Dr. Dibyendu Roy

Assistant Professor
IIIT Vadodara
Email: dibyendu.roy1988@gmail.com

PERSONAL DETAILS

- Date of Birth: 1st October, 1988
- Nationality: Indian
- Marital Status: Married

EDUCATION

- Ph.D. in Mathematics (Cryptology), (2016)
  Indian Institute of Technology Kharagpur, Kharagpur, India
  Date of Defense Seminar: 15th November, 2016.
  Title of Thesis: "A study on selective stream ciphers and construction of T-function"
  Supervisor: Prof. Sourav Mukhopadhyay
- Master of Science (M.Sc.) in Mathematics, (2011)
  Grade : First Class
  CGPA : 8.40
  Indian Institute of Technology Kharagpur, Kharagpur, India
- Bachelor of Science (B.Sc.) in Mathematics, (2009)
  Grade : First Class
  Marks : 74.38 %
  Ramakrishna Mission Residential College, Narendrapur
  University of Calcutta
- Higher Secondary (H.S.) (10+2) in Science, (2006)
  Grade : First Class
  Marks : 82.7 %
  Arambagh High School
  West Bengal Council of Higher Secondary Education
- Secondary (10), (2004)
  Grade : First Class
  Marks : 82.25 %
  Kamarpukur Ramakrishna Mission Multipurpose School
  West Bengal Board of Secondary Education

PRESENT STATUS

Assistant Professor (Grade II) at IIIT Vadodara.

POST PHD EXPERIENCE

- Indian Institute of Information Technology Vadodara, Gandhinagar Campus, India
  Position: Assistant Professor (Grade II)
  Period: From 28th December to Till date.

- R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India
  Position: Postdoctoral-Fellow-cum-Lecturer
  Period: From October, 2020 to December 2020.
- R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India
  Position: Visiting Scientist
  Period: From April, 2020 to September 2020.
- Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
  Position: Visiting Scientist
  Period: From January, 2020 to March 2020.
- ERTL(E), STQC Dte., Kolkata, India
  Position: Consultant
  Period: From December, 2018 to December, 2019.
- School of Mathematical Sciences, National Institute of Science Education and Research Bhubaneswar, India
  Position: Postdoctoral Researcher
  Period: Two years (November, 2016 – November, 2018).

COURSES TAUGHT

1. Cryptography and Network Security (Theory) – (PG, Even Semester 2021, IIIT Vadodara) (ongoing).
2. Introduction to Cryptography and Network Security (Theory) – (UG, Even Semester 2021, IIIT Vadodara) (ongoing).
3. Introduction to Cryptography and Network Security (LAB) – (UG, Even Semester 2021, IIIT Vadodara) (ongoing).
4. Discrete Mathematics – PG (CrS) Odd Semester 2020-2021, ISI Kolkata jointly with Dr. Sabyasachi Karati.
5. Cryptology – PG, University of Calcutta, Even Semester 2020 jointly with Dr. Bappaditya Ghosh.
6. C++ LAB – UG, NISER, Odd Semester, 2017.
7. Math-I and Math-II tutorials – Dept. of Mathematics, Indian Institute of Technology Kharagpur for 5 semesters.

ACADEMIC ACHIEVEMENTS

- Offered Assistant Professorship position from IIIT Vadodara, India (December, 2020).
- Offered Postdoctoral-Fellow-cum-Lecturer/Assistant Professor position from R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India (September, 2020).
- Offered Visiting Scientist position from R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India (January, 2020).
- Offered Visiting Scientist position from Applied Statistics Unit, Indian Statistical Institute, Kolkata, India (December, 2019).
- Offered Research Scientist from C.R. Rao AIMSCS, Hyderabad, India (June 2019).
- Offered Consultant position from STQC Dte., Kolkata, India (December, 2018).

- Offered Visiting Scientist position from Applied Statistics Unit, Indian Statistical Institute, Kolkata, India (October, 2018).
- Offered Post-doctoral research fellow position from Mobi Sec Lab, Soonchunhyang University, South Korea (November, 2017).
- Offered Post-doctoral research fellow position from National Institute of Science Education and Research Bhubaneswar, India (October, 2016).
- Selected for PhD program in Dept. of Mathematics, Indian Institute of Technology Kharagpur, India.
- Selected for Joint M.Sc. PhD program in Dept. of Mathematics, Indian Institute of Technology Kharagpur, India.

TALKS

1. Invited talk in a short term trainee course on Advanced Topics in Cryptography organized by Dept. of Mathematics, IIT Kharagpur, 2020.
2. Invited talk in a short term trainee course on Cyber Security organized by Dept. of Mathematics, IIT Kharagpur, 2020.
3. "Overview on Signal protocol". Indian Statistical Institute, Kolkata, India. June, 2019.
4. "Cryptanalysis on Some Cryptographic Primitives". Indian Statistical Institute, Kolkata, India. April, 2019.
5. "Tools in analysing linear approximation for Boolean functions related to FLIP". Indian Habitat Centre, Delhi, India, 2018 (Indocrypt 2018).
6. "An Observation of Non-randomness in the KSA of Grain family of stream ciphers". SPACE 2018 (Skype presentation), 2018.
7. "Grain v1: Design & Cryptanalysis", Indian Statistical Institute, Kolkata, India. April, 2018.
8. "Non-randomness in the KSA of Grain family of stream ciphers", SMS, NISER, India. 3 November, 2017.
9. Invited talk in a short term course on "Introduction to Cryptography" organized by Dept. of Mathematics, IIT Kharagpur, 2017.
10. "Fault analysis & weak key-IV attack on Sprout and constructions of T-function", SMS, NISER, India. 26 September, 2016.
11. "New constructions of T-function" , Beihang University, China. 07 May, 2015 (ISPEC 2015).

LIST OF ACCEPTED AND COMMUNICATED BOOKS & ARTICLES

BOOK

1. Chandra Sekhar Mukherjee, Dibyendu Roy and Subhamoy Maitra. "Design & Cryptanalysis of ZUC: A Stream Cipher in Mobile Telephony", DOI: 10.1007/978-981-33-4882-0, Springer.

PUBLISHED/ACCEPTED ARTICLES

JOURNALS

1. Dibyendu Roy, Deepak Kumar Dalai. "An Observation of Non-randomness in NFSR Based Stream Ciphers with Reduced Initialization Round". Journal of Hardware and Systems Security, 2021. (To appear)

2. Dibyendu Roy, Bhagwan Bathe and Subhamoy Maitra. "Differential Fault Attack on - Kreyvium & FLIP". IEEE Transactions on Computers, DOI: 10.1109/TC.2020.3038236, 2020.

3. Ravi Anand, Dibyendu Roy and Santanu Sarkar. "Some results on lightweight stream ciphers Fountain v1 & Lizard". Advances in Mathematics of Communications, American Institute of Mathematical Sciences, DOI: 10.3934/amc.2020128, 2020.

4. Chandra Sekhar Mukherjee, Subhamoy Maitra, Vineet Gaurav and Dibyendu Roy. "On Actual Preparation of Dicke State on a Quantum Computer". IEEE Transactions on Quantum Engineering, DOI: 10.1109/TQE.2020.3041479, 2020.

5. Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy and Pantelimon Stănică. "Analysis on Boolean function in a restricted (biased) domain". IEEE Transactions on Information Theory, Vol. 66, pp. 1219–1231, 2020.

6. Abhishek Kesarwani, Dibyendu Roy, Santanu Sarkar and Willi Meier. "New cube distinguishers on NFSR-based stream ciphers". Designs, Codes and Cryptography, Springer, Vol. 88, pp. 173–199, 2020.

7. Deepak Kumar Dalai, Subhamoy Maitra, Santu Pal and Dibyendu Roy. "Distinguisher & Non-randomness of Grain-v1 for 112, 114 & 116 initialization rounds with multiple-bit difference in IVs". IET Information Security, IET Digital Library, Vol. 13, pp. 603–613, 2019.

8. Dibyendu Roy, Pratish Datta and Sourav Mukhopadhyay, "Algebraic cryptanalysis of stream ciphers using decomposition of Boolean function". Journal of Applied Mathematics and Computing, Springer, Vol. 49, pp. 397–417, 2015.

CONFERENCES

1. Akhilesh Anilkumar Siddhanti, Srinivasu Bodapati, Anupam Chattopadhyay, Subhamoy Maitra, Dibyendu Roy and Pantelimon Stănică. "Analysis of the Strict Avalanche Criterion in variants of Arbiter-based Physically Unclonable Functions ". In the Proceeding of the 20th International Conference on Cryptology in India (Indocrypt 2019) LNCS, Springer, 2019.

2. Debajyoti Bera, Subhamoy Maitra, Dibyendu Roy and Pantelimon Stănică."Limitation of the BLR testing in estimating nonlinearity (Extended Abstract)". WCC 2019: The Eleventh International Workshop on Coding and Cryptography, 2019.

3. Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy and Pantelimon Stănică. "Tools in analysing linear approximation for Boolean functions related to FLIP". In the Proceeding of the 19th International Conference on Cryptology in India (Indocrypt 2018), LNCS, Springer, 2018.

4. Deepak Kumar Dalai and Dibyendu Roy. "An Observation of Non-randomness in the KSA of Grain family of stream ciphers". In the Proceeding of the 8th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2018), LNCS, Springer, 2018.

5. Deepak Kumar Dalai and Dibyendu Roy. "A state recovery attack on ACORN-v1 and ACORN-v2", In the Proceeding of the 11th International Conference on Network and System Security (NSS 2017) , LNCS, Springer, 2017.

6. Dibyendu Roy, Sourav Mukhopadhyay. "A deterministic approach for finding cube variables for cube attack (short paper)". In 12th International Conference on Information Security and Cryptology (Inscrypt 2016), 2016.

7. Dibyendu Roy, Ankita Chaturvedi and Sourav Mukhopadhyay. "New constructions of T-function", In the Proceeding of the 11th Information Security Practice and Experience Conference (ISPEC 2015), LNCS, Springer, 2015.

8. Pratish Datta, Dibyendu Roy and Sourav Mukhopadhyay. "A probabilistic algebraic attack on the Grain family of stream ciphers". In the Proceeding of the 8th International Conference on Network and System Security (NSS 2014), LNCS, Springer, 2014.
9. Dibyendu Roy, Pratish Datta and Sourav Mukhopadhyay. "A new variant of algebraic attack". In the Proceeding of the 2nd International Conference on Security in Computer Networks and Distributed Systems (SNDS 2014), CCIS, Springer, 2014.

TECHNICAL REPORTS

1. Dibyendu Roy and Sourav Mukhopadhyay. "Some results on ACORN". IACR Cryptology ePrint Archive 2016: 1132.
2. Dibyendu Roy and Sourav Mukhopadhyay. "Fault analysis and weak key-IV attack on Sprout". IACR Cryptology ePrint Archive 2016: 207.
3. Dibyendu Roy and Sourav Mukhopadhyay. "Fault analysis on the stream ciphers LILI-128 and Achterbahn". IACR Cryptology ePrint Archive 2015: 1077.

REFERENCES

- Prof. Sourav Mukhopadhyay
  Dept. of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302,
  E-mail: sourav@maths.iitkgp.ernet.in
- Prof. Subhamoy Maitra
  Applied Statistics Unit, Indian Statistical Institute, Kolkata- 700108,
  E-mail: subho@isical.ac.in
- Prof. Pantelimon Stănică
  Applied Mathematics Department & Center for Joint Services Electronic Warfare,
  Naval Postgraduate School, Monterey, CA 93943,
  E-mail: pstanica@nps.edu