Curriculum Vitae

Dr. Amit Kumar Singh

CONTACT INFORMATION (CURRENTLY WORKING)

Assistant Professor,
Department of Science (Mathematics),
IIIT Ranchi
Jharkhand 835217, India

Phone: +91-8945975556
E-mail: amitmintu01991@gmail.com
amit.math@iiitranchi.ac.in

EDUCATION

Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India

Doctor of Philosophy (Ph.D.), Department of Mathematics, 2017-2023.
- Thesis Title: *Construction of Broadcast Encryption and Mutli-signature Scheme*
- Thesis Supervisor: Prof. Sourav Mukhopadhyay

Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India

Master of Technology (M.Tech.), Computer Science and Data Processing, 2015-2017.
- Thesis Title: *Design and Implementation of Public Key Cryptography in Smart Card Operating System*

University of Allahabad, Prayagraj, India

Master of Science (M.Sc.), Mathematics, 2012-2014.

Chhatrapati Shahu Ji Maharaj University (CSJM) University, Kanpur, India

Bachelor of Science (B.Sc.), Information Technology and Mathematics, 2008-2011.

TEACHING EXPERIENCE

- **Assistant Professor at SOA University (July 2022-March 2025)**
  - Programming in Python — Autumn 2022, 2023
  - Introduction to Data Science using Python — Spring 2023
  - Algorithms Design — Autumn 2024
- **Teaching Assistant at IIT Kharagpur during M.Tech. and Ph.D.**
  - Design and Analysis of Algorithm Lab — Autumn 2016
  - Numerical Techniques — Spring 2017
  - Mathematics-I — Autunm 2018, 2019, 2020, 2021
  - Mathematics-II — Spring 2018, 2019, 2020, 2021
- **Teaching Assistant for NPTEL at IIT Kharagpur**
  - Introduction to Abstract and Linear Algebra — Aug-Oct 2018, 2019, 2020, 2021
  - Cryptography and Network Security — January-April 2019, 2020, 2021
- **Assistant Professor at Brahmanand College, Kanpur (Aug 2014-Feb 2015)**
  - Real Analysis and Complex Analysis

RESEARCH INTERESTS

- Cryptography
- Theoretical Computer Science
- Applied Mathematics

ARTICLES (PUBLISHED)

1. Kansal, M., **Singh, A. K.** and Dutta, R. Efficient Multi-Signature Scheme Using Lattice, ***The Computer Journal***, *Oxford university press*, 65 (9), 2421-2429, 2022.

2. Dutta, S. , Pal, T., **Singh, A. K.** and Mukhopadhyay, S.Embedded Identity Traceable Identity-Based IPFE from Pairings and Lattices, ***Cryptology ePrint Archive***, 2022.

3. **Singh, A. K.**, Acharya, K., and Dutta, R. Cloud Assisted Semi-static Secure Accountable Authority Identity-based Broadcast Encryption Featuring Public Traceability without Random Oracles, ***Annals of Telecommunications***, *Springer*, 78 (1-2), 79-90, 2023 (Corresponding author).

4. **Singh, A. K.**, Acharya, K., and Mukhopadhyay, S. Post-quantum Secure Recipient Revocable Broadcast Encryption Supporting Anonymity, ***Multimedia Tools and Applications***, *Springer*, 83 (2), 4519-4531 2023 (Corresponding author).

5. Acharya, K., **Singh, A. K.**, and Mukhopadhyay, S. Constructions of Broadcast Encryption with Personalized Messages from Bilinear Map, ***Computer Communications***, *Elsevier*, 209, 91-101, 2023 (Corresponding author).

6. Dutta, S. , Pal, T., **Singh, A. K.** and Mukhopadhyay, S. Fully Collusion Resistant Traceable Identity-Based Inner Product Functional Encryption, ***IACR Communications in Cryptology***, 2025.

AWARDS & ACHIEVEMENTS

1. Qualified Graduate Aptitude Test in Engineering (**GATE**) in 2015 and **CSIR-UGC NET** examination in December 2018.

2. Institute fellowship during M.Tech. and Ph.D. from IIT Kharagpur.

3. University of Allahabad rank holder in M.Sc.

4. Qualified University of Allahabad, India, Combined Research Entrance Test (CRET) in 2014.

5. Offered Ph.D. student position at the Cyber Security and Network lab, Innopolish University, Respublika Tatarstan, Russia.

TECHNICAL SKILLS

1. Software: Matlab, LaTeX

2. Languages: C, Python, SageMath

3. Operating Systems: Linux, Windows

COURSE WORK INFORMATION

1. Cryptography and Network Security, Data Structure and Algorithm, Introduction to Data Science, Graph Theory, DBMS, Operating System, Object Oriented Programming, Computer Networks, Design and Analysis of Algorithm.

2. Linear algebra, Modern Algebra, Complex Analysis, Real Analysis, Topology, Differential Equations, Operation Research, Numerical Analysis etc.

PROFESSIONAL ACTIVITY

1. I am serving as a reviewer of Journal of Medical Systems.

2. Technical program committee member of international conferences ICSP 2020, 2021, 2024, 2025.

3. Technical program committee member of national level short term training program on "Statistical Machine Learning" organised during August 2-11, 2023 at SOA University, Bhubaneswar, India.

EXTRACURRICULAR ACTIVITY	1. Worked as Assistant Superintendent for a hostel in Siksha 'O' Anusandhan (Deemed to be) University.
	2. Worked as Research Scholar Representative to the Institute Senate at Indian Institute of Technology, Kharagpur for the academic session 2021-2022.
	3. Worked as Vice-Chairperson of Research Scholars Council at Indian Institute of Technology, Kharagpur for the academic session 2021-2022.

CONFERENCES ATTENDED	1. Volunteered for "IMS-2019 Conference" held at IIT Kharagpur during November 22-25, 2019.
	2. International Conference on "Class Groups of Number Fields and Related Topics" held at HRI, Prayagraj on October 16-19, 2019.
	3. INDOCRYPT 2017 held at IMSc Chennai during Dec 10-13, 2017.
	4. ICRTM 2015 International Conference on "Recent Trends in Mathematics" held at Dept. of Mathematics, University of Allahabad during July 10-12, 2015.
	5. DGACON 2014 National Conference on "Differential Geometry and Its Applications" held at Dept. of Mathematics, University of Allahabad during Dec 27-28, 2014.

LECTURE DELIVERED & WORKSHOPS ATTENDED	1. Delivered a lecture on "Advanced Topics in Cryptography" at TEQIP sponsored short-term course (Organized by IIT Kharagpur) during February 10-14, 2020.
	2. "Foundational Aspects of Blockchain Technology Program" held at ICTS-TIFR Bengaluru during January 15-17, 2020.
	3. MPC-TP 2020 Workshop on "Secure Multiparty Computation" held at IISc Bengaluru during January 19-22, 2020.
	4. NCM Workshop on "Cryptology" held at Indian Statistical Institute, Kolkata during April 10-14, 2018.
	5. BLOCKCHAIN 2017, workshop on "Blockchain Technology" held at ISI Kolkata during Nov 29- Dec 1, 2017.
	6. National Seminar on "Recent Advances in Mathematics and its Applications" held at Dept. of Mathematics, B.N.D. College, Kanpur during Feb 12, 2011.
	7. National Level Workshop on "Emerging Trends in Interdisciplinary Mathematical Sciences" held at Dept. of Mathematics D.A.V. College, Kanpur during Oct. 15-16, 2011.

REFERENCES

Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology Kharagpur, India
E-mail: msourav@gmail.com, sourav@maths.iitkgp.ac.in

Dr. Ratna Dutta
Associate Professor
Department of Mathematics
Indian Institute of Technology Kharagpur, India
E-mail: ratna@maths.iitkgp.ac.in

Dr. Mriganka Mandal
Assistant Professor
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute, Kolkata, India
E-mail: mriganka@isical.ac.in