

Subhadip Singha

Research Fellow in Computer Science

Applied Statistics Unit
Indian Statistical Institute, Kolkata
email: subhadip2404@gmail.com

Profile Highlights:

I am a senior 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 Academic Degrees

- **Doctor of Philosophy in Computer Science** from [Indian Statistical Institute](#), 2016 - 2023.
Submitted on March, 2023.
Supervisor: [Prof Palash Sarkar](#).
- **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.

2 Publications

2.1 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.aims sciences.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.aims sciences.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.aims sciences.org/article/doi/10.3934/amc.2022082>.

2.2 Editorial Work

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

2.3 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.

3 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 (WB-JEE) 2006, India.

3.1 Industry

- February 2011 - July 2014: [Deloitte Consulting](#), Gurugram.
Position: **Technical Consultant**.
Client: Various Indian Government and non-Government Clients.
Product: SAP.
Responsibilities: Understanding the business process and automating the 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.

3.2 Internships

- May 2015 - August 2015: [Indian Statistical Institute](#), Kolkata.
I worked under the supervision of [Dr. Rishiraj Bhattacharyya](#) in designing Key Exchange Protocols for memory constraints devices.
- December 2022 - till date: [TCS Research](#), Bengaluru.
I am working with the cryptography team, supervised by [Dr. Rajan M A](#) in designing post-quantum digital signature protocols using multivariate cryptography.

4 Personal Details

Name: SUBHADIP SINGHA.

Mailing Address:

Bidya Bhaban Pally, Farm Side Road, 1st Lane, Chinsurah, Hooghly, INDIA. Pin - 712102.

E-mail Address: subhadip2404@gmail.com

Mobile Number: +91 9836205521
Date of Birth: 2nd April, 1989.
Nationality: Indian.

5 References

- **Prof Palash Sarkar**
Indian Statistical Institute.
palash@isical.ac.in
- **Dr Rishiraj Bhattacharyya**
School of Computer Science - University of Birmingham.
r.bhattacharyya@bham.ac.uk
- **Prof Neal Koblitz**
Department of Mathematics - University of Washington.
koblitz@math.washington.edu