

BINANDA SENGUPTA

CONTACT INFORMATION	Applied Statistics Unit Indian Statistical Institute 203 Barrackpore Trunk Road Kolkata 700108, India	E-mail: binanda_r@isical.ac.in binujucse3@gmail.com
RESEARCH INTERESTS	Cryptography, Security and Privacy, Coding Theory, Computational Number Theory	
CURRENT AFFILIATION	PhD Student (Senior Research Fellow) (2013 – present) Applied Statistics Unit, Indian Statistical Institute, Kolkata PhD Supervisor: Dr. Sushmita Ruj	
EDUCATION	Master of Science (MS) (2010 – 2013) Department of Computer Science and Engineering Indian Institute of Technology Kharagpur Thesis Title: SIMD-Based Implementations of Sieving in Integer-Factoring Algorithms Thesis Advisor: Dr. Abhijit Das Bachelor of Engineering (2003 – 2007) Department of Computer Science and Engineering Jadavpur University, Kolkata	
CONFERENCE PUBLICATIONS	Abhishek Singh, Binanda Sengupta and Sushmita Ruj, <i>Certificate Transparency with Enhancements and Short Proofs</i> , in Australasian Conference on Information Security and Privacy (ACISP 2017) Binanda Sengupta and Sushmita Ruj, <i>Publicly Verifiable Secure Cloud Storage for Dynamic Data Using Secure Network Coding</i> , in ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016) Binanda Sengupta, Samiran Bag, Sushmita Ruj and Kouichi Sakurai, <i>Retricoin: Bitcoin Based on Compact Proofs of Retrievability</i> , in International Conference on Distributed Computing and Networking (ICDCN 2016) Binanda Sengupta and Abhijit Das, <i>SIMD-Based Implementations of Sieving in Integer-Factoring Algorithms</i> , in International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2013)	
JOURNAL PUBLICATIONS	Binanda Sengupta and Sushmita Ruj, <i>Efficient Proofs of Retrievability with Public Verifiability for Dynamic Cloud Storage</i> , IEEE Transactions on Cloud Computing, (accepted, 2017) Binanda Sengupta and Abhijit Das, <i>Use of SIMD-Based Data Parallelism to Speed up Sieving in Integer-Factoring Algorithms</i> , Applied Mathematics and Computation, Volume 293, Elsevier, January 2017	
MANUSCRIPT	Binanda Sengupta and Sushmita Ruj, <i>Secure Cloud Storage with Data Dynamics and Privacy-Preserving Audits Using Secure Network Coding</i> (2016)	

BOOK CHAPTER Binanda Sengupta and Sushmita Ruj, *Cloud Data Auditing Using Proofs of Retrievability*, Guide to Security Assurance for Cloud Computing, Springer International Publishing (2015)

INTERNSHIP Research intern at Microsoft Research India, Summer 2016 (mentored by Dr. Satya Lokam)

ACADEMIC VISIT Sakurai Laboratory, Kyushu University, Japan, June 2015 (hosted by Prof. Kouichi Sakurai)

INVITED TALKS An Introduction to Proofs of Retrievability. Crypto Seminar Series, Institute of Mathematics for Industry, Kyushu University, Japan, June 2015

An Introduction to Proofs of Retrievability and Its Application in Bitcoin. Institute of Systems, Information Technologies and Nanotechnologies, Fukuoka, Japan, June 2015

SIMD-Based Implementations of Sieving in Integer-Factoring Algorithms. Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University, Japan, June 2015

REVIEWED PAPERS FOR Asiacrypt 2017, ISPEC 2017, IEEE ICC 2017, ACISP 2016, INDOCRYPT 2015

RESEARCH PROJECT “Investigation of Cryptanalytic Techniques” under the guidance of Dr. Abhijit Das at the Department of Computer Science and Engineering, IIT Kharagpur (2010 – 2012)

INDUSTRIAL EXPERIENCE Worked as an Assistant Systems Engineer at Tata Consultancy Services Limited, Kolkata in the field of data warehousing (2007 - 2010)

MAJOR SUBJECTS STUDIED AT GRADUATE LEVEL

- Advanced Cryptology
- Algorithm Design and Analysis
- Automata, Languages and Computation
- Computational Number Theory
- Cryptology
- Discrete Mathematics
- Foundations of Computing Science
- Information and Coding Theory
- Probability and Stochastic Processes

TEACHING

- Cryptology Internship Program, ISI Kolkata, 2017
- Cryptology Internship Program, ISI Kolkata, 2015
- Teaching Assistantship (IIT Kharagpur): Formal Languages and Automata Theory, Algorithms (Theory and Laboratory)