SNEHAL S. MITRAGOTRI

Department of Mathematics,
Shivaji University,
Kolhapur, MH
INDIA

Phone : (+91)231-2609217-28
Email : ssm_maths@unishivaji.ac.in

CURRENT POSITION : Assistant Professor (tenured), Department of Mathematics, Shivaji University, Kolhapur

EDUCATION :

2009-2007	**INDIAN INSTITUTE OF TECHNOLOGY, ROORKEE** **भारतीय प्रोद्योगिकी संस्थान, रूडकी** Master of Science (M.Sc) in Applied Mathematics, CGPA - 7.93 on 10 Point Scale, First Class with Distinction Percentage Equivalent - 84.30% (as per Conversion Policy of IITR) Rank Holder - Overall 2nd rank
2007-2005	**UNIVERSITY OF PUNE, PUNE** **पुणे विद्यापीठ, पुणे** Master of Science (M.Sc) in Pure Mathematics, CGPA - 6.3 on 10 Point Scale, First Class
2005-2002	**SHIVAJI UNIVERSITY, KOLHAPUR** **शिवाजी विद्यापीठ, कोल्हापूर** Bachelor of Science (B.Sc) in Mathematics**,** Percentage - 81.44%, First Class with Distinction

RESEARCH WORK @ IIT ROORKEE :

- **Project** - Construction of Irreducible Polynomials over Finite Fields and It's Applications
  (The goal of this project was to survey various algorithms to construct irreducible polynomials over finite fields and implementation of one of them)

- **Dissertation** – Construction of Rotational Symmetric Boolean Functions with Cryptographic Significance
  (The goal of this dissertation was to construct rotational symmetric boolean functions on 6 & 8 variables and implement the important data structure, the matrix nA)

  Advisor – Dr Sugata Gangopadhyay

COMPUTER SKILLS :

➢ Computer Languages	- C, C++, Python
➢ Software Packages	- SAGE, GAP, Maxima

RESEARCH INTEREST : Cryptology (Interdisciplinary Research)

COURSES TAUGHT :

- **Undergraduate Courses @** Department of Technology, Shivaji University Kolhapur
  - MA 211 - Applied Mathematics III (B.Tech II Computer Science & Technology)
  - MA 211 - Applied Mathematics III (B.Tech II Electronics & Technology)

- **Postgraduate Courses @** Department of Mathematics, Shivaji University Kolhapur
  - MT 101 - Algebra I (Master of Science - I)
  - MT 201 - Algebra II (Master of Science - I)
  - MT 202 - Linear Algebra (Master of Science - I)
  - MT 204 - Numerical Analysis (Master of Science - I)
  - MT 303 - Number Theory (Master of Science - II)
  - MT 317 - Commutative Algebra I (Master of Science - II)
  - MT 401 - Field Theory (Master of Science - II)
  - MT 403 - Algebraic Number Theory (Master of Science - II)
  - MT 417 - Commutative Algebra II (Master of Science - II)
  - MIM 102 - Algebra I (Master of Science Tech - I)
  - MIM 405 - Design and Analysis of Algorithms (Master of Science Tech - II)

RESEARCH PUBLICATIONS

- **International :**

- *Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri, Mridul Nandi (2020)* From Combined to Hybrid : Making Feedback-based AE even Smaller, **IACR Transactions on Symmetric Cryptology**, 2020 (S1) (Special Issue 1), 417-445. https://doi.org/10.13154/tosc.v2020.iS1.417-445 **Cite Score: 1.3**

  Note - The ordering of the author names, in the publications, follows the Hardy-Littlewood principle i.e. it is determined by the alphabetical ordering of the last names of the respective authors.

RESEARCH PRESENTATIONS

- **International :**

- *Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri, Mridul Nandi* 'From Combined to Hybrid: Making Feedback-based AE even Smaller' in **27th Fast Software Encryption (FSE) 2020 Conference** held virtually online organised by the International Association for Cryptologic Research (IACR), 9-13 November 2020

- *Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri, Mridul Nandi* 'Security Analysis of HyENA Authenticated Encryption Mode' in **NIST Third Lightweight Cryptography Workshop 2019** at NIST* Main Campus Gaithersburg, Maryland (MD), United States of America, 4-6 November 2019
  *NIST - National Institute of Standards & Technology, Department of Commerce, Government of USA

WORKSHOPS/SCHOOLS ATTENDED

- **International :**

- 4th Lightweight Cryptography Workshop 2020 held virtually online organised by NIST (National Institute of Standards & Technology, Department of Commerce, Government of USA) Gaithersburg, Maryland (MD) United States of America (USA), 19-21 October 2020

- International Workshop on ‘Cryptography and It’s Applications' webinar on zoom online platform organised by West Bengal State University, Institute for Advanced Intelligence TCG CREST & Indian Statistical Institute Kolkata WB, 26-30 August 2020

- Indo-Japan Joint Workshop on ‘Quantum Computation & Quantum Information’ sponsored by DST GoI (Department of Science & Technology, Government of India) at Indian Statistical Institute Kolkata WB, 2-8 January 2020

- 8th Asian Workshop on Symmetric Key Cryptography (ASK) 2018 at Indian Statistical Institute Kolkata WB, 13-16 November 2018

- International Workshop on Complex Analysis and Its Applications (CAA 2012) at Walchand College of Engineering (WCE) Sangli MH, 11-15 June 2012

➢ **National :**

- Association for Computing Machinery (ACM-W) Women in Computing India Grad Cohort - a Pan India Workshop for Women in Computing held virtually online by Indian Institute of Technology GandhiNagar GJ, 24-26 July 2020

- Association for Computing Machinery (ACM) India Summer School on ‘Fundamentals for Cryptology Research’ at Indian Statistical Institute Kolkata WB, 4-22 June 2018

- Advanced Training in Mathematics (ATMW) Workshop on Cryptology at Indian Statistical Institute Kolkata WB, 10-14 April 2018

- Advanced Instructional School (AIS) on Cryptography at Society for Electronic Transactions & Security (SETS) Chennai TN, 16 June-5 July 2014

- A Short term Course on Cryptography at Indian Institute of Technology Kharagpur WB, 18-24 May 2014

- Instructional School for Lecturers (ISL) on ‘Real Analysis & Measure Theory’ at University of Delhi, New Delhi 26 March-7 April 2012

- Workshop on ‘Development of Mathematics in India’ at Indian Institute of Technology Bombay MH, February 2012

- Advanced Training in Mathematics for Lecturers (ATML) School on ‘Ordinary Differential Equations’ at The Maharaja Sayajirao (MS) University of Baroda, Vadodara GJ, 2-15 June 2011

- National Workshop on Computer Algebra Systems (CAS) at Bhaskaracharya Pratishthana Pune MH, 27-31 January 2011

- Mathematics Training and Talent Search (MTTS) Program Level-1 at Sir Parshurambhau (SP) College Pune MH, 16 May-11 June 2005

- Mathematics Workshop held at Indian Institute of Technology Bombay MH, November 2004

- Mathematics Training and Talent Search (MTTS) Program Level-0 at Regional Institute of Education (RIE), Mysore KN, 17 May-12 June 2004

- **University Level :**

- Participated in a Workshop on ‘Challenges before Higher Education in 21st Century’ at Shivaji University Kolhapur MH, December 2011

- Participated in an Orientation Program on ‘Innovative Teaching Techniques and Professional Development of University Teachers’ at Department of Education, Shivaji University Kolhapur MH, December 2011

CONFERENCES ATTENDED

- **International :**

- 19th International Conference on Cryptology in India (IndoCrypt) 2018 sponsored by Scientific Analysis Group SAG, DRDO at India Habitat Centre New Delhi, Delhi NCR, 9-12 December 2018

- Participated in an International Conference on Python ‘SciPy India 2012’ at Indian Institute of Technology Bombay MH, 27-29 December 2012

- Participated in an International Conference ‘SAGE Days 25, India’ at Indian Institute of Technology Bombay MH, 9-12 August 2010

- **National :**

- Participated & Presented a research paper entitled ‘Construction of Rotational Symmetric Boolean Functions with Cryptographic Significance’ in a National Conference on Mathematical Sciences (NCMS 2012) at North Maharashtra University Jalgaon MH, March 2012

WORKSHOPS/CONFERENCES ORGANIZED

- **National :**

- **CONVENER**, UGC-NBHM sponsored ‘National Workshop on Algebra 2015’ at Department of Mathematics, Shivaji University Kolhapur MH, 21-26 December 2015

BOOKS CO-AUTHORED :

- **Field Theory** Shivaji University Press, 2017 (with *S.S.Kumbhar, G.D.Shelake*) ISBN : 978-81-8486-570-7

INVITED TALKES :

- A Series of lectures on ‘Applications of Number Theory & Finite Fields in Cryptography’ delivered for M.Tech Computer Science students at Department of Technology, Shivaji University Kolhapur

- A lecture on LaTeX delivered in the Spoken Tutorial Workshop at Department of Technology, Shivaji University Kolhapur

- A Series of lectures on ‘Number Theory’ delivered in NET-SET Workshop at Department of Mathematics, Shivaji University Kolhapur

- A lecture on ‘Career Opportunities in Summer Vacation’ delivered in a Workshop ‘Career Opportunities in Mathematics & Computer Science’ at Department of Mathematics, Shivaji University Kolhapur

PROFESSIONAL MEMBERSHIP :

- Life Member - Cryptology Research Society Of India (CRSI)
- Member - Shivaji University PG Teachers Association, Shivaji University Kolhapur

HONORS & AWARDS :

- Senior Research Fellowship SRF in Computer Science by Indian Statistical Institute Kolkata, 2019
- Qualified Junior Research Fellowship JRF in Computer Science (through a National level Written Examination ISI Admission Test and Interview) by Indian Statistical Institute Kolkata, July 2017
  (All India Rank-6, All India Topper in Female Category)
- Certificate Course in Russian Language
- Qualified Maharashtra State Eligibility Test (SET) in Mathematical Sciences conducted by University of Pune, September 2009
- Qualified National Eligibility Test (NET) for Lectureship in Mathematical Sciences conducted by Council of Scientific and Industrial Research (CSIR), MHRD, Government of India, June 2009
- National Stock Exchange NSE Certification in Financial Markets (NCFM)-Derivatives Market Dealers Module (Percentage-84%)
- Qualified Joint Admission Test (IIT-JAM) Examination, 2007
- Merit Scholarship - Shivaji University Merit Scholarship during Undergraduate Studies
- Rank Holder - 1st Rank in Statistics Quiz conducted by Shivaji University Statistics Teachers Association during Undergraduate Studies
- Rank Holder - 1st Rank in ‘Sanskrit Subject’ on Maharashtra State Board Secondary School Certificate (Xth) Examination, Pune Divisional Board

(updated-December 2020)