Mahesh Sreekumar Rajasree[1][2]

Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi, India

PRINCIPAL INTERESTS Lattice theory, Algorithms, Computational Complexity, Cryptanalysis, Cryptography

Employment

Post Doc. Computer Science and Engineering April 2023 - Present
Indian Institute of Technology Delhi, New Delhi, India

ACADEMIC BACKGROUND

Ph.D. & M.Tech. Computer Science and Engineering August 2016 - Present
Indian Institute of Technology Kanpur, Uttar Pradesh, India

- Advisor: Prof. Manindra Agrawal
- Ph.D. Thesis: Analysis of Symmetric-Key Cryptosystems and Subset-Sum Problem
- M.Tech. Thesis: New Results and Proofs in Lattice Theory
- CPI: 10/10

B.Tech. Computer Science and Engineering August 2012 - May 2016
National Institute of Technology Calicut, Kerala, India

- Advisor: Dr. Sumesh T.A.
- B.Tech. Thesis: Firewall for Preventing Anonymous Proxy Usage
- CPI: 8.89/10

Secondary & Higher Secondary Education June 2009 - March 2012
Arya Central School, Trivandrum, Kerala, India

- All India Senior Secondary School Examination Percentage: 91.2
- All India Secondary School Examination CGPA: 9.6/10

Peer-reviewed Works

1. **Cryptanalysis of 1-Round KECCAK**
   with Rajendra Kumar and Hoda Al Khzaimi,
   10th International Conference on Cryptology, AFRICACRYPT 2018
2. **Cryptanalysis of Round-Reduced KECCAK using Non-Linear Structures**
   20th International Conference on Cryptology, INDOCRYPT 2019
3. **Algebraic algorithms for variants of Subset Sum problem**
   with Pranjal Dutta,
   8th Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2022 (**Best Student Presentation Award**)
4. **On the hardness of monomial detection and zero-sum distinguishers for Ascon**
   with Pranjal Dutta and Santanu Sarkar,
   12th International Workshop on Coding and Cryptography, WCC 2022

[1] srmahesh@iitd.ac.in
[2] https://sites.google.com/view/mahesh-sreekumar-rajasree

5. **Weak-keys and key-recovery attack for TinyJAMBU**
   with Pranjal Dutta and Santanu Sarkar,
   Scientific Report, Nature
6. **On the bases of $\mathbb{Z}^n$ lattice**
   with Shashank K Mehta,
   24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNACS 2022
7. **Efficient reductions and algorithms for Subset Product**
   with Pranjal Dutta,
   9th Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2023 (**Best Student Presentation Award**)

Unpubished works (Not submitted)

1. **On the Selective Opening Security of Pointcheval's transformation**
2. **Efficient Lattice and Algebraic Algorithms for Two Variants of Subset Sum**
   with Pranjal Dutta
3. **A New Reduction among Lattice Problems**
   with Rajendra Kumar and Shashank K Mehta

Academic Achievements

1. Won the Best Student Presentation award (one of the 5 winners) in CALDAM 2023.
2. Won the Best Student Presentation award (one of the 3 winners) in CALDAM 2022.
3. Awarded Prime Minister's Research Fellowship in 2018 (received approximately USD 50,000 for a duration of 4 years to cover stipend and other expenses relaled to research).
4. Awarded Academic Excellence 2017 at IIT Kanpur.
5. Secured All Indian Rank 28 in Joint Entrance Screening Test (JEST-2016).
6. Secured All India Rank 575 in Graduate Aptitude Test in Engineering (GATE 2016)
7. Secured fourth place in the first round of Amrita InCTF 2015.

Research Internships & Projects

1. Visiting scholar at Microsoft Research India hosted by Satya Lokam (Jun 2018, Oct 2018, Mar 2019, Sept 2019).
2. Visited Prof. Hoda AlKhzaimi at New York University, Abu Dhabi (Oct 2017).
3. Automated subglottic secretions drainage device for patients in ventilators - Programmed the arduino of a device which helps to drain subglottic secretions automatically at particular intervals on the patient specific data input by the doctor.

Short Term Research Visit

1. **Institute of Science and Technology Austria**, Host: Dr. Krzysztof Pietrzak
2. **Indian Insitute of Technology Delhi**, Host: Dr. Venkata Koppula

Academic Talks and Presentations

1. **CALDAM 2023**, Conference Talk.
   Title: Efficient reductions and algorithms for Subset Product
2. **SYNACS 2022**, Conference Talk.
   Title: On the bases of $\mathbb{Z}^n$ lattice
3. **SIGTACS**, CSE, IIT Kanpur.
   Title: On the hardness of monomial prediction problem.
4. **Invited Talk**, CSE, IUST Jammu & Kashmir.
   Title: On the Subset Sum Problem.
5. **SIGTACS**, CSE, IIT Kanpur.
   Title: An Algebraic Algorithm for Hamming Subset-Sum Problem.
6. **WCC 2022**, Workshop Talk.
   Title: On the hardness of monomial prediction problem.
7. **Invited Talk**, PMRF Symposium.
   Title: Cryptanalysis of KECCAK & Algorithms for Lattice Problems.
8. **SIGTACS**, CSE, IIT Kanpur.
   Title: Cryptanalysis of Round-Reduced KECCAK using Non-linear Structures.
9. **INDOCRYPT 2019**, Conference Talk.
   Title: Cryptanalysis of Round-Reduced KECCAK using Non-Linear Structures.
10. **SIGTACS**, CSE, IIT Kanpur.
    Title: Leftover Hash Lemma
11. **SIGTACS**, CSE, IIT Kanpur.
    Title: Lattices in Computer Science
12. **SIGTACS**, CSE, IIT Kanpur.
    Title: A Deterministic Exponential Time Algorithm for some lattice problems

Teaching Experience

1. Modern Cryptology at Emaster Program, IITK 2023, 2022
2. Introduction to Linear Algebra at Emaster Program, IITK 2022
3. Modern Algebra at NPTEL 2021, 2018
4. Modern Cryptology at IITK 2021, 2020, 2019, 2018, 2017
5. Data Structures and Algorithms at IITK 2019, 2018, 2017
6. Mathematics for Computer Science at IITK 2020

Professional Activities

1. Reviewed for INDOCRYPT 2021.

Volunteer Works

1. Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2017.
2. Cybersecurity Awareness Week CSAW 2017.
3. Head Coordinator of Special Interest Group on Theoretical Aspects of Computer Science SIGTACS at IIT Kanpur.

Conference & Workshop Attended (online)

1. 9th Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2023, Gandhinagar, India.
2. 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNACS 2022, Hagenberg, Austria.
3. Quantum Algorithms at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
4. Quantum Cryptanalysis of Post-Quantum Cryptography at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
5. Lattices: Geometry, Algorithms and Hardness at Simons Institute for the Theory of Computing (2020), Berkeley, USA.
6. Secure Multiparty Computation: Theory and Practice workshop held at IISc (2020), Bangalore, India.
7. 20th International Conference on Cryptology, INDOCRYPT 2019, Hyderabad, India.
8. Theory of Cryptography Conference, TCC 2018, Goa, India.
9. 37th Foundations of Software Technology and Theoretical Computer Science 2017, Kanpur, India.

Conference & Workshop Attended (offline)

1. 12th International Workshop on Coding and Cryptography, WCC 2022.
2. 8th Annual International Conference on Algorithms and Discrete Applied Mathematics, CALDAM 2022

Referees

1. **Dr. Venkata Koppula**
   Assistant Professor
   Department of CSE, IIT Delhi
2. **Dr. Nikhil Balaji**
   Assistant Professor
   Department of CSE, IIT Delhi
3. **Dr. Manindra Agrawal**
   Professor
   Department of CSE, IIT Kanpur
4. **Dr. Shashank K Mehta**
   Professor (Retired)
   Department of CSE, IIT Kanpur