Subhadip Singha

Post-Doctoral Research Fellow in Computer Science

Deaprtment of Combinatorics and Optimization
University of Waterloo
email: subhadip2404@gmail.com

Profile Highlights:

I am a post-doctoral research fellow in computer science with an interdisciplinary research interest in both theoretical and practical aspects of computer science.

Research:

- I have worked on lattice-based cryptography for my doctoral thesis.
- Analysis of various lattice-based reductions from a practice-oriented perspective.
- Studying the "Learning With Error" (LWE) problem and its utility in lattice-based cryptography.
- Concrete security analysis of NIST's candidates for lattice-based post-quantum cryptography.

1 Position

- **Post-doctoral Fellow** at Deaprtment of Combinatorics and Optimization of University of Waterloo, November, 2023 - till date.
  Supervisor: Dr. Douglas Stebila.

2 Academic Degrees

- **Doctor of Philosophy in Computer Science** from Indian Statistical Institute, 2016 - 2023.
  Supervisor: Prof. Palash Sarkar.
  Thesis title: "*On the Tightness Gap Analysis of Reductions of some Lattice problems to the Learning with Error problem*".

- **Master of Technology in Computer Science** from Indian Statistical Institute, 2014 - 2016.
  Passed in **First Division with Honours**.
  Overall percentage: 83.70%. Received **book grants**, awarded for outstanding performance in the third semester.

- **Bachelor of Engineering in Computer Science and Engineering** from Jadavpur University, 2006 - 2010.
  Passed in **First Class**. Scored an average of 73.69% over the 8 semesters.

- **Higher Secondary[10(+2)](WBCHSE)** from Hooghly Collegiate School, Chinsurah, 2006.
  Based on the marks obtained in Bengali, English, Mathematics, Physics and Chemistry, Statistics (Additional)
  Ranked **3rd in school**.
  Percentage: 93.50.

- **Madhyamik[10](WBBSE)** from Hooghly Collegiate School, Chinsurah, 2004.
  Based on the marks of Bengali, English, Mathematics, Physical Science, Life Science, History, Geography, and Physics (Additional):
  Percentage: 83.25.

3 Publications

3.1 Journal Publications

1. Palash Sarkar and Subhadip Singha. Verifying Solutions to LWE with Implications for Concrete Security. **Advances in Mathematics of Communications**, May 2021, 15(2): 257-266, https://www.aimsciences.org/article/doi/10.3934/amc.2020057.

2. Palash Sarkar and Subhadip Singha. Classical Reduction of GapSVP to LWE: A Concrete Security Analysis. **Advances in Mathematics of Communications**, https://www.aimsciences.org/article/doi/10.3934/amc.2021004.

3. Neal Koblitz, Subhabrata Samajder, Palash Sarkar, Subhadip Singha. Concrete Analysis of Approximate Ideal-SIVP to Decision Ring-LWE Reduction. **Advances in Mathematics of Communications**, https://www.aimsciences.org/article/doi/10.3934/amc.2022082.

3.2 Editorial Work

I have reviewed a paper for the Africacrypt'18 conferences.

3.3 Dissertation

- **M. Tech Dissertation:** "A Study on Cryptographic Key Exchange Protocols" under the supervision of Dr. Rishiraj Bhattacharyya in Indian Statistical Institute, Kolkata.
- **B.E. Dissertation:** "A Practical Implementation of AES" under the supervision of Prof. Anupam Sinha in Jadavpur University, Kolkata.

4 Some attainments

- Qualified for **Lecturership** in the National Eligibility Test (NET) in Computer Science in 2019, conducted by the University Grants Commission (UGC).
- Secured **Senior Research Fellowship** in Indian Statistical Institute for 2018 - 2022.
- Secured **Junior Research Fellowship** in Indian Statistical Institute for 2016 - 2018.
- Secured **99.58 percentile** (out of more than two lakh examinees) in the (Indian) national level Graduate Aptitude Test in Engineering (GATE) 2013 examinations.
- Ranked **130** (out of 76327 examinees) in the state-level West Bengal Joint Entrance Examinations (WBJEE) 2006, India.

4.1 Industry

- February 2011 - July 2014: **Deloitte Consulting**, Gurugram.
  Position: **Technical Consultant**.
  Client: Various Indian government and non-government clients.
  Product: SAP.
  Responsibilities: Understanding and automating the business process through enterprise resource planning (ERP) software SAP. Additionally, proposing solutions for optimizing processes for higher efficiency for different enterprises in different areas like finance, human resources, production planning, material management, and data-analytic modules.

4.2 Internships and Visiting Positions

- May 2015 - August 2015: **Indian Statistical Institute**, Kolkata.
  I worked under the supervision of Dr. Rishiraj Bhattacharyya in designing Key Exchange Protocols for memory-constrained devices.
- December 2022 - August 2023: **TCS Research**, Bengaluru.
  I am working with the cryptography team, supervised by Dr. Rajan MA and Dr. Habeeb Syed in designing post-quantum digital signature protocols using multivariate cryptography.

- September 2023 - October 2023: **R. C. Bose Centre for Cryptology and Security** of **Indian Statistical Institute**, Kolkata.
  I worked with Dr. Sabyasachi Karati in a reading course on **Algebraic Number Theory**.

5 Personal Details

Name: SUBHADIP SINGHA.
Mailing Address:
386 Hazel Street, Waterloo, ON N2L 3P6, Canada.
E-mail Address: subhadip2404@gmail.com
Mobile Number: +1 548 577 1049
Date of Birth: 2^{nd} April, 1989.
Nationality: Indian.

6 References

- **Prof. Palash Sarkar**
  Indian Statistical Institute.
  palash@isical.ac.in
- **Prof. Neal Koblitz**
  Department of Mathematics - University of Washington.
  koblitz@math.washington.edu
- **Prof. Bimal Kumar Roy**
  Indian Statistical Institute, Kolkata.
  bimal@isical.ac.in
- **Dr. Rishiraj Bhattacharyya**
  School of Computer Science - University of Birmingham.
  r.bhattacharyya@bham.ac.uk
- **Dr. Douglas Stebila**
  Department of Combinatorics and Optimization - University of Waterloo.
  dstebila@uwaterloo.ca