ANINDYA GANGULY

PhD Scholar, IIT Kanpur

✉ Official: anindyag@cse.iitk.ac.in
✉ Personal: anindyagangulymath@gmail.com
🌐 https://www.cse.iitk.ac.in/users/anindyag/
📱 (+91)7872648932 (WA+Telegram)
📍 (E) KD-106, CSE, IIT Kanpur, Kanpur, UP-208016, INDIA

Employment History

Feb-21- July-21

Project Associate, R&D, IIT Bhilai
Project Title *Building Trust on Computing Platform and Training of Secure Coding of Security Chips.*
Principal Investigators Prof. Dhiman Saha.

July 19- Dec-20

Junior Reserach Fellow, SRIC, IIT Kharagpur
Project Title *Cryptanalysis of Cryptographic Ciphers with Emphasis on AES and RSA.*
Principal Investigators Prof. Dipanwita Roy Chowdhury and Prof. Abhijit Das

Oct '16 - Jul '19

Senior Project Officer, SRIC, IIT Kharagpur
Project Title *Design and Efficient Implementation of Advanced Encryption and Decryption Techniques for Use in Space Craft Communication.*
Principal Investigators Prof. Abhijit Das and Prof. Dipanwita Roy Chowdhury

Education

Aug-2021 – present

PhD in Computer Science and Engineering
Broad area: Computational Number Theory and Algebra, Mathematical Cryptography and Computational Complexity.
Supervisor: Prof. Nitin Saxena
Department of Computer Science and Engineering, IIT Kanpur.
CGPA: 8.4/10; Percentage: 84% (till second sem)

Jan-2017 - April-2021)

MS in Computer Science and Engineering, (Cryptography)
Thesis: *"A Study of Hyperelliptic Curve Cryptography"*
Supervisors: Prof. Abhijit Das and Prof. Dipanwita Roy Chowdhury
Department of Computer Science and Engineering, IIT Kharagpur.
CGPA: 9/10; Percentage: 90%.

2014- 2016

M.Sc. in Mathematics
Thesis: *"A Tale on RSA Cryptosystem"*
Supervisor: Prof. Sourav Mukhopadhyay
Department of Mathematics, IIT Kharagpur.
CGPA: 7.93/10; Percentage: 79.3%

2011 - 2014

B.Sc. (Hons) in Mathematics
Minors: Physics and Chemistry
Marks: 69.75%
Bankura Christian College under The University of Burdwan

Education (continued)

2009-2011
- **Higher Secondary (Science)**
  Marks: 68.8%
  School: Manbazar Radha Madhab Institution
  Board: West Bengal Council of Higher Secondary Education

2009
- **Madhyamik**
  Marks: 71.125%
  School: Manbazar Radha Madhab Institution
  Board: West Bengal Board of Secondary Education

Research Contributions

Publications

2020
- Anindya Ganguly, Abhijit Das, Dipanwita Roy Chowdhury and Deval Mehta, *A Family of Subfield Hyperelliptic Curve for Use in Cryptography*, 22nd International Conference on Information and Communications Security (ICICS 2020), Copenhagen, Denmark, 2020.

Talks

Cynosure-21
- Presented a paper titled "*A Family of Subfield Hyperelliptic Curve for Use in Cryptography*" at Cynosure-2021 & National Symposium on Advances in Mathematics organized by the Department of Mathematics, IIT Ropar.

NSMA-21
- Presented a paper titled "*A Family of Subfield Hyperelliptic Curve for Use in Cryptography*" at NSMA-21 organized by the Department of Mathematics, IIT Madras.

IISF-20
- Gave a talk at named as "*A New Family of Hyperelliptic Curve*" at IISF-2020

Implementations

- Developed an indigenous cryptographic library (in *C*) based on hyperelliptic curves. It includes multi-precision arithmetic, prime field arithmetic, extension field arithmetic, Jacobian arithmetic and various cryptographic primitives.

Achievements and Fellowships

Academic Achievements

- JEST 2019 in Theoretical Computer Science
- GATE 2018 in Computer Science and Engineering
- GATE 2016, 2020 in Mathematics
- National Eligibility Test (NET) in Mathematical Science: UGC-JRF Dec 2015, CSIR-JRF June 2016, CSIR-JRF Dec 2016
- JAM 2014 in Mathematics

Fellowships

Aug-2021-Present
- Institute Assistantship for PhD program at IIT Kanpur, funded by Ministry of Education, Government of India.

2014-2016
- Receive INR12000 (per year) for two years during M.Sc. at IIT Kharagpur.

Membership

- Student member of Cryptology Research Society of India

Research Interest

- Post-quantum cryptography (lattice, multivariate and isogeny-based cryptography) and Quantum Cryptanalysis
- Curve-based cryptography (Elliptic and hyperelliptic curves)
- Crypto motivated Computational Number Theory Problems
- Standardization of Cryptographic Protocols
- Cryptanalysis of symmetric key cryptography

Relevant Courses

- **During PhD (at CSE, IITK)** Computational Complexity, Complexity Measures for Boolean Functions, Modern Cryptography, Computational Algebra and Number Theory, Design for Security
- **During MS (in CSE, IITKGP)** Foundation of Cryptography, Algorithm Design and Analysis, High Performance Computer Architecture, Foundation of Computing Science
- **During M.Sc. (in Math, IITKGP)** Cryptography and Network Security, Number Theory, Information and Coding Theory, Switching and Finite Automata (Only elective papers are mentioned)

Skills

Languages	Strong reading, writing and speaking competencies for Bengali and English. Only speaking competencies for Hindi.
Coding	C, FORTRAN, Java, Python, Verilog, OpenSSL
Mathematical Library	MATLAB, PARI/GP, SageMath, NTL, GMP Library
Quantum	Qskit, QSim, ProjectQ
Documentation	LaTeX, Html

Extra Curricular Activities

Social Work	Volunteer at Ranjit Singh Rozi Shiksha Kendra, IIT Kanpur
Hall attachement	Served General Secretary for Soc & Cult at VSRC, IIT Kharagpur
Hobbies	Member of Technology Dramatic Society, Druheen (IIT Kharagpur) and Boikalik
	Having interest in Photography
	Cooking