Banashri Karmakar

Curriculum Vitae

Department of Computer Science and Automation
Indian Institute of Science, Bangalore, India
✉ *banashrik@iisc.ac.in, banashri1995@gmail.com*
Github *Linkedin*

Education

2022–present **PhD, Computer Science & Engineering**, *Indian Institute of Science*, Bangalore, Karnataka, India.
Topic: Secure Multiparty Computation, Cryptography

2018–2020 : **Master of Technology, Computer Science & Engineering**, *Indian Institute of Technology Bhilai*, Raipur, Chhattisgarh, India.

2012–2016 : **Bachelor of Technology, Computer Science & Engineering**, *Govt. College of Engg. & Textile Technology, Serampore*, Hooghly, West Bengal, India (*Under* Maulana Abul Kalam Azad University of Technology, West Bengal, India).

2012 : **Higher Secondary Examination**, *Haripal Gurudayal Institution*, Hooghly, West Bengal, India.

2010 : **Secondary Examination**, *Haripal Tirthabasi Girls' High School*, Hooghly, West Bengal, India.

Publications

Journal Articles

2022 Anup Kumar Kundu, Aikata, **Banashri Karmakar**, and Dhiman Saha. Fault analysis of the PRINCE family of lightweight ciphers. *J. Cryptogr. Eng.*, volume 12, pages 475–494, 2022.

In Conference Proceedings

2021 Anubhab Baksi, **Banashri Karmakar**, and Vishnu Asutosh Dasu. POSTER: Optimizing Device Implementation of Linear Layers with Automated Tools. In Jianying Zhou, Chuadhry Mujeeb Ahmed, Lejla Batina, Sudipta Chattopadhyay, Olga Gadyatskaya, Chenglu Jin, Jingqiang Lin, Eleonora Losiouk, Bo Luo, Suryadipta Majumdar, Mihalis Maniatakos, Daisuke Mashima, Weizhi Meng, Stjepan Picek, Masaki Shimaoka, Chunhua Su, and Cong Wang, editors, *Applied Cryptography and Network Security Workshops - ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21-24, 2021, Proceedings*, volume 12809 of *Lecture Notes in Computer Science*, pages 500–504. Springer, 2021.

2021 Anubhab Baksi, **Banashri Karmakar**, and Vishnu Asutosh Dasu. POSTER: Another Look at Boyar-Peralta's Algorithm. In Jianying Zhou, Chuadhry Mujeeb Ahmed, Lejla Batina, Sudipta Chattopadhyay, Olga Gadyatskaya, Chenglu Jin, Jingqiang Lin, Eleonora Losiouk, Bo Luo, Suryadipta Majumdar, Mihalis Maniatakos, Daisuke Mashima, Weizhi Meng, Stjepan Picek, Masaki Shimaoka, Chunhua Su, and Cong Wang, editors, *Applied Cryptography and Network Security Workshops - ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21-24, 2021, Proceedings*, volume 12809 of *Lecture Notes in Computer Science*, pages 495–499. Springer, 2021.

2021 Anubhab Baksi, Vishnu Asutosh Dasu, **Banashri Karmakar**, Anupam Chattopadhyay, and Takanori Isobe. Three Input Exclusive-OR Gate Support for Boyar-Peralta's Algorithm. In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *Progress in Cryptology - INDOCRYPT 2021 - 22nd International Conference on Cryptology in India, Jaipur, India, December 12-15, 2021, Proceedings*, volume 13143 of *Lecture Notes in Computer Science*, pages 141–158. Springer, 2021.

2020 Anubhab Baksi, **Banashri Karmakar**, Vishnu Asutosh Dasu, Dhiman Saha, and Anupam Chattopadhyay. Further Insights on Implementation of the Linear Layer. In *SILC Workshop-Security and Implementation of Lightweight Cryptography*, volume 1, 2020.

2020 Anubhab Baksi, Vinay B. Y. Kumar, **Banashri Karmakar**, Shivam Bhasin, Dhiman Saha, and Anupam Chattopadhyay. A Novel Duplication Based Countermeasure to Statistical Ineffective Fault Analysis. In Joseph K. Liu and Hui Cui, editors, *Information Security and Privacy - 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*, volume 12248 of *Lecture Notes in Computer Science*, pages 525–542. Springer, 2020.

2020 Aikata, **Banashri Karmakar**, and Dhiman Saha. PRINCE under Differential Fault Attack: Now in 3D. In Chip-Hong Chang, Ulrich Rührmair, Stefan Katzenbeisser, and Patrick Schaumont, editors, *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES@CCS 2020, Virtual Event, USA, November 13, 2020*, pages 81–91. ACM, 2020.

2020 Aikata, **Banashri Karmakar**, and Dhiman Saha. DESIV: Differential Fault Analysis of SIV-Rijndael256 with a Single Fault. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2020, San Jose, CA, USA, December 7-11, 2020*, pages 241–251. IEEE, 2020.

Projects

Ardent Computech Private Limited, Kolkata, West Bengal, India

Jun, 2015 – Jul, 2015 ***Music Player***, *(Android Application Development)*.
Developed an android application to play music.

Dec, 2014 – Jan, 2015 ***E-Cops***, *(Java Enterprise Edition 7)*.
Developed a Java based web application where people can lodge their complaints, view processing status etc. online and police also can view those complaints online and takes necessary actions.

Research Experience

Indian Institute of Science, Bangalore

Jan, 2022 – present ***Secure Multiparty Computation***.
Doing literature study on secure multiparty computation.

Advisor : **Dr. Arpita Patra**, *Associate Professor, Department of Computer Science & Automation, EECS Division*, IISc Bangalore (*Personal Web-page*)

Indian Institute of Technology Bhilai

May, 2019 – May, 2020 ***Design and Analysis of Lightweight Cryptography***, *(M. Tech Thesis)*.
Analyzed few round-1 candidates from NIST LWC competition and mounted a differential fault attack on one of these. Analyzed few heuristic based algorithms used for estimating the hardware implementation cost of the linear diffusion layer of cryptographic primitives. Focused on the construction of lightweight MDS matrices with minimal d-XOR cost.

Advisor : **Dr. Dhiman Saha**, *Assistant Professor, Department of Electrical Engineering & Computer Science*, IIT Bhilai (*Personal Web-page*)

Teaching Assistantship

2022-23-EVEN : **PEC-IT601A: Advanced Algorithms**, GCELT.

2019-20-W : **CS503: Lightweight Cryptography**, IIT Bhilai.

2019-20-M : **CS553: Cryptography**, IIT Bhilai.

2018-19-S : **CA150: Professional Communication**, IIT Bhilai.

2018-19-W : **CS252: Algorithms II**, IIT Bhilai.

2018-19-M : **IC100: Introduction to Programming**, IIT Bhilai.

Internship

Tata Consultancy Services (Innovation Lab), Hyderabad, Telangana, India

Dec, 2019 – Jan, 2020 ***Improving the cost of AES Mixcolumn Matrix***.
Worked on an algorithm to reduce the number of minimum XOR gates required to implement AES Mixcolumn operation.

Work Experience

Radisys India Private Limited, Bangalore, Karnataka, India

May, 2020 – Feb, 2022 ***Engineer***.
Worked on 5G NR development using C++.

Tata Consultancy Services, Kolkata, West Bengal, India

Mar, 2017 – Jun, 2018 ***Assistant Systems Engineer***.
Worked primarily on Java based software development.

Fellowships & Awards

2023–present Recipient of **Prime Minister Research Felllowship**, Government of India, as a PhD research scholar in Indian Institute of Science, Bangalore.

2022 Recipient of **Junior Research Fellowship** of Ministry of Human Resource Development (MHRD), Government of India, as a PhD research scholar in Indian Institute of Science, Bangalore.

2021 Recipient of **Senate Award** at the 1st convocation of Indian Institute of Technology Bhilai, for securing the highest grade in Computer Science & Engineering, M. Tech.

2018–2020 Recipient of **M. Tech Scholarship** of Ministry of Human Resource Development (MHRD), Government of India, as a M. Tech student in Indian Institute of Technology Bhilai.

2017 Awarded **Star of the Learners Group**, as a quick learner during the training period at Tata Consultancy Services.

2012–2016 Recipient of **Swami Vivekananda Merit-cum-Means Scholarship** of Government of West Bengal, while pursuing B. Tech, for securing more than 75% in Higher Secondary examination.

2011–2012 Recipient of **Swami Vivekananda Merit-cum-Means Scholarship** of Government of West Bengal, for securing more than 75% in Secondary examination.

Academic Achievements & Recognitions

2022–present Member of **Cryptography and Information Security (CRIS) Lab**, IISc Bangalore

2019–2020 Alumni of **de.ci.phe.red Lab**, IIT Bhilai

2019 Qualified for **Junior Research Fellow (JRF) & Assistant Professor** in National Eligibility Test (NET), December, 2019

2018 **All India Rank (AIR) 201** in Graduate Aptitude Test in Engineering (GATE), 2018

Computer skills

Programming Languages: C, C++, Java, Python

Tools / Web Technologies: LaTeX, Eclipse, Leonardo Spectrum, Modelsim, Xilinx Vivado, Xilinx ISE, yEd, Oracle SQL, MySQL, J2EE, Hibernate

Operating Systems: Linux, Windows

Areas of Interest: Secure Multiparty Computation, Cryptography, Blockchain Technology, Algorithms, Operating Systems, Database Management Systems, Computer Architecture