosystem July-September 2012

for post-graduate research scholars at AIMSCS

Student Number Theory Seminar 2004-2006

School of Mathematics, University of Minnesota, USA

STUDENTS (CO)MENTORED

Number of Ph.D. Students: 1

Dipayan Das Ph.D. Thesis, 2015 - *present*
National Institute of Technology, Durgapur, West Bengal

Number of Postgraduate (M.Tech. & M.S.) Students: 12

Number of Undergraduate (B.Tech. & B.S.) Students: 4

PROFESSIONAL MEMBERSHIPS

Cryptology Research Society of India
Executive Committee Member

Indian Science Congress Association
Life Member

American Mathematical Society
Nominee Member

Society for Industrial and Applied Mathematics (SIAM)
Member

AWARDS

Full-tuition Scholarship and Assistantship 2003 - 2012
Graduate School, University of Minnesota, USA

TIFR Alumni Association Scholarship for Career Development 2002 - 2003
School of Mathematics, Tata Institute of Fundamental Research, Bombay

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

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

REFEREES

Andrew Odlyzko <odlyzko@umn.edu>, Professor, School of Mathematics, University of Minnesota (UMN), Minneapolis, MN, USA.

Bimal Roy <bimal@isical.ac.in>, Director, R.C.Bose Centre for Cryptology and Security, Indian Statistical Institute, India.

Subhamoy Maitra <subho@isical.ac.in>, Professor, Applied Statistics Unit, Indian Statistical Institute, India.

Debdeep Mukhopadhyay <debdeep@cse.iitkgp.ernet.in>, Professor, Deptartment of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India.